

# B LIST



99

99

BROW)

**From:** Gaudino, Francesca <Francesca.Gaudino@bakermckenzie.com>  
**Sent:** 19 February 2013 19:59  
**To:** (MARKT)  
**Cc:** (MARKT); (MARKT); (MARKT);  
**Subject:** RE: National Legal Frame Work in the member States

Dear

Thanks for this information. At first sight it appears that most of the comments are due to the fact that specific information is reported in the country summaries and/or in the country specific questionnaires. In any case, we are taking due care of all the comments and will address them in our final version of the Study.

With kind regards,  
Francesca

Francesca Gaudino  
Counsel

Studio Professionale Associato a  
Baker & McKenzie  
3, Piazza Filippo Meda  
20121 Milan, Italy  
Tel: +39 02.76.231.1  
Fax: + 39 02.76.231.501



Do you really need to print this e-mail?  
Think twice and protect the environment, now.

---

**From:** @ec.europa.eu [mailto: @ec.europa.eu]  
**Sent:** martedì 19 febbraio 2013 15:49  
**To:** Gaudino, Francesca  
**Cc:** @ec.europa.eu @ec.europa.eu; @ec.europa.eu;  
@ec.europa.eu  
**Subject:** National Legal Frame Work in the member States

Dear Francesca,

In an informal meeting that we had with representatives of Member States in December, we have made available to them a short overview of the differences in the national law, based on the results of the Hogan Lovells study and the preliminary results of your study – see doc attached.

As a result we have received comments from some of the Member States, which we would like you to take into account when presenting the final version of the study.

For that purpose, I attach the replies that we have received; except for Luxembourg and Sweden which have replied that the summary was accurate.

Having said this we would still need to receive the final version as soon as possible.

Kind regards,



**EUROPEAN COMMISSION**

Internal Market and Services DG

D3 - Fight against counterfeiting and piracy

Rue de Spa 2, B-1049 Brussels

Tel. (+32) 27

<mailto:>

[ec.europa.eu](http://ec.europa.eu)

This message may contain confidential and privileged information. If it has been sent to you in error, please reply to advise the sender of the error and then immediately delete this message. Please visit [www.bakermckenzie.com/disclaimer\\_italy](http://www.bakermckenzie.com/disclaimer_italy) for other important information concerning this message.

Questo messaggio può contenere informazioni confidenziali tutelate da segreto professionale. Se avete ricevuto questo messaggio per errore, vogliate per cortesia informare il mittente immediatamente rispondendo a questo messaggio e provvedendo quindi a cancellarlo dal vostro computer. Visitate [www.bakermckenzie.com/disclaimer\\_italy](http://www.bakermckenzie.com/disclaimer_italy) per ulteriori importanti informazioni riguardanti questo messaggio.

## LEGISLATIVE FRAMEWORK IN EU MEMBER STATES ON THE PROTECTION OF TRADE SECRETS AGAINST MISAPPROPRIATION

*N.B. Unless otherwise stated, the information contained in this annex is based on: (a) the results of a study recently conducted by Hogan Lovells for the Commission on this matter (available at: [http://ec.europa.eu/internal\\_market/iprenforcement/documents/index\\_en.htm#maincontentSec2](http://ec.europa.eu/internal_market/iprenforcement/documents/index_en.htm#maincontentSec2)) and (b) the preliminary results of another study being carried out for the Commission (by Baker & McKenzie, final results expected for 1<sup>st</sup> quarter 2013).*

### INTRODUCTION

Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)<sup>1</sup> requires its signatories to protect "undisclosed information" (see Box 1).

#### **Box 1 - Article 39 of the TRIPS**

*"1. In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967)<sup>2</sup>, Members shall protect undisclosed information in accordance with paragraph 2 and the data submitted to governments or governmental agencies in accordance with paragraph 3.*

*2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices<sup>10</sup> so as long as such information:*

- (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;*
- (b) has commercial value because it is secret; and*
- (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.*

*3. Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use."*

<sup>10</sup> For the purpose of this provision, "a manner contrary to honest commercial practices" shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition.

There is no specific EU law directly dealing with the misappropriation of trade secrets by third parties (i.e. the case referred to in paragraph 2 of Article 39 of the TRIPS). Therefore, the protection of trade secrets against misappropriation by third parties is primarily addressed by national legislation.

National laws in this area provide for different types of protection. Table 1 provides an overview per country of this protection, which is explained the following sections of this Annex.

<sup>1</sup> The TRIPS is a multilateral agreement which must be joined to by all the members of the World Trade Organisation (WTO).

<sup>2</sup> Cf. The Stockholm Act of the Paris Convention for the Protection of Industrial Property, 14 July 1967.

**Table 1 – Main protection against trade secrets misappropriation by national law**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK	
Trade secrets specific law																								✓				
Trade secret protection in intellectual property code															✓							✓						
Unfair competition law (civil and criminal provisions)	✓				✓	✓	✓											✓			✓		✓					
Unfair competition law (civil provisions only)		✓	✓					✓		✓	✓		✓			✓	✓								✓	✓		
Unfair competition law (criminal provisions only)				✓					✓													✓						
Common law (breach of confidence)														✓												✓		
Criminal law other than unfair competition	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓		
Tort law		✓				✓			✓			✓			✓		✓			✓								
Contract law ONLY																				✓								
Labour law																												
	Most Member States																											

Most Member States

However, there are EU rules concerning the treatment of confidential information submitted to public authorities pursuant to legal obligations (i.e. corresponding to the case described in paragraph 3 of Article 39 of the TRIPS). See below Section (E).

### (A) CIVIL/COMMERCIAL LAW<sup>3</sup>

#### (A.1) Civil/commercial law protection in national law: summary

##### (i) Summary

All EU Member States offer some, more or less extensive, form of protection against the misappropriation of trade secrets, albeit this is achieved in different ways.

Some Member States have specific provisions in their civil/commercial law providing protection against the misappropriation of trade secrets

- Sweden has an Act specifically directed against the misappropriation of trade secrets.
- In Italy and Portugal, specific provisions on the protection of trade secrets are included in their respective codes of industrial property – although this does not mean that trade secrets are intellectual property rights.

Other Member States have more general legislation which can be applied.

- Most of them deal with the issue via their law of unfair competition (either civil or criminal provisions, or both): Austria, Belgium, Bulgaria, Czech Republic, Germany, Denmark, Estonia, Greece, Spain, Finland, Hungary, Latvia, Lithuania, Poland, Romania, Slovenia, Slovakia.
- Tort law (or liability for non-contractual responsibility) is used in some countries, either as the main means to address trade secrets misappropriation (Luxembourg, Netherlands) or supplementing the protection offered by unfair competition law (Belgium, Greece).

<sup>3</sup> Understood as opposed to criminal law. It therefore includes: contract law, labour law, unfair competition law, tort law, intellectual property law.

Almost all jurisdictions have general provisions included in their labour laws or civil codes to prevent employees disclosing their employers' trade secrets, at least during the employment relationship. Contract law can be used to protect trade secrets in all of them, but only Malta seems to exclusively rely on contract law to protect trade secrets.

Common law countries (Ireland, United Kingdom) have developed case law (cf. regarding breach of confidence) in the absence of legislation.

*(ii) Civil rules in Member States<sup>4</sup>*

AT (Austria): Austria's Unfair Competition Act provides civil (and criminal) sanctions against trade or business secret misuse by employees and those who exploit such information without consent for the purposes of competition. Other legislation such as the Patents Act and the Criminal Code also provides legal remedies in particular circumstances, such as disclosure of inventions by employees or in cases of industrial espionage. In addition, the Austrian courts have held that obtaining trade or business secrets by breach of confidence (in the course of contractual negotiations) falls within the Unfair Competition Act.

BE (Belgium): There is no one piece of legislation on the protection of trade secrets as such in Belgium but there are several provisions of Belgian law which can be used against the misuse or disclosure of trade secrets. Trade secret owners generally rely on the general law of tort (Article 1382 of the Belgian Civil Code), unfair competition and specific provisions in Belgian labour law.

BG (Bulgaria): There is no specific legislation on trade secrets in Bulgaria but various laws including the Law on Protection of Competition and the Law on Access to Public Information contain general provisions which may be used to protect trade secrets. In fact, there are over 60 such statutory and non-statutory provisions (including criminal liability under the Criminal Code).

CY (Cyprus): There is no specific legislation governing trade secret misuse in Cyprus but there are a number of different laws which mention trade, business and professional secrets. For example, the Commercial Descriptions Law, the General Product Safety Law and the Competition Law. However, liability is criminal; there is no civil liability for trade secret misuse.

CZ (Czech Republic): The Czech Commercial Code defines a trade secret and provides remedies for trade secret infringement. The TRIPS Agreement is directly applicable in Czech law and thus the definition of a trade secret under Article 39(2) of the TRIPS Agreement also applies in Czech law. The basis of trade secret protection in the Czech Commercial Code, however, is the civil law of unfair competition.

DE (Germany): There are a number of provisions in German legislation protecting trade secrets. The most important statutory provisions for the protection of trade secrets are found in the Act against Unfair Competition. These provisions apply to employees and to third parties. Many of the statutes protecting trade secrets under the criminal law also have civil law provisions. These provisions allow for damages and injunctive relief if one of the relevant criminal law provisions is violated. Civil law remedies are also available under the Civil Code (tort law). German contract law also provides effective protection where there is a contractual obligation to maintain the secrecy of trade secrets.

DK (Denmark): In Denmark there is no statutory definition of trade secrets; however case law has clarified the types of information that are protectable to include both technical and

---

<sup>4</sup> See generally Hogan Lovells (2012).

commercial information. Several statutes, both civil and criminal, are used to protect the rights of trade secret owners as well as legal principles derived from contract law, competition law, employment law and unfair competition law. Most notably, the Criminal Code and the Marketing Practices Act contain provisions protecting trade secrets.

EE (Estonia): Estonian legislation provides specific provisions on the protection of trade secrets, most notably in the Competition Act, the Commercial Code, the Employment Contracts Act and the Penal Code. The Competition Act includes an illustrative list of information considered to constitute trade secrets. The Supreme Court has also held that in addition to this definition, the definition of trade secrets provided in the TRIPS Agreement can also be used to interpret the term "trade secrets" under Estonian law.

EL (Greece): Greek Unfair Competition Law provides specific provisions on the protection of trade secrets. More general protection is found in the Greek Civil Code which includes general tort provisions.

ES (Spain): Trade secrets are mainly protected in Spain under the Unfair Competition Act and the Criminal Code. The Act contains provisions specifically aimed at trade secrets. There are also other laws which deal with trade secret protection indirectly, for example, the laws establishing the obligations of directors and other employees.

FI (Finland): There are a number of Acts which include provisions for the protection of trade secrets, most importantly the Unfair Business Practices Act, the Employment Contracts Act and the Criminal Code. Unlike its neighbour, Sweden, Finland does not have one piece of legislation directed specifically to the protection of trade secrets. Although trade secrets are not considered to be typical intellectual property rights, the broad definition of intellectual property rights under Finnish law encompasses their protection under the Unfair Business Practices Act.

FR (France): The only specific trade secrets legislation in French law is that protecting "manufacturing secrets" in the Intellectual Property Code. Other provisions of civil law (tort law) protect trade secrets more generally. The Labour Code also provides criminal liability for trade secret violations by employees or former employees. When parties are bound by a contractual obligation not to disclose secret information, an action lies for breach of contract.

HU (Hungary): Hungarian law provides specific provisions on the protection of trade secrets. The Civil Code and Unfair Competition Act in particular provide specific protection. Provisions also exist in the Labour Code and in various financial/banking laws.

IE (Ireland): There is no specific legislation in Ireland directed to the protection of trade secrets. However, proceedings may be brought under laws relating to breach of confidence, data protection, criminal damage and specific sectorial pieces of legislation. As in England, Irish law has the equitable principle that a person who has received information in confidence cannot take unfair advantage of it. Generally, Irish law imposes a duty of confidentiality in both non-employment cases and employment cases. In both situations, there must be an obligation of confidence and once it is established that such an obligation exists then the person to whom the information is given has a duty to act in good faith and only use the information for the intended purpose. Again, as in England, an obligation to keep information confidential may either be imposed by contract; implied because of the circumstances of the disclosure or implied because of the special relationship between the parties.

IT (Italy): Specific provisions on the protection of trade secrets are contained in the Italian Code of Industrial Property (IPC). Secret information may only be protected if the requirements set out in the IPC are met. There are also general tortious obligations and unfair

competition provisions in the Civil Code which can be employed to compensate for trade secrets misuse.

LT (Lithuania): Lithuanian legislation provides specific provisions on the protection of trade secrets, most importantly in the Civil Code, the Law on Competition, the Labour Code and the Criminal Code. Under the Civil Code, anyone unlawfully acquiring a commercial secret is liable to compensate the owner for the damage caused. There are also express provisions in the Labour Code regarding disclosure by employees who disclose a commercial secret in breach of their employment contract.

LU (Luxembourg): There are no specific legal provisions protecting trade secrets in Luxembourg. However, trade secrets can be protected by unfair competition law, criminal law, tort law and contractual law.

LV (Latvia): Latvia has a number of pieces of legislation which provide specific provisions on the protection of commercial secrets. The Commercial Law is the main Act regulating commercial activities. It defines "commercial secrets" and provides express protection for them. The Labour Law also includes provisions regarding use of commercial secrets by employees. Latvia also has an Unfair Competition Act which expressly provides that the acquisition, use or disclosure of commercial secrets of another competitor without their consent is a form of unfair competition.

MT (Malta): There is no specific legislation on the protection of trade secrets in Malta. Trade secrets may be protected contractually, by express or implied terms, and, an employee is presumed to be under an obligation not to disclose confidential information. If no contract exists there will be no civil law right to protect a trade secret.

NL (Netherlands): There are no specific provisions on the protection of trade secrets in Dutch legislation. In the Netherlands, the protection of trade secrets is based on the general principle of tort law i.e. an unlawful act. In 1919, the Dutch Supreme Court held that the provision in the Dutch Civil Code on unlawful acts could be used to secure protection against trade secret infringement. Contract law also provides some protection in contractual relationships if there are confidentiality obligations in the contract.

PL (Poland): There are specific provisions on the protection of trade secrets in Polish legislation, notably in the Unfair Competition Act. A number of other Acts mention trade secrets, for example, the Civil Code, the Labour Code, the Act on Competition and Consumer Protection, the Code of Commercial Companies and Partnerships etc. The Labour Code includes express provisions requiring employees to maintain the confidentiality of information the disclosure of which could cause damage to their employer.

PT (Portugal): The Portuguese Industrial Property Code has specific provisions relating to the protection of trade secrets. The Industrial Property Code is directed towards unlawful acts against competitors. A violation is punished, not as a crime, but as a misdemeanour. The Labour Code also contains provisions which stipulate that an employee may not disclose information, while employed, relating to his employer's organisation, production methods and company business.

RO (Romania): There is specific legislation in Romania on the protection of trade secrets. Provisions regulating protection of trade secrets have been included in the Law for the Prevention of Unfair Competition ("Law on Unfair Competition") and specify that the unfair use of a competitor's trade secrets is regarded as contrary to honest commercial practices. Trade.

SE (Sweden): Sweden is the only country in the EU to have an Act specifically protecting trade secrets. The Act provides a definition of trade secrets, penalises trade secret espionage and contains provisions on civil liability.

SI (Slovenia): Trade secrets are specifically protected in Slovenia by a number of pieces of legislation, in particular, the Companies Act, the Employment Relationship Act, the Protection of Competition Act, the Penal Code and the Code of Obligations.

SK (Slovakia): Civil protection of trade secrets in the Slovak Republic is regulated by the Commercial Code. The relevant fields of protection are civil law, commercial law, intellectual property law, non-contractual liability and unfair competition law.

UK (United Kingdom): There is no legislation providing specific protection for trade secrets. Trade secrets are protected by contract and/or by the law of equity.

### ***(A.2) Differences in the scope of protection: the trade secret and the misappropriation***

The absence of homogenous pieces of legislation in this area implies that there is no uniform understanding of what a trade secret is and what misappropriation is:

- In Italy, Portugal and Sweden, there is a specific statutory definition of trade secrets in the applicable legislation.
- A statutory definition of trade secrets is also available in the unfair competition provisions of the Czech Republic, Lithuania and the Slovak Republic.
- In the Czech Republic, Greece, the Netherlands and Spain, the TRIPS definition has been expressly acknowledged and adopted<sup>5</sup>.
- In some cases, definitions of trade secrets can be found in other pieces of laws, for other purposes (e.g. Freedom of Information Act in the UK).

In principle information which meets the requirements of Article 39(2) of the TRIPS<sup>6</sup> would be protectable in all EU Member States. Also, no restrictions seem to exist regarding the type of information which could be protectable and in all EU Member States both technical (e.g. know-how etc.) and commercial secrets (e.g. business strategies etc.). However, the absence of specific definition results in risk of inconsistent interpretation as to what is protectable as trade secrets and consequently, a different protection depending on the type of action initiated by the trade secret owner<sup>7</sup>. Also, differences in courts practices are reported<sup>8</sup>.

Concerning the question of misappropriation, the main divergences relate to the situation of the third party who obtain the secret information in good faith<sup>9</sup>: see below on remedies.

### ***(A3) Differences in the remedies: injunctions, destruction of goods and compensation for prejudice suffered***

#### ***(i) General***

---

<sup>5</sup> Cf. Baker & McKenzie study.

<sup>6</sup> In essence, information which is secret, has commercial value (because it is secret) and has been subject to reasonable steps to keep it secret.

<sup>7</sup> Baker & McKenzie study.

<sup>8</sup> Baker & McKenzie study.

<sup>9</sup> To be sure, no Member State grants any action against a third party who autonomously developed the same information.

The remedies available in civil/commercial law proceedings for the misappropriation of trade secrets do vary and appear to depend on the origin of the action (e.g. based on tort, contract law, unfair competition law etc.): see Table 2 for a summary view.



**Table 2 – Available civil remedies**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Injunctions (cease and desist orders: ordinary action)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Injunctions (cease and desist orders: interim relief)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Return/destruction of trade secrets / goods produced using misappropriated trade secrets: ordinary action	✓	✓			✓	✓	✓			✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Return/destruction of trade secrets / goods produced using misappropriated trade secrets: interim relief	✓	✓				✓				✓		✓	✓	✓	✓		✓		✓								✓
Seizure of trade secrets / goods produced using misappropriated trade secrets: ordinary action		✓			✓		✓	✓	✓			✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Seizure of trade secrets / goods produced using misappropriated trade secrets: interim relief		✓					✓	✓	✓			✓	✓		✓		✓		✓	✓	✓					✓	✓
Withdrawal from the market of goods produced using misappropriated trade secrets: ordinary action		✓			✓		✓	✓	✓			✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Withdrawal from the market of goods produced using misappropriated trade secrets: interim relief		✓			✓			✓	✓			✓	✓		✓		✓		✓		✓	✓	✓				✓
Damages	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Publication of decisions: ordinary action		✓	✓				✓			✓	✓	✓	✓		✓		✓		✓	✓	✓		✓			✓	✓
Publication of decisions: interim relief		✓										✓			✓												
Restraint measures (e.g. penalty for future breach of the Court's order): ordinary action	✓	✓	✓	✓				✓		✓	✓				✓	✓	✓		✓					✓			
Restraint measures (e.g. penalty for future breach of the Court's order): interim relief		✓		✓				✓			✓				✓		✓							✓			

The above remedies are, in general, all cumulatively available to the trade secret owner, with few exceptions. For example, in Belgium, damages are available but not for cease-and-desist claims brought under the Unfair Competition Act (in the form of expedite action). In Bulgaria, it appears that final injunctions are not available (at least cease-and-desist orders in the strict sense of the word) with damages being the usual final remedy. In Latvia, although potentially available, it is not clear which remedies can effectively be used as there is no case law as to whether remedies provided in the Civil Procedure Code for intellectual property rights apply also to trade secrets (trade secrets are not expressly included among the definition of intellectual property). In Italy damages may only be awarded in ordinary proceedings. In Luxembourg, while injunctions are granted by the President of the Commercial Court, damage claims shall be brought before the District Courts.

*(ii) Injunctions (cease and desist orders)*

In general, injunctions (cease and desist orders) are available in all EU Member States. In all Member States, injunctions (i.e. cease and desist orders) are usually available also as interim

relief remedy (i.e. during preliminary and summary proceedings where the claimant's requests are summarily examined by the Court and measures are granted within a very short time limit).

Therefore, there is civil law redress in order to block the commercialisation of goods (or services) which have been manufactured (or designed) using misappropriated trade secrets (so-called "resulting goods/services"). However, this redress varies from Member State to Member State and there is no guarantee that the "resulting goods/services" will be stopped everywhere in the EU. Cease and desist orders against the use of misappropriated trade secrets by third parties (i.e. beyond a contractual relationship) are not always available:

- (i) when trade secrets are protected under unfair competition rules, the trade secret owner needs to sue a competitor but cannot sue a person having the secret with a view to sell it to another third party or to exploit it for other purposes than competing with the original owner of the secret;
- (ii) solutions diverge regarding the possibility to obtain a cease and desist order against negligent third parties or third parties who obtained the misappropriated trade secrets in good faith but before the trade secrets had reached the public domain. In some EU Member States, remedies are potentially available regardless of the recipient's good or bad faith (Austria<sup>10</sup>, Czech Republic, Denmark, Estonia, Finland, Germany, Ireland, Latvia, Lithuania, and Portugal) and injunctions can be obtained also against a third party who obtained the secret in good faith – however, the third party is likely not to be held liable for damages, unless the use of the secret information continues even after the recipient has been informed of the confidential nature of the information. In others, this is not possible<sup>11</sup>; and
- (iii) cease and desist orders may be limited in time even if the trade secret has not yet reached the public domain. Belgium<sup>12</sup>, Cyprus, Denmark<sup>13</sup>, Greece, The Netherlands<sup>14</sup>, Poland and Slovenia, which do not allow unlimited injunctions. In Common Law countries, injunctions are equitable remedies and, as such, courts are free to determine terms and duration of the restrictions.

Concerning the situation of employees, the Baker & McKenzie study finds that though in general, whilst employed, employees have a (statutory) duty of loyalty (including non-disclosure and non-compete obligations) towards the employer, a common practice in most jurisdictions is to provide for non-use and non-disclosure, as well as non-compete clauses in contracts of employment. However, the position differs as to what can be done in relation to an ex-employee who uses or discloses secrets after leaving employment. The balance between the interests of the employer and the employee is indeed assessed differently in the relevant

---

<sup>10</sup> In Austria, damage claims are also available in cases of default; accordingly damage compensation could be awarded also in case of the third party's slight negligence.

<sup>11</sup> For instance, in the United Kingdom a duty of confidentiality may be implied by the circumstances (the duty of confidentiality is easy to identify in case of an employment contract or a non-disclosure agreement, but it could prove to be very difficult to demonstrate where a person has obtained the confidential information in absence of any relationship between the owner and the recipient), but a person who innocently receives a confidential information will not be under a duty of confidentiality until he is made aware the information is confidential.

<sup>12</sup> In Belgium, courts refuse to grant final injunctions against future trade secrets misappropriation because, contrary to intellectual property rights, trade secret protection can potentially last forever and thus courts are not willing to grant the owner of a trade secret a broader protection than most intellectual property right holders.

<sup>13</sup> In Denmark, although depending on a case by case analysis, final injunctions are usually granted for a period of two to three years from termination of the cooperative relationship.

<sup>14</sup> In Greece and The Netherlands, injunctions are considered temporary in nature.

countries. In general, post-employment, an employee cannot be prevented from using the skill and knowledge gained during the employment, provided that said knowledge does not consist of trade secrets or confidential information that the employee wilfully memorised or (mis)appropriated with the purpose to misuse them after termination of the employment relationship<sup>15</sup>.

*(iii) Destruction of the goods produced using the misappropriate trade secrets or the restitution of the misappropriated information*

Compared to injunctions, other measures such as the destruction of the goods produced using the misappropriate trade secrets or the restitution of the misappropriated information) are not available everywhere and are available in interim proceedings in certain countries only (see [Table A6.2](#)). Since resulting goods are not always destroyed, there is no guarantee for the trade secret owner that such goods will no reappear in the market.

*(iv) Damages*

Compensation for the prejudice suffered from the misappropriation of a trade secret is available in all jurisdictions<sup>16</sup>. Damages claims are mainly based on tort or contract and only in a few cases specific provisions on damages are included in either the unfair competition laws (see for example Spain) or in the specific provisions applying to trade secret misappropriation ( Italy and Sweden).

Damages based on tort cover both accruing damages (“*damnum emergens*”) and loss of profits (“*lucrum cessans*”). Loss of profits, however, is in most cases very difficult to prove, since the misappropriated information is an intangible asset<sup>17</sup>. This helps explaining the often low compensation obtained<sup>18</sup>. A claim for unjust enrichment is available in some countries

---

<sup>15</sup> In Denmark (and similarly in Poland), the statutory non-disclosure and non-use obligations survive termination of the employment contract for a period of three years. In Italy, as in many other European countries, non-compete agreements (or clauses) are commonly used to prevent use or disclosure after the contract of employment ceases, albeit offering more limited restrictions than those which exist during the period of employment (to be enforceable non-compete clauses must generally be limited in time and space, identify the activities which the former employee cannot engage in and provide for a monetary compensation). In Sweden, damages for breach of confidentiality obligations after termination of employment are only available where there are “extraordinary circumstances”. In Ireland and the United Kingdom there is a distinction between general (low grade) confidential information that the employee is not entitled to disclose whilst employed but can use and disclose thereafter and “real trade secrets” which he cannot disclose or use without authority at any time. The distinction depends on a number of factors including whether the employer impressed the secrecy of the relevant information upon the employee; and whether the “secret” can be readily isolated from other information which the employee is free to use.

<sup>16</sup> In Bulgaria, damage compensation is the sole final remedy available to the owner of a trade secret.

<sup>17</sup> According to Baker & McKenzie, there are often evidentiary problems in proving the loss incurred by the owner of a trade secret. In some countries, damages are awarded only if the claimant is able to demonstrate that he had suffered some loss. Other countries allow courts to award damages on an equitable basis - taking into account all the circumstances of the case - if the claimant has not been able to provide sufficient evidence on the amount of damages

<sup>18</sup> According to Baker & McKenzie, damages vary on a case-by-case basis but the average figures collected during the study “seem not to be particularly encouraging”. This study mentions a few cases in Italy and Sweden, where courts awarded high amounts of damages: in Italy, in two cases of trade secrets infringement the Court of Milan awarded damages for EUR 1,100,000.00 and EUR 10,000,000.00, respectively. In Sweden, courts have awarded damages for SEK 7/10,000,000.00 and 48,000,000.00. However, the study reports that these appear to be exceptional cases. In the Force India Formula One Team Ltd. case, only €25000 were awarded by a UK court to the claimant. The plaintiff had claimed compensation in excess of £13 million (which was based on the assumption that it succeeded in the entirety of its claims for breach of confidence, which it did not). However, the judge did not accept the plaintiff argument that the relevant information was of great

only, such as among others, Belgium, Estonia, Finland and Spain (for further details please see [Table 3](#) below). In some other countries (for example, Austria, Germany, Italy, Ireland, Lithuania, Poland, Sweden and the United Kingdom) the claimant has the right to claim the account of profits obtained by the infringer from its wrongdoing. In most of the cases, however, the account of profits is alternative to the loss of profits or is considered a criterion to calculate said loss. In Italy, the owner of trade secrets may claim the restitution of the infringer's profit in addition to the loss of profits to the extent that the infringer's profits exceed the claimant's loss. In Greece, account of profits and unjust enrichment are alternative ways to calculate the loss of profits. Similarly in The Netherlands loss or profits excludes account of profits.

**Table 3 – Available damages options**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Accruing damage ( <i>damnum emergens</i> )	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Loss of revenues ( <i>lucrum cessans</i> )	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Moral damages			✓					✓					✓		✓					✓		✓	✓			✓	
Punitive damages														✓													✓
Other monetary compensation					✓																✓						
Account of profits	✓			✓	✓	✓		✓	✓		✓		✓	✓	✓	✓		✓		✓	✓			✓			✓
Fair royalty	✓					✓	✓		✓				✓		✓					✓							✓
Unjust enrichment		✓			✓			✓	✓	✓	✓								✓		✓	✓	✓		✓	✓	
<i>Ex aequo et bono</i> global account		✓	✓					✓			✓		✓		✓	✓	✓		✓	✓		✓	✓				
Cumulation of these options		✓	✓		✓		✓		✓	✓					✓	✓		✓	✓	✓	✓			✓	✓	✓	

If damages are claimed on contract, liquidated damages (if provided by the agreement) can also be claimed in addition to damages. Contractual liability, however, is often limited to the damages which were foreseeable at the time of conclusion of the contract.

The available options are in principle all cumulative (exceptions are Austria, Cyprus, Estonia, Finland, France, Germany, Hungary, Ireland, Luxembourg, Portugal, Romania and United Kingdom) provided that the total amount awarded by the court does not exceed the actual claimant's loss. Furthermore, in countries where courts are allowed to award an "*ex aequo et bono*" global amount in cases where damages cannot be alternatively calculated, such criteria are of course to be considered as alternative to all the other available damage options.

Since most of the EU Member States do not have specific criteria for the calculation of damages, they apply the general criteria of tort liability (i.e., *damnum emergens* and *lucrum cessans*). The license analogy has been indicated as a possible criterion for the calculation of damages<sup>19</sup>, among EU Member States in Austria, Denmark, Germany, Greece, Hungary, Italy, The Netherlands and United Kingdom.

## (B) CRIMINAL LAW

### (B.1) Criminal law protection in national law: summary

value and considered that the misuse of the information was limited in nature, purpose and benefit. As a result, the judge considered that €25000 was the figure the parties would have negotiated had they been in the position of a willing licensor and willing licensee acting reasonable as at the date of the breach of confidence.

<sup>19</sup> This method of calculation is used regarding infringements of intellectual property rights, pursuant to Article 13(1)(b) of Directive 2004/48/EC. This Article provides for the rules on abstract calculation of damages (i.e. calculated on the basis of royalties which could have been due should a licence have existed) as an alternative to the general *damnum emergens* and *lucrum cessans* criteria.

Criminal protection of trade secrets against misappropriation differs from Member State to Member State on several levels, although almost all of them have provisions in this respect. Since there is a lack of a common/shared definition of the scope of trade secrets, the actual extent of the protection provided by states may vary depending on the aims pursued by the provisions implemented for this purpose.

Only a few Member states (i.e., Bulgaria, Ireland, Malta and U.K.) have not established any specific criminal framework with respect to trade secrets violations. However, even in those Member States, the conduct of the infringer may be punished under other related criminal offences (see below). In some cases, where no specific criminal provision has been implemented, penal sanctions of trade secrets misappropriation apply under unfair competition laws or commercial laws. Sweden is the only EU Member state that has implemented a specific law on trade secrets (the Swedish Act on the Protection of Trade Secrets), even though some relevant provisions are also contained in the Criminal Code<sup>20</sup>. Table 4 below summarises the criminal provisions in force:

Table 4 – Criminal provisions applying to trade secrets misappropriation <sup>21</sup>																												
	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK	
Criminal code	✓	✓		✓		✓	✓	✓	✓	✓		✓	✓		✓	✓	✓	✓		✓		✓	✓	✓	✓	✓	✓	
Unfair competition / commercial law	✓			✓	✓	✓	✓		✓												✓		✓					
Specific law on trade secrets																								✓				

## **(B.2) Differences in the conducts considered as crimes**

### **(i) Unauthorised disclosure/use of trade secrets**

Many of the countries seem to limit the scope of trade secrets to the information that a company has a reasonable and objective interest to keep confidential, in accordance with an objective criterion (e.g., Austria, Belgium, France, Germany, Hungary, Italy, Lithuania, Luxembourg, Netherlands, Slovakia, Spain, Sweden). Nonetheless, in some cases the relevant protection is afforded to any information having economic value that the owner deems it opportune for his benefit to keep secret according to a subjective criterion and that are subject to reasonable measures for protection of confidentiality (e.g., this broader interpretation seems to be prevailing in Czech Republic, Finland, Greece, Poland, Romania and Slovenia).

- In Austria the offender to be held criminally liable for trade secrets violations must have acted at least with conditional intent. In Belgium, Estonia, Finland, France the conduct may be punished even if the offender acted with negligence.
- Cyprus does not establish any specific requirement that the offender must meet to be charged with criminal liability for trade secret violations. Nor is there any stated obligation on the claimant to keep information confidential.
- In the Czech Republic the offender must act deliberately to commit the offence. As the relevant conduct is defined as an act of unfair competition, the offender must qualify as a competitor or someone participating in the competitive process. The concept of competition has nevertheless been construed very broadly, including even indirect or potential competitors.

<sup>20</sup> In particular, the Act on the Swedish Protection of Trade Secrets establishes two different offences: business espionage and the unauthorized dealing with trade secrets. Other complimentary or more general offences, such as, for instance, unauthorized access to computer systems or breach of faith against principal are regulated under the Criminal Code.

<sup>21</sup> Baker & McKenzie study.

- In Denmark the offences provided for under the Criminal Code require intent. Only upon certain circumstances if the employee causes a substantial risk of dissemination of confidential information by negligence he or she may be charged with criminal liability pursuant to Section 19 of the Marketing Practices Act. without having acted with intent.
- Germany requires that the infringer acts with intent and, specifically, for the purpose of competition, for personal gain, for benefit of a third party or causing damage to the owner of the secret.
- In Greece the offender must act (with intent) for purpose of competition, that means that two criteria have to be met: (i) the conduct of the offender must be suitable to serve the purpose of competition; (ii) he or she must act with the “intention of competition”, i.e. enhance his or third parties’ competitiveness.
- As to Hungary and Italy, the offender may be punished only if he or she acts with intent.
- In Latvia the employer is obliged to identify in writing the information considered to be commercial secrets. In any case, the offender requires the offender to have acted for use or disclosure by himself or another person, therefore intent is required for the offence to occur.
- Lithuania requires that the offender, in case of business espionage, acted with the intent to unlawfully obtain a trade secret, whereas, in the case of violation of trade secrets, with the intent to get a financial gain or to injure the owner by the disclosure to third parties or the use of the information.

As almost all EU Member states require that the offender acted with intent, it emerges that whoever commits a trade secrets infringement must have clearly the knowledge that the business information constituted trade secrets, even if there is no express obligation to keep such information confidential.

- In Luxembourg, Netherlands and Portugal the offender must act with the intent to reach a competitive advantage or to cause harm to the owner.
- Also Poland requires intent, as the offender must breach an obligation of confidentiality that must be prior established by the owner of the secret, either directly or indirectly.
- Under Romanian and Slovak law the offender must act with intent, but no specific purpose is required.
- The same applies in Slovenia, where if the conduct reaches certain outcome, the offender may be charged with the more severe correspondent penalties.
- Spain also requires intent, even if the purposes to be pursued vary depending on the type of offence considered (for instance, commercial advantage).
- The Swedish Act on the Protection of Trade Secret does not pose any requirement as to the purpose that the offender acts for. It only requires that he acted wilfully and without authorization.

#### *(ii) Related offences*

In Belgium a person who commits the offence under Section 309 of Criminal Code (unauthorized disclosure of trade secrets) may also be charged with theft or misappropriation (provided that he qualifies as an employee with the company). Similarly, Section 491 applies

when a person is entrusted as a data processor/handler manufacturing secrets that are physically stored breaches his duty of confidence.

In Bulgaria, for instance, the offence of business bribery is punishable and applicable to, any individual who discloses to third parties information that he knows in return for something.

In France there is a wide range of crimes that may arise in connection to trade secrets violations:

- First, the offence of theft may occur when the conduct at stake consists in the fraudulent appropriation of third parties' data carriers containing confidential information. Such an offence has been found by the Court of cassation to apply even in connection to disclosure of trade secrets. Theft is punished by imprisonment up to three years and a fine of Euro 45,000.00.
- Additionally, the offence of breach of trust may be committed where an individual with the company misappropriates documents containing confidential information entrusted to them for temporary use. In such a case, the offender shall be punished by imprisonment up to three years or a fine of Euro 375,000.00.
- Also, other provisions of the Criminal Code punish the act of supplying secret information to foreign powers by imprisonment up to fifteen years and a fine of Euro 225,000.00.

In Germany cases of industrial espionage may result in theft or misappropriation.

In Greece the infringement of trade secret may constitute, among other offences, a breach of trust under Section 390 of the Criminal Code. In such a case, the offender shall be punished by imprisonment up to ten years and a fine up to Euro 15,000.00.

Depending on the circumstances, violations of trade secrets may result, further to civil lawsuits, in a number of offences, including but not limited to insider trading, unauthorized access to computer systems and a breach of privacy.

As to Italy, the conduct of the offender who commits an unauthorized use or disclosure of trade secrets may also constitute theft or misappropriation.

In Latvia acts of unauthorized disclosure or acquisition of trade secrets may constitute unfair competition practices where repeated within a one-year period and, thus, result in a punishment by imprisonment of up to two years and a fine, in addition to disqualification penalties.

Violations of trade secrets may constitute fraud or bribery in Lithuania or theft in Luxembourg. In Netherlands the conducts may also result in the theft of secret documents or hacking of computer systems. In Portugal the related offences include computer and communications fraud. Slovakia, in addition to breach of trade secrets, criminalizes the misuse of participation in economic competition through unfair acts.

In Slovenia the same act may be punished under the crime of "disclosure of and unauthorized access to trade secrets" as well as, for instance, the offence of abuse of insider information. Spain provides an extensive regulation of trade secrets infringements: however, pursuant to Section 278.3 of the Criminal Code the specific provisions apply without prejudice to the penalties that may arise for appropriating or destroying the computer media, i.e. for the offences of theft or misappropriation.

In Sweden, further to the offences provided for under the act on the Protection of Trade Secrets, other criminal provisions may apply, including unauthorized access to computer

systems, unlawful dispossession, unlawful use, espionage, unlawful dealing with secret information and negligent dealing with confidential information.

Offences in any way related to trade secrets violations have significant importance in the legal systems that do not establish any specific provision in this respect:

- In Bulgaria violations of trade secrets may be punished only indirectly. The relevant offences in this respect include the disclosure of service/office secrets, the business bribe and computer crimes.
- Under Irish law, for instance, trade secrets infringements may result in: (i) disclosure of personal data obtained without authority; (ii) unauthorised accessing of data; (iii) unlawful use of a computer; (iv) theft or (v) criminal infringements of intellectual property rights.
- Under Maltese criminal law, in the absence of provisions specifically concerning trade secrets, one could be charged with misappropriation and fraudulent gains as a result of his conduct.
- In the U.K. the criminal provisions that may apply in connection to trade secrets infringement cases include theft, fraud, conspiracy to defraud as well as, upon certain circumstances, some of the offences provided for under the Computer Misuse Act (such as unauthorized access to information contained on a computer) and the Data Protection Act (although it is very unlikely that personal data qualify as trade secrets).

### (iii) Qualified offences

Certain Member States also establish qualified offences when the revelation or use of confidential information is committed by a person acting in a particular capacity (e.g., as civil servant, public official, or as person handling confidential information by reason of his job, e.g. lawyers, officers). Please note that this does not mean that for each of the offences a specific provision is established. Separate provisions may have been implemented (e.g. Italy) or, like in Estonia, the same provision may apply to professional and official secrets, also covering trade secrets. See [Table 5](#):

**Table 5 – Qualified offences<sup>22</sup>**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Breach of professional secrecy	✓	✓		✓				✓	✓						✓				✓	✓		✓	✓	✓	✓	✓	✓
Breach of official secret	✓		✓	✓				✓	✓		✓				✓							✓	✓				
Other breach of confidence									✓				✓														
Separate provisions	Y	Y	N	N	N/A		N/A	N	N		Y	N		Y	N				N/A	N		Y	Y			N	

### (iv) Threshold for the applicability of criminal penalties

In the Czech Republic only violations resulting in a damage of at least Euro 2,000.00 may give rise to criminal liability. The offender must cause harm to a competitor or a consumer equivalent to such an amount or provide someone else than the owner of the secret with a benefit of the same amount. The offender does not necessarily need to be a legal person or an enterprise.

A *de minimis* threshold applies in Lithuania, where for the offender to be prosecuted it is required that the conduct caused a damage of at least EUR 5,648.00.



Something like a *de minimis* threshold is established in Poland, where the conduct must have caused substantial damage to the owner, although no quantification of this concept is provided for in the law.

Slovakia establishes that for the offender to be prosecuted a significant damage (more than EUR 26,600.00) must be caused by his conduct to another competitor. It also provides for a more severe penalty in cases where the conduct causes a large scale damage (over EUR 133,000.00).

Also under Estonian and Finnish criminal law a general safe harbor clause applies, preventing prosecution in case the offence is found to be of minor harm.

In Austria the offender will not be prosecuted if his conduct is justified by a compelling public or private interest.

No safe harbor seems to exist in Latvia and Sweden. In Cyprus disclosure of trade secrets is allowed, for instance, when protection of health and safety of citizens is affected, i.e. where compelling public interests are at stake or to prove the violations of statutory provisions.

Similarly, no safe harbor or *de minimis* threshold applies in Denmark, Finland, Italy, Luxembourg, Slovenia. Germany does not provide for any safe harbor; however, disclosure of trade secrets is justified when committed to avert an imminent danger to life, limb, freedom, honour, property or other prevailing legal interests. In Greece trade secrets are not protected in case a witness is examined to represent certain circumstances before the Court, excluding state secrets. In Hungary Section 300(2) of Criminal Code expressly sets forth some safe harbors that justify infringement of trade secrets. These clauses include:

- (i) fulfilment of duties prescribed in a separate act governing the publication of information and information to be disclosed in the public interest;
- (ii) fulfilment of duties subject to statutory reporting obligations, even in the case the report was filed in good faith and proved to be unfounded.

In the Netherlands a specific provision sets out an exemption for those who disclosed in good faith a trade secret assuming that the disclosure was in the public interest. Portugal and Romania consider the consent of the owner to the disclosure of a secret as a safe harbor clause. In addition to that, Romanian law permits the disclosure of trade secrets where compelling public interests are at stake. Spain does not consider information about illegal activities carried out by the owner to be a trade secret: therefore, its revelation would not determine any prosecution.

Generally speaking, the risk of dissemination of confidential information does not amount to a criminal offence (except for Slovakia, Slovenia). The conduct carried out by the infringer must result in an actual violation of the interest protected under the relevant provisions. In contrast, most legal systems (including Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Italy, Latvia, Lithuania, Slovakia, Slovenia) provide criminal protection against the intent to commit a trade secret violation. The acts carried out with the purpose of disclosing or using confidential business information which reach a certain threshold in the realisation of the offence are likely to trigger criminal liability.

### ***(B.3) Differences in the penalties***

The conducts which normally give rise to violations of trade secrets include the access to confidential information, the use or the disclosure thereof or the illicit acquisition for exploitation by the offender or third parties. These conducts are generally punished regardless

of the fact that the offender qualifies as a competitor and may be committed either by (past) employees of the company or by external persons (such as consultants, contractors, agents).

It is quite frequent, however, that the violation of trade secrets committed by an employee of the company owning the confidential business information results in a more severe punishment than that provided for the same offence in other cases (i.e., in Belgium, Germany, Greece and Spain).

Table 6 below provides a summary of the main conducts concerning trade secrets violation and the related punishment provided for under the legal systems.

**Table 6 – Criminal penalties applying to trade secrets misappropriation<sup>23</sup>**

Country	Offender	Conduct	Penalties
Austria	Whoever	Disclosure or exploitation of trade or business secrets	Up to six months imprisonment; up to one year if the conduct is committed with the purpose to obtain a pecuniary advantage or to cause harm to the owner or monetary penalties
		Spying out trade or business secrets for their exploitation by somebody else or disclosure	Up to two years imprisonment OR monetary penalties
		Spying out trade or business secrets for their exploitation abroad	Up to three years imprisonment AND monetary penalties
Belgium	Whoever	Communicating in bad faith manufacturing secrets appropriated during the (past) employment with the owner	From three months up to three years imprisonment AND monetary fine from Euro 50 to 2,000.00
Bulgaria		There is no specific criminal provision concerning violation of trade secrets. However, depending on the characteristics of the conduct, the offender may be charged with more general offences, such as business bribe or computer crimes	
Cyprus	Whoever	Disclosure of trade secrets	Imprisonment up to one year OR monetary fine up to Euro 1,275.00
		Disclosure of information protected by professional secrecy involving trade secrets	Imprisonment up to six months AND/OR monetary fine up to Euro 1,700.00
Czech Republic	Whoever	Acts of unfair competition infringing trade secrets and causing damage in or in excess of Euro 2,000.00 to other competitors/consumers or providing someone with unjustified benefit in the same or greater amount	Monetary fine up to Euro 1.5 Million*
Denmark	Whoever	Unauthorized misuse or appropriation of trade secrets	Imprisonment up to 1 year and 6 months OR monetary fine
		Serious violations such as appropriation of trade secrets in a contract of service or in the performance of assignments	Imprisonment up to six years
Estonia	Whoever	Unauthorized disclosure or use of business secret learned by reason of the professional or official duties with the purpose of causing damage	Imprisonment up to one year OR monetary fine
Finland	Whoever	Disclosure or use of trade secrets known by reason of the employment, position or other lawful activities to obtain financial benefit or to injure the owner	Imprisonment up to two years OR monetary fine
		Misuse of trade secrets obtained or revealed through an unlawful act	Imprisonment up to two years OR monetary fine
		Business espionage: Unlawfully obtaining information regarding trade secrets	Imprisonment up to two years OR monetary fine
France	Whoever	Revelation of manufacturing secrets	Imprisonment up to two years AND monetary fine of Euro 30,000.00
		Theft (for instance, of carriers or materials containing trade secrets)	Imprisonment up to three years AND monetary fine of Euro 45,000.00
Germany	Employees	Unauthorized communication of trade or business secrets that the offender was granted access to for the purpose of obtaining financial advantage or injuring the owner	Imprisonment up to three years OR monetary fine
	Whoever	Unauthorized acquiring or securing trade or business secrets or using thereof	Imprisonment up to three years OR monetary fine. Imprisonment up to five years if aggravating circumstances occur
Greece	Whoever	Copying, printing, using, disclosing or in any way	Imprisonment from three months up to

		violating data or computer programs constituting secrets of an enterprise	one year. Imprisonment from one year to five years if the offender is in the service of the owner and the secrets are of great financial significance
	Employees	Unauthorized communication to third parties of secrets that the offender has known by reason of his employment to obtain financial advantage or to cause a damage to the owner; Unauthorized use of the information so obtained	Imprisonment up to six months AND monetary fine up to Euro 8.80
Hungary	Whoever	Making available to unauthorized persons secrets for financial advantage or to cause damage to others; Using the secrets so obtained	Imprisonment up to three years
Ireland	Not applicable		
Italy	Whoever	Disclosure or use of any information concerning scientific discoveries or inventions or industrial applications that is intended to remain secret known by the offender by reason of his status, function, job or art, to obtain a profit	Imprisonment up to two years
Latvia	Whoever	Revelation of non-disclosable information other than a state secret; Unauthorized acquisition and disclosure of commercial secrets	Imprisonment up to five years OR monetary fine
Lithuania	Whoever	Unlawful acquisition of commercial secrets or communication to third persons; Disclosure of information that the offender was entrusted with by reason of his employment	Imprisonment up to two years AND/OR disqualification penalties
Luxembourg	Employees	Use or disclosure, during the employment or within two years after its expiration, trade or manufacturing secrets known by reason of the job to obtain financial advantage or to cause damage to the owner	Imprisonment from three months to three years AND monetary fine from Euro 251 to 12,500.00
Malta	Not applicable		
Netherlands	Employee	Intentional disclosure of confidential information that may harm the owner	Imprisonment up to six months AND/OR monetary fine up to Euro 19,500.00
Poland	Whoever	Disclosure or exploitation of trade secret in breach of confidential duties that causes substantial damage to the owner; Use of information illegally acquired or disclosure to third persons	Imprisonment from one month to two years AND monetary fine up to Euro 260,000.00*
Portugal	Whoever	Use or disclosure to third parties of secrets that the offender knows by reason of his status, job, profession or art	Imprisonment up to one year OR monetary fine
Romania	Whoever	Disclosure, acquisition or use of trade secrets without the consent of the owner, as a result of an action of commercial or industrial espionage	Imprisonment from six months up to two years OR monetary fine from Euro 570 to 5,000.00*
		Disclosure of data or information not intended to be publicly known by a person who knows it by reason of his employment, provided that the offence is likely to cause damages	Imprisonment from two up to seven years; Imprisonment from six months to five years if the disclosure is made by another person
Slovakia	Whoever	Spying out trade secrets with the intention to disclose them to unauthorized persons	Imprisonment from six months up to three years; Imprisonment from seven to twelve years if aggravating circumstances occur
Slovenia	Whoever	Disclosure of trade secrets; Providing unauthorized third parties with access to trade secrets; Collection of trade secrets with the purpose of delivering them to unauthorized persons; Unlawful obtaining of trade secrets with the purpose of delivering them to unauthorized persons	Imprisonment up to three years; Imprisonment up to five years if the information is of particular importance
Spain	Whoever	Acquiring data, documents, media and other objects to discover trade secrets; Disclosure, revelation or communication to third parties of the discovered information	Imprisonment from two up to four years AND monetary fine; Imprisonment from three to five years AND monetary fine in case the secrets are disclosed
		Diffusion, disclosure or communication of trade secrets in breach of duties of confidentiality	Imprisonment from two up to four years AND monetary fine, in case the information is disclosed in breach of confidentiality
Sweden	Whoever	Unauthorized access of trade secrets as business espionage	Imprisonment up to two years OR monetary fine; Imprisonment up to six years in case of information of significant importance
		Acquiring trade secrets knowing that the person who made it available accessed the trade secret through acts of business espionage	Imprisonment up to two years OR monetary fine; Imprisonment up to four years in case of information of significant importance

U.K.	Not applicable	
------	----------------	--

\* Monetary penalties are expressed in local currency and converted to Euro for the reader's convenience

Generally, punishment of the offender is by imprisonment, even though he or she may also be charged, either in addition to that or alternatively, with monetary penalties: see Table 7 with penalties that shall apply for the main offence (for instance, unauthorized disclosure/use of trade secrets).

**Table 7 – Penalties<sup>24</sup>**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Imprisonment OR monetary penalties	✓			✓		✓	✓	✓		✓	✓							✓		✓		✓	✓	✓			
Imprisonment AND monetary penalties		✓							✓	✓		✓					✓			✓	✓						
Imprisonment ONLY													✓		✓	✓									✓	✓	
Monetary penalties ONLY					✓																						
Other penalties					✓											✓							✓				

Hungary, Italy, Lithuania, Slovakia and Slovenia only provide for the imprisonment of the offender whereas in Czech Republic only monetary penalties and, where possible, forfeiture of property shall apply. Lithuania, as well as Romania, also provide for disqualification penalties in addition to imprisonment, such as deprivation of the right to be employed in certain positions or to engage in certain activities. This is a very significant solution, as it directly impacts on the opportunity for the offender to be entrusted with certain responsibilities in his future employment.

With respect to the extent of punishment, the Czech Republic is the state where the heaviest fines apply: under Czech law, the infringer shall be punished with a fine up to 1.5 Million Euro. In contrast, Czech law does not provide for imprisonment in case of trade secrets violations.

In most of states trade secrets infringements are punished with imprisonment up to a term of two-three years. There are a few exceptions: in Denmark the offender may be charged with up to six years imprisonment, provided that serious violations have taken place; in Slovenia imprisonment may be up to five years when the acts carried out by the offender concerns information of particular importance. Under the Swedish Act on the Protection of Trade Secrets, terms of imprisonment of up to six years are foreseen for cases of business espionage and up to four years for the unlawful acquisition of trade secrets of significant importance.

### (C) THE SPECIFIC CASE OF IMPORTS OF GOODS INTO THE EU

In the specific case of goods imported from third countries which would have been manufactured using misappropriated trade secrets of EU companies, there is no specific administrative procedure before customs authorities to block them.

The EU Regulation on customs enforcement of intellectual property rights<sup>25</sup> provides for such administrative customs procedures<sup>26</sup>: the holder of an intellectual property right can ask

<sup>24</sup> Baker & McKenzie study.

<sup>25</sup> Regulation (EC) No 1383/2003 of 22 July 2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights, OJ L 196, 2.8.2003, p.7. The Commission made a proposal in 2011 for a new Regulation concerning customs enforcement of intellectual property rights (COM(2011)285). Negotiations on this text before the European Parliament and the Council are on-going.

customs authorities to block imports of goods infringing and intellectual property right. Once the imports blocked, the holder of the intellectual property right has to file a case before a civil court which will decide on the existence (or not) of the infringement. However, this EU rules only applies as regards formal intellectual property rights and do not extent to trade secrets misappropriation claims<sup>27</sup>. Hence, national customs authorities do not process claims for misappropriation of trade secrets.

This situation differs from that in the United States. In the United States, it is possible to engage administrative proceedings before the US International Trade Commission (ITC) in order to block imported goods manufactured using misappropriated trade secrets<sup>28</sup>. Section 337 of the Tariffs Act<sup>29</sup> gives power to the US ITC to deal with claims involving infringements of intellectual property rights but also other forms of unfair competition involving imported products, such as misappropriation of trade secrets. The US ITC has investigative powers. The procedure includes trial proceedings before administrative law judges and review by the US ITC. In terms of remedies, the primary remedy available in Section 337 investigations is an exclusion order that directs US Customs to stop infringing goods from entering the US. In addition, the US ITC may issue cease and desist orders against named importers and other persons engaged in unfair acts that violate Section 337.

Therefore, in order to block goods imported from third countries which would have been manufactured using misappropriated trade secrets of EU companies, the EU owner of the trade secrets in question would need to first go to court in order to have the misappropriation of the trade secrets declared and to obtain an injunction against the third party in question which could be enforced by customs authorities. Compared to formal intellectual property rights, there is therefore an inversion of the burden of proof.

#### **(D) THE PROCEDURAL RULES BEFORE NATIONAL COURTS**

Procedural rules in national law are not always adapted to litigation in trade secrets. Secrecy of information is often at risk during civil proceedings and the absence of protection from (further) disclosure of information as a consequence of court proceedings is a considerable deterrent from starting a legal action<sup>30</sup>.

##### ***(D.1) The insufficient protection of confidential information in national proceedings***

When litigating to defend a trade secret, these procedural rules can result in disclosure of confidential information to the other party or to the public. There are three main situations.

(1) The need to describe the misappropriated trade secret in the application, so that the judge can understand it, could imply that, if the plaintiff does not know the extent of the information misappropriated by the defendant, he could disclose to the defendant (since the application is served to him) more confidential information than actually needed to defend his case<sup>31</sup>.

(2) The general rules on the production of evidence could also have the effect of having to disclose information otherwise considered confidential. In common law countries, the pre-trial duty of (full) discovery rules applies; in continental countries, the defendant may ask for

---

<sup>26</sup> Indeed, administrative customs procedures of this type would be a matter of EU law.

<sup>27</sup> Unless of course the claim encompasses both an intellectual property right infringement (e.g. a patent) as well as a trade secrets misappropriation claim.

<sup>28</sup> See generally [http://www.usitc.gov/intellectual\\_property/](http://www.usitc.gov/intellectual_property/)

<sup>29</sup> For the text of Section 337 of the Tariffs Act, see: [http://www.usitc.gov/intellectual\\_property/documents/statute.pdf](http://www.usitc.gov/intellectual_property/documents/statute.pdf)

<sup>30</sup> Baker & McKenzie study.

<sup>31</sup> See for instance, Hogan Lovells (2012), §57 regarding Belgium, at p.12.

certain documents/evidence to be presented by the other party when such evidence lies in the control of that party – which could imply further disclosure of trade secrets. It should be noted that this plays both ways: bad faith plaintiffs could try this way (and therefore abusing the litigation rules) to obtain confidential information from defendants<sup>32</sup>.

(3) The inherent publicity of judicial proceedings (civil proceedings in all EU Member States are public) could also result in the disclosure of trade secrets, in this case to the public:

- Firstly, hearings are often public. While national procedural laws normally include general provisions which allow Courts to exclude the public from the hearing for reasons relating to security, public order and decency, there do not necessarily apply to trade secrets litigation. In some EU Member States (notably Bulgaria<sup>33</sup>, Estonia<sup>34</sup>, Hungary<sup>35</sup>, Germany<sup>36</sup>, The Netherlands, Poland, Romania, Slovakia, Slovenia), a party has the right to request the court to order that the entire proceeding or a part thereof be heard in private to preserve the secrecy of the trade secret. However, according to Baker & McKenzie (2013), this seems to rarely happen in practice and there would be no case law on this point<sup>37</sup>. In the United Kingdom the parties may agree or apply to the Court to ensure that certain information to be revealed during the pre-trial disclosure procedure remains confidential. The parties may enter into a contractual agreement whereby the parties agree that certain information may remain confidential or only be disclosed to legal counsel or where the parties do not reach such agreement, a party may unilaterally apply to the Court requesting that confidential information is not disclosed to the other party during the proceeding. Requests for restriction of disclosure are at the discretion of the Court.
- Judicial decisions may describe the misappropriated trade secret in question when explaining the reasons for the decision<sup>38</sup>; and in some countries other judicial documents (including applications) may be accessed by third parties. According to Baker & McKenzie (2013), in most countries, pleadings and in general court documents are public and potentially accessible by anyone. Courts have a general duty to adopt adequate measures to safeguard the secret information of a party, for example, by restricting access to those documents which contain trade secrets only to

<sup>32</sup> General procedural rules will normally allow the defendant to refuse to provide a document if it includes a trade secret or a confidential information of the defendant.

<sup>33</sup> In Bulgaria private hearing is specifically provided for cases related to “protection of trade, manufacturing, invention or tax-related secrets” if public disclosure may impair a party’s legitimate interest. When publicity is precluded, only the parties, their attorneys, experts and witnesses are allowed to enter into the court room and are subject to a statutory obligation not to disclose subject matter and content of the relevant proceeding (breach of such obligation entails liability for compensation).

<sup>34</sup> In Estonia (similarly in Finland and Lithuania), in-camera examination can be ordered for the protection of trade secrets if the interest in a public hearing is not deemed to be greater than the commercial interest in protecting the secret.

<sup>35</sup> In Hungary, when the Court orders in-camera examination, the parties are also prohibited from making copies of the minutes of the hearing or of any document containing a trade secret. Examination of documents containing trade secrets is subject to a declaration of non-disclosure and special review procedures are established by the Judge.

<sup>36</sup> In Germany, besides the exclusion of the public if trade secrets are to be discussed, legal practice has developed the so called “Düsseldorfer Procedure” (originally developed for patent law claims but likely applicable to trade secrets cases), which consists in a procedure where Courts order independent proceedings for the preservation of evidence as an interim injunction handed to the defendant together with the statement of claims so that there is no chance to destroy evidence. Evidence is then examined exclusively by authorized experts and attorneys bound to confidentiality. The parties do not have access to the confidential information.

<sup>37</sup> Baker & McKenzie (2013) study.

<sup>38</sup> See for instance, Hogan Lovells (2012), §57 regarding Belgium, at p.12.

the other party's attorney or to the court's expert (in certain cases the confidential information can be put under closed seals), or not disclosing certain information in the court's final decision (by blanking out the relevant information in the decision and other court's documents). However, according to that study, such measures have proved to be of limited effect to prevent the actual leak of confidential information during proceedings<sup>39</sup>.

#### ***(D.2) The example of antitrust proceedings protecting confidential information***

There are specific rules protecting secrecy of confidential information during antitrust proceedings in the Member States. All of them have measures aimed at protecting business secrets/confidential information from being disclosed during proceedings before national competition authorities, even if the procedural steps needed to obtain protection of secret information varies, to a certain extent, from jurisdiction to jurisdiction. In particular, the involved undertakings have the right to indicate the information that, in their opinion, shall not be divulged<sup>40</sup>. Similar provisions exist at EU level for the antitrust proceedings before the European Commission.

#### **(E) THE SPECIFIC CASE OF TRADE SECRETS WHICH ARE DISCLOSED TO PUBLIC AUTHORITIES PURSUANT TO REGULATORY OBLIGATIONS: EU RULES**

Several EU rules are addressing the specific case of trade secrets which are disclosed to public authorities – normally because of regulatory obligations.

#### ***(E.1) The protection of confidential information in public procurement cases***

Industry often expresses the fear that valuable confidential information (i.e. a trade secret) which is disclosed to a public authorities as part of a tender procedure for public procurement could not be sufficiently protected against misappropriation.

This concern is addressed by EU legislation. Current EU rules provide for protection in this regard: *"Without prejudice to the provisions of this Directive, in particular those concerning the obligations relating to the advertising of awarded contracts and to the information to candidates and tenderers [...] the contracting authority shall not disclose information forwarded to it by economic operators which they have designated as confidential; such information includes, in particular technical or trade secrets and the confidential aspects of tenders."*<sup>41</sup>

This protection is also integrated in the 2011 Commission proposal for a new directive on public procurement<sup>42</sup>:

- Article 18 of that proposal<sup>43</sup> requires the contracting authority not to disclose information forwarded to it by economic operators which they have designated as

<sup>39</sup> Baker & McKenzie study.

<sup>40</sup> According to Baker & McKenzie (2013), however, the secrecy of information may not be sufficient to prevent disclosure when such information is relevant to prove the infringement or for the right of defence of the parties (Bulgaria, Estonia, Germany, Greece, Italy, Luxembourg, Portugal). See Baker & McKenzie study.

<sup>41</sup> Article 6 of Directive 2004/18/EC of the European Parliament and the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts.

<sup>42</sup> Commission proposal for a Directive of the European Parliament and of the Council on public procurement, COM(2011) 896 final, Brussels, 20.12.2011. Negotiations before the European Parliament and the Council are on-going.

<sup>43</sup> "Article 18  
Confidentiality

confidential, including, but not limited to, technical or trade secrets and the confidential aspects of tenders. In addition, Article 19(2) of the proposal requires the contracting authorities to ensure, in all communication, exchange and storage of information, that the integrity of data and the confidentiality of tenders are preserved.

- Other provisions in the proposal also require the contracting authorities not to reveal to the other participants in the tender solutions proposed or other confidential information communicated by a candidate participating in the "competitive procedure with negotiation"<sup>44</sup> or in the "competitive dialogue"<sup>45</sup> without its agreement. Such agreement shall not take the form of a general waiver but shall be given with reference to the intended communication of specific solutions or other specific confidential information

The underlying rationale was explained by an English Court of Appeal judge as follows: "*...it is plain that there is a strong public interest in the maintenance of valuable commercial confidential information ... If the penalty for contracting with public authorities were to be the potential loss of such confidential information, then public authorities and the public interest would be the losers, and the result would be potentially anticompetitive.*"<sup>46</sup>

### ***(E.2) The protection of confidentiality of trade secrets disclosed to EU institutions and agencies***

EU institutions have a general policy of transparency and allow third parties to access to the documents they hold, under certain conditions. Given that businesses may disclose confidential business information to EU institutions in the context of specific procedures (e.g. a complaint against a Member State for failure to apply EU law etc) the risk exists that such confidential business information could be disclosed to a third party. This issue is of particular importance when businesses transfer trade secrets to EU regulatory agencies, such as the European Medicines Agency, the European Chemical Agency or the three European financial authorities.

This concern has been considered when adopting the EU general rules<sup>47</sup> dealing with access to documents held by a European institution. Regulation (EC) No 1049/2001<sup>48</sup> provides for the protection of business secrets when the information has been forwarded to a EU institution or body. Article 4(2) states in particular that "*the institutions shall refuse access to a document where disclosure would undermine the protection of the commercial interests of a natural or legal person, including intellectual property*").

---

*1. Unless otherwise provided in this Directive or in the national law concerning access to information, and without prejudice to the obligations relating to the advertising of awarded contracts and to the information to candidates and tenderers set out in Articles 48 and 53 of this Directive, the contracting authority shall not disclose information forwarded to it by economic operators which they have designated as confidential, including, but not limited to, technical or trade secrets and the confidential aspects of tenders.*

*2. Contracting authorities may impose on economic operators requirements aimed at protecting the confidential nature of information which the contracting authorities make available throughout the procurement procedure."*

<sup>44</sup> Cf. Article 27(4) of the proposal.

<sup>45</sup> Cf. Article 28(3) of the proposal.

<sup>46</sup> Veolia vs. Nottinghamshire CC [2010] EWCA 1214 per Rix LJ.

<sup>47</sup> There are specific rules for the access to file in competition cases, see above.

<sup>48</sup> Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. OJ L 145, 31.5.2001, p. 43



EU rules also provide for professional secrecy obligations for their staff. In the case of the EU regulatory agencies, they are under the obligation of professional secrecy and respect of confidentiality of the information when cooperating with other authorities<sup>49</sup>.

***(E.3) The protection of confidentiality of trade secrets disclosed to national supervisory/regulatory agencies***

EU rules also deal with the preservation of confidentiality of information (including business secrets) by national regulatory authorities<sup>50</sup>.

***(E.4) Rules on the non-disclosure of trade secrets to supervisory/regulatory authorities by intermediaries***

Financial intermediaries and some regulated professionals (e.g. lawyers, auditors) often know trade secrets owned by their customers. This is why (inter alia) they are subject to professional secrecy rules, which is a guarantee to their customers.

A specific issue may arise when public authorities require those intermediaries or regulated professionals to disclose to them, in the context of their supervisory functions, confidential information which is sensitive for their customers.

EU rules have addressed this issue and exceptions to the principle of respecting professional secrecy have been established in exceptional circumstances. For instance, the EU anti-money laundering rules<sup>51</sup> require financial intermediaries and regulated professions to disclose to specific authorities (so-called financial intelligence units) data regarding situations suspected of involve money laundering.

<sup>49</sup>

See for instance Article 70 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), OJ L 331, 15.10.2010, p. 12.

"[...]

2.

*Without prejudice to cases covered by criminal law, any confidential information received by persons referred to in paragraph 1 whilst performing their duties may not be divulged to any person or authority whatsoever, except in summary or aggregate form, such that individual financial institutions cannot be identified.*

*Moreover, the obligation under paragraph 1 and the first subparagraph of this paragraph shall not prevent the Authority and the national supervisory authorities from using the information for the enforcement of the acts referred to in Article 1(2), and in particular for legal procedures for the adoption of decisions.*

3.

*Paragraphs 1 and 2 shall not prevent the Authority from exchanging information with national supervisory authorities in accordance with this Regulation and other Union legislation applicable to financial institutions.*

*That information shall be subject to the conditions of professional secrecy referred to in paragraphs 1 and 2. The Authority shall lay down in its internal rules of procedure the practical arrangements for implementing the confidentiality rules referred to in paragraphs 1 and 2."*

Recital 62 of that Regulation says:

*"It is essential that business secrets and other confidential information be protected. The confidentiality of information made available to the Authority and exchanged in the network should be subject to stringent and effective confidentiality rules."*

<sup>50</sup>

See for instance Article 25 of Directive 2004/109/EC of the European Parliament and of the Council of 15 December 2004 on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC, OJ L 390, 31.12.2004, p.38.

<sup>51</sup>

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, p.15.

In other cases, EU rules underlined the need to protect the business secrets of clients. A recent Commission legislative proposal indirectly addressed the protection of business secrets in the specific circumstance where an EU auditor would be required by a third country public authority, for their supervisory purposes<sup>52</sup>, to disclose to it audit working papers containing business secrets of the audited entity. In accordance with this proposal, the EU auditor could only transfer the audit working papers to the third country authority provided that "*the protection of the commercial interests of the audited entity, including its industrial and intellectual property is not undermined*"<sup>53</sup>.

---

<sup>52</sup>

E.g. the audited entity may be an EU subsidiary of an audited entity of that third country.

<sup>53</sup>

Cf. European Commission Proposal of 30 November 2011 for a Directive of the European Parliament and of the council amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts, COM(2011) 778 final. See Article 1(23), introducing a point (ba) in Article 47(2) of Directive 2006/43/EC.



The German comments are as follows:

A.1(ii) (page 3):

Here we would propose to add the following passage to the part dealing with Germany:

"Special rules relating to the protections of trade secrets apply to stock corporations (AG) and limited liability companies (GmbH). As for stock corporations, pursuant to art. 93 sec. 1 of the Stock Corporation Act (Aktiengesetz - AktG), the members of the management board shall keep confidential any information and secrets of the company, namely trade or business secrets. If they fail to comply with this duty, they are liable to the company for any resulting damage."

B.2 (i) (page 12):

Here we would propose that the word "partly" be added to the existing part dealing with Germany ("Germany partly requires that the infringer...") and that the following passage be added to the end of the draft text:

"Pursuant to sec. 85 of the Limited Liability Company Act (GmbHG), any person who reveals a secret of the company without authorization, particularly an operational or business secret, that became known to him in his capacity as managing director, member of the supervisory board or liquidator shall be subject to imprisonment for a period of up to one year or a fine. Indirect intention (dolus eventualis) is sufficient for such act."

B.2 (iii) table 5 (page 14)

In table 5, Germany can be checked in all three categories. There are special regulations for special professions/capacities, such as section 333 of the German Commercial Code (Handelsgesetzbuch - HGB) and section 203 of the German Criminal Code (Strafgesetzbuch - StGB)

B.3 (page 16)

Since section 17 III of the German Unfair Competition Act (Gesetz gegen den unlauteren Wettbewerb - UWG) provides imprisonment of up to five years if aggravating circumstances occur for both groups mentioned in table 6 ("Employees" and "Whoever"), we would propose the addition of the sentence "Imprisonment up to five years if aggravating circumstances occur" to the column "Employees" of table 6 as well. Therefore the reference to Germany in the introductory remarks to table 6 (as an example of a country with varying severity of punishment, depending on whether the offender is an employee or not) should be deleted.

D.1 (3) (page 20)

Here we would prefer the following wording:

"In some EU Member States (notably Bulgaria, Estonia, Hungary, the Netherlands, Poland, Romania, Slovakia, Slovenia), a party has the right to request that the court order the entire proceeding or a part thereof to be heard in private to preserve the trade secret. In Germany, courts can exclude the public from the hearing for reasons relating to trade secrets (section 172 no. 2 of the German Courts Constitution Act [Gerichtsverfassungsgesetz -GVG])."



## LEGISLATIVE FRAMEWORK IN EU MEMBER STATES ON THE PROTECTION OF TRADE SECRETS AGAINST MISAPPROPRIATION

*N.B. Unless otherwise stated, the information contained in this annex is based on: (a) the results of a study recently conducted by Hogan Lovells for the Commission on this matter (available at: [http://ec.europa.eu/internal\\_market/iprenforcement/documents/index\\_en.htm#maincontentSec2](http://ec.europa.eu/internal_market/iprenforcement/documents/index_en.htm#maincontentSec2)) and (b) the preliminary results of another study being carried out for the Commission (by Baker & McKenzie, final results expected for 1<sup>st</sup> quarter 2013).*

### INTRODUCTION

Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)<sup>1</sup> requires its signatories to protect "undisclosed information" (see Box 1).

#### **Box 1 - Article 39 of the TRIPS**

*"1. In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967)<sup>2</sup>, Members shall protect undisclosed information in accordance with paragraph 2 and the data submitted to governments or governmental agencies in accordance with paragraph 3.*

*2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices<sup>10</sup> so as long as such information:*

- (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;*
- (b) has commercial value because it is secret; and*
- (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.*

*3. Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use."*

<sup>10</sup> For the purpose of this provision, "a manner contrary to honest commercial practices" shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition.

There is no specific EU law directly dealing with the misappropriation of trade secrets by third parties (i.e. the case referred to in paragraph 2 of Article 39 of the TRIPS). Therefore, the protection of trade secrets against misappropriation by third parties is primarily addressed by national legislation.

National laws in this area provide for different types of protection. Table 1 provides an overview per country of this protection, which is explained the following sections of this Annex.

<sup>1</sup> The TRIPS is a multilateral agreement which must be joined to by all the members of the World Trade Organisation (WTO).

<sup>2</sup> Cf. The Stockholm Act of the Paris Convention for the Protection of Industrial Property, 14 July 1967.

**Table 1 – Main protection against trade secrets misappropriation by national law**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK	
Trade secrets specific law																								✓				
Trade secret protection in intellectual property code															✓							✓						
Unfair competition law (civil and criminal provisions)	✓				✓	✓	✓											✓			✓		✓					
Unfair competition law (civil provisions only)		✓	✓					✓		✓	✓		✓			✓	✓								✓	✓		
Unfair competition law (criminal provisions only)				✓					✓													✓						
Common law (breach of confidence)														✓												✓		
Criminal law other than unfair competition	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	
Tort law		✓				✓			✓			✓			✓		✓				✓							
Contract law ONLY																				✓								
Labour law																												
	Most Member States																											

Most Member States

However, there are EU rules concerning the treatment of confidential information submitted to public authorities pursuant to legal obligations (i.e. corresponding to the case described in paragraph 3 of Article 39 of the TRIPS). See below [Section \(E\)](#).

### (A) CIVIL/COMMERCIAL LAW<sup>3</sup>

#### (A.1) Civil/commercial law protection in national law: summary

##### (i) Summary

All EU Member States offer some, more or less extensive, form of protection against the misappropriation of trade secrets, albeit this is achieved in different ways.

Some Member States have specific provisions in their civil/commercial law providing protection against the misappropriation of trade secrets

- Sweden has an Act specifically directed against the misappropriation of trade secrets.
- In Italy and Portugal, specific provisions on the protection of trade secrets are included in their respective codes of industrial property – although this does not mean that trade secrets are intellectual property rights.

Other Member States have more general legislation which can be applied.

- Most of them deal with the issue via their law of unfair competition (either civil or criminal provisions, or both): Austria, Belgium, Bulgaria, Czech Republic, Germany, Denmark, Estonia, Greece, Spain, Finland, Hungary, Latvia, Lithuania, Poland, Romania, Slovenia, Slovakia.
- Tort law (or liability for non-contractual responsibility) is used in some countries, either as the main means to address trade secrets misappropriation (Luxembourg, Netherlands) or supplementing the protection offered by unfair competition law (Belgium, Greece).

<sup>3</sup>

Understood as opposed to criminal law. It therefore includes: contract law, labour law, unfair competition law, tort law, intellectual property law.

Almost all jurisdictions have general provisions included in their labour laws or civil codes to prevent employees disclosing their employers' trade secrets, at least during the employment relationship. Contract law can be used to protect trade secrets in all of them, but only Malta seems to exclusively rely on contract law to protect trade secrets.

Common law countries (Ireland, United Kingdom) have developed case law (cf. regarding breach of confidence) in the absence of legislation.

*(ii) Civil rules in Member States<sup>4</sup>*

AT (Austria): Austria's Unfair Competition Act provides civil (and criminal) sanctions against trade or business secret misuse by employees and those who exploit such information without consent for the purposes of competition. Other legislation such as the Patents Act and the Criminal Code also provides legal remedies in particular circumstances, such as disclosure of inventions by employees or in cases of industrial espionage. In addition, the Austrian courts have held that obtaining trade or business secrets by breach of confidence (in the course of contractual negotiations) falls within the Unfair Competition Act.

BE (Belgium): There is no one piece of legislation on the protection of trade secrets as such in Belgium but there are several provisions of Belgian law which can be used against the misuse or disclosure of trade secrets. Trade secret owners generally rely on the general law of tort (Article 1382 of the Belgian Civil Code), unfair competition and specific provisions in Belgian labour law.

BG (Bulgaria): There is no specific legislation on trade secrets in Bulgaria but various laws including the Law on Protection of Competition and the Law on Access to Public Information contain general provisions which may be used to protect trade secrets. In fact, there are over 60 such statutory and non-statutory provisions (including criminal liability under the Criminal Code).

CY (Cyprus): There is no specific legislation governing trade secret misuse in Cyprus but there are a number of different laws which mention trade, business and professional secrets. For example, the Commercial Descriptions Law, the General Product Safety Law and the Competition Law. However, liability is criminal; there is no civil liability for trade secret misuse.

CZ (Czech Republic): The Czech Commercial Code defines a trade secret and provides remedies for trade secret infringement. The TRIPS Agreement is directly applicable in Czech law and thus the definition of a trade secret under Article 39(2) of the TRIPS Agreement also applies in Czech law. The basis of trade secret protection in the Czech Commercial Code, however, is the civil law of unfair competition.

DE (Germany): There are a number of provisions in German legislation protecting trade secrets. The most important statutory provisions for the protection of trade secrets are found in the Act against Unfair Competition. These provisions apply to employees and to third parties. Many of the statutes protecting trade secrets under the criminal law also have civil law provisions. These provisions allow for damages and injunctive relief if one of the relevant criminal law provisions is violated. Civil law remedies are also available under the Civil Code (tort law). German contract law also provides effective protection where there is a contractual obligation to maintain the secrecy of trade secrets.

DK (Denmark): In Denmark there is no statutory definition of trade secrets; however case law has clarified the types of information that are protectable to include both technical and

---

<sup>4</sup> See generally Hogan Lovells (2012).



commercial information. Several statutes, both civil and criminal, are used to protect the rights of trade secret owners as well as legal principles derived from contract law, competition law, employment law and unfair competition law. Most notably, the Criminal Code and the Marketing Practices Act contain provisions protecting trade secrets.

EE (Estonia): Estonian legislation provides specific provisions on the protection of trade secrets, most notably in the Competition Act, the Commercial Code, the Employment Contracts Act and the Penal Code. The Competition Act includes an illustrative list of information considered to constitute trade secrets. The Supreme Court has also held that in addition to this definition, the definition of trade secrets provided in the TRIPS Agreement can also be used to interpret the term "trade secrets" under Estonian law.

EL (Greece): Greek Unfair Competition Law provides specific provisions on the protection of trade secrets. More general protection is found in the Greek Civil Code which includes general tort provisions.

ES (Spain): Trade secrets are mainly protected in Spain under the Unfair Competition Act and the Criminal Code. The Act contains provisions specifically aimed at trade secrets. There are also other laws which deal with trade secret protection indirectly, for example, the laws establishing the obligations of directors and other employees.

FI (Finland): There are a number of Acts which include provisions for the protection of trade secrets, most importantly the Unfair Business Practices Act, the Employment Contracts Act and the Criminal Code. Unlike its neighbour, Sweden, Finland does not have one piece of legislation directed specifically to the protection of trade secrets. Although trade secrets are not considered to be typical intellectual property rights, the broad definition of intellectual property rights under Finnish law encompasses their protection under the Unfair Business Practices Act.

FR (France): The only specific trade secrets legislation in French law is that protecting "manufacturing secrets" in the Intellectual Property Code. Other provisions of civil law (tort law) protect trade secrets more generally. The Labour Code also provides criminal liability for trade secret violations by employees or former employees. When parties are bound by a contractual obligation not to disclose secret information, an action lies for breach of contract.

HU (Hungary): Hungarian law provides specific provisions on the protection of trade secrets. The Civil Code and Unfair Competition Act in particular provide specific protection. Provisions also exist in the Labour Code and in various financial/banking laws.

IE (Ireland): There is no specific legislation in Ireland directed to the protection of trade secrets. However, proceedings may be brought under laws relating to breach of confidence, data protection, criminal damage and specific sectorial pieces of legislation. As in England, Irish law has the equitable principle that a person who has received information in confidence cannot take unfair advantage of it. Generally, Irish law imposes a duty of confidentiality in both non-employment cases and employment cases. In both situations, there must be an obligation of confidence and once it is established that such an obligation exists then the person to whom the information is given has a duty to act in good faith and only use the information for the intended purpose. Again, as in England, an obligation to keep information confidential may either be imposed by contract; implied because of the circumstances of the disclosure or implied because of the special relationship between the parties.

IT (Italy): Specific provisions on the protection of trade secrets are contained in the Italian Code of Industrial Property (IPC). Secret information may only be protected if the requirements set out in the IPC are met. There are also general tortious obligations and unfair

competition provisions in the Civil Code which can be employed to compensate for trade secrets misuse.

LT (Lithuania): Lithuanian legislation provides specific provisions on the protection of trade secrets, most importantly in the Civil Code, the Law on Competition, the Labour Code and the Criminal Code. Under the Civil Code, anyone unlawfully acquiring a commercial secret is liable to compensate the owner for the damage caused. There are also express provisions in the Labour Code regarding disclosure by employees who disclose a commercial secret in breach of their employment contract.

LU (Luxembourg): There are no specific legal provisions protecting trade secrets in Luxembourg. However, trade secrets can be protected by unfair competition law, criminal law, tort law and contractual law.

LV (Latvia): Latvia has a number of pieces of legislation which provide specific provisions on the protection of commercial secrets. The Commercial Law is the main Act regulating commercial activities. It defines "commercial secrets" and provides express protection for them. The Labour Law also includes provisions regarding use of commercial secrets by employees. Latvia also has an Unfair Competition Act which expressly provides that the acquisition, use or disclosure of commercial secrets of another competitor without their consent is a form of unfair competition.

MT (Malta): There is no specific legislation on the protection of trade secrets in Malta. Trade secrets may be protected contractually, by express or implied terms, and, an employee is presumed to be under an obligation not to disclose confidential information. If no contract exists there will be no civil law right to protect a trade secret.

NL (Netherlands): There are no specific provisions on the protection of trade secrets in Dutch legislation. In the Netherlands, the protection of trade secrets is based on the general principle of tort law i.e. an unlawful act. In 1919, the Dutch Supreme Court held that the provision in the Dutch Civil Code on unlawful acts could be used to secure protection against trade secret infringement. Contract law also provides some protection in contractual relationships if there are confidentiality obligations in the contract.

PL (Poland): There are specific provisions on the protection of trade secrets in Polish legislation, notably in the Unfair Competition Act. A number of other Acts mention trade secrets, for example, the Civil Code, the Labour Code, the Act on Competition and Consumer Protection, the Code of Commercial Companies and Partnerships etc. The Labour Code includes express provisions requiring employees to maintain the confidentiality of information the disclosure of which could cause damage to their employer.

PT (Portugal): The Portuguese Industrial Property Code has specific provisions relating to the protection of trade secrets. The Industrial Property Code is directed towards unlawful acts against competitors. A violation is punished, not as a crime, but as a misdemeanour. The Labour Code also contains provisions which stipulate that an employee may not disclose information, while employed, relating to his employer's organisation, production methods and company business.

RO (Romania): There is specific legislation in Romania on the protection of trade secrets. Provisions regulating protection of trade secrets have been included in the Law for the Prevention of Unfair Competition ("Law on Unfair Competition") and specify that the unfair use of a competitor's trade secrets is regarded as contrary to honest commercial practices. Trade.

SE (Sweden): Sweden is the only country in the EU to have an Act specifically protecting trade secrets. The Act provides a definition of trade secrets, penalises trade secret espionage and contains provisions on civil liability.

SI (Slovenia): Trade secrets are specifically protected in Slovenia by a number of pieces of legislation, in particular, the Companies Act, the Employment Relationship Act, the Protection of Competition Act, the Penal Code and the Code of Obligations.

SK (Slovakia): Civil protection of trade secrets in the Slovak Republic is regulated by the Commercial Code. The relevant fields of protection are civil law, commercial law, intellectual property law, non-contractual liability and unfair competition law.

UK (United Kingdom): There is no legislation providing specific protection for trade secrets. Trade secrets are protected by contract and/or by the law of equity.

### ***(A.2) Differences in the scope of protection: the trade secret and the misappropriation***

The absence of homogenous pieces of legislation in this area implies that there is no uniform understanding of what a trade secret is and what misappropriation is:

- In Italy, Portugal and Sweden, there is a specific statutory definition of trade secrets in the applicable legislation.
- A statutory definition of trade secrets is also available in the unfair competition provisions of the Czech Republic, Lithuania and the Slovak Republic.
- In the Czech Republic, Greece, the Netherlands and Spain, the TRIPS definition has been expressly acknowledged and adopted<sup>5</sup>.
- In some cases, definitions of trade secrets can be found in other pieces of laws, for other purposes (e.g. Freedom of Information Act in the UK).

In principle information which meets the requirements of Article 39(2) of the TRIPS<sup>6</sup> would be protectable in all EU Member States. Also, no restrictions seem to exist regarding the type of information which could be protectable and in all EU Member States both technical (e.g. know-how etc.) and commercial secrets (e.g. business strategies etc.). However, the absence of specific definition results in risk of inconsistent interpretation as to what is protectable as trade secrets and consequently, a different protection depending on the type of action initiated by the trade secret owner<sup>7</sup>. Also, differences in courts practices are reported<sup>8</sup>.

Concerning the question of misappropriation, the main divergences relate to the situation of the third party who obtain the secret information in good faith<sup>9</sup>: see below on remedies.

### ***(A3) Differences in the remedies: injunctions, destruction of goods and compensation for prejudice suffered***

#### ***(i) General***

---

<sup>5</sup> Cf. Baker & McKenzie study.

<sup>6</sup> In essence, information which is secret, has commercial value (because it is secret) and has been subject to reasonable steps to keep it secret.

<sup>7</sup> Baker & McKenzie study.

<sup>8</sup> Baker & McKenzie study.

<sup>9</sup> To be sure, no Member State grants any action against a third party who autonomously developed the same information.

The remedies available in civil/commercial law proceedings for the misappropriation of trade secrets do vary and appear to depend on the origin of the action (e.g. based on tort, contract law, unfair competition law etc.): see Table 2 for a summary view.

**Table 2 – Available civil remedies**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Injunctions (cease and desist orders: ordinary action	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Injunctions (cease and desist orders: interim relief	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Return/destruction of trade secrets / goods produced using misappropriated trade secrets: ordinary action	✓	✓			✓	✓	✓			✓		✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Return/destruction of trade secrets / goods produced using misappropriated trade secrets: interim relief	✓	✓			<u>A</u>	✓				✓		✓	✓	✓	✓		✓		✓				✓				✓
Seizure of trade secrets / goods produced using misappropriated trade secrets: ordinary action		✓			✓		✓		✓	✓		✓	✓		✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓
Seizure of trade secrets / goods produced using misappropriated trade secrets: interim relief		✓			<u>A</u>		✓		✓	✓		✓	✓		✓		✓		✓	✓	✓					✓	✓
Withdrawal from the market of goods produced using misappropriated trade secrets: ordinary action		✓			✓		✓		✓	✓		✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓	✓		
Withdrawal from the market of goods produced using misappropriated trade secrets: interim relief		✓			✓				✓	✓		✓	✓		✓		✓		✓				✓	✓	✓		
Damages	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Publication of decisions: ordinary action		✓	✓		<u>A</u>		✓			✓	✓	✓	✓		✓		✓			✓	✓		✓			✓	✓
Publication of decisions: interim relief		✓										✓			✓												
Restraint measures (e.g. penalty for future breach of the Court's order): ordinary action	✓	✓	✓	✓	<u>A</u>				✓		✓	✓			✓	✓	✓			✓					✓		
Restraint measures (e.g. penalty for future breach of the Court's order): interim relief		✓		✓	<u>A</u>				✓			✓			✓		✓								✓		

The above remedies are, in general, all cumulatively available to the trade secret owner, with few exceptions. For example, in Belgium, damages are available but not for cease-and-desist claims brought under the Unfair Competition Act (in the form of expedite action). In Bulgaria, it appears that final injunctions are not available (at least cease-and-desist orders in the strict sense of the word) with damages being the usual final remedy. In Latvia, although potentially available, it is not clear which remedies can effectively be used as there is no case law as to whether remedies provided in the Civil Procedure Code for intellectual property rights apply also to trade secrets (trade secrets are not expressly included among the definition of intellectual property). In Italy damages may only be awarded in ordinary proceedings. In Luxembourg, while injunctions are granted by the President of the Commercial Court, damage claims shall be brought before the District Courts.

*(ii) Injunctions (cease and desist orders)*

In general, injunctions (cease and desist orders) are available in all EU Member States. In all Member States, injunctions (i.e. cease and desist orders) are usually available also as interim

relief remedy (i.e. during preliminary and summary proceedings where the claimant's requests are summarily examined by the Court and measures are granted within a very short time limit).

Therefore, there is civil law redress in order to block the commercialisation of goods (or services) which have been manufactured (or designed) using misappropriated trade secrets (so-called "resulting goods/services"). However, this redress varies from Member State to Member State and there is no guarantee that the "resulting goods/services" will be stopped everywhere in the EU. Cease and desist orders against the use of misappropriated trade secrets by third parties (i.e. beyond a contractual relationship) are not always available:

- (i) when trade secrets are protected under unfair competition rules, the trade secret owner needs to sue a competitor but cannot sue a person having the secret with a view to sell it to another third party or to exploit it for other purposes than competing with the original owner of the secret;
- (ii) solutions diverge regarding the possibility to obtain a cease and desist order against negligent third parties or third parties who obtained the misappropriated trade secrets in good faith but before the trade secrets had reached the public domain. In some EU Member States, remedies are potentially available regardless of the recipient's good or bad faith (Austria<sup>10</sup>, Czech Republic, Denmark, Estonia, Finland, Germany, Ireland, Latvia, Lithuania, and Portugal) and injunctions can be obtained also against a third party who obtained the secret in good faith – however, the third party is likely not to be held liable for damages, unless the use of the secret information continues even after the recipient has been informed of the confidential nature of the information. In others, this is not possible<sup>11</sup>; and
- (iii) cease and desist orders may be limited in time even if the trade secret has not yet reached the public domain. Belgium<sup>12</sup>, Cyprus, Denmark<sup>13</sup>, Greece, The Netherlands<sup>14</sup>, Poland and Slovenia, which do not allow unlimited injunctions. In Common Law countries, injunctions are equitable remedies and, as such, courts are free to determine terms and duration of the restrictions.

Concerning the situation of employees, the Baker & McKenzie study finds that though in general, whilst employed, employees have a (statutory) duty of loyalty (including non-disclosure and non-compete obligations) towards the employer, a common practice in most jurisdictions is to provide for non-use and non-disclosure, as well as non-compete clauses in contracts of employment. However, the position differs as to what can be done in relation to an ex-employee who uses or discloses secrets after leaving employment. The balance between the interests of the employer and the employee is indeed assessed differently in the relevant

---

<sup>10</sup> In Austria, damage claims are also available in cases of default; accordingly damage compensation could be awarded also in case of the third party's slight negligence.

<sup>11</sup> For instance, in the United Kingdom a duty of confidentiality may be implied by the circumstances (the duty of confidentiality is easy to identify in case of an employment contract or a non-disclosure agreement, but it could prove to be very difficult to demonstrate where a person has obtained the confidential information in absence of any relationship between the owner and the recipient), but a person who innocently receives a confidential information will not be under a duty of confidentiality until he is made aware the information is confidential.

<sup>12</sup> In Belgium, courts refuse to grant final injunctions against future trade secrets misappropriation because, contrary to intellectual property rights, trade secret protection can potentially last forever and thus courts are not willing to grant the owner of a trade secret a broader protection than most intellectual property right holders.

<sup>13</sup> In Denmark, although depending on a case by case analysis, final injunctions are usually granted for a period of two to three years from termination of the cooperative relationship.

<sup>14</sup> In Greece and The Netherlands, injunctions are considered temporary in nature.

countries. In general, post-employment, an employee cannot be prevented from using the skill and knowledge gained during the employment, provided that said knowledge does not consist of trade secrets or confidential information that the employee wilfully memorised or (mis)appropriated with the purpose to misuse them after termination of the employment relationship<sup>15</sup>.

*(iii) Destruction of the goods produced using the misappropriate trade secrets or the restitution of the misappropriated information*

Compared to injunctions, other measures such as the destruction of the goods produced using the misappropriate trade secrets or the restitution of the misappropriated information) are not available everywhere and are available in interim proceedings in certain countries only (see Table A6.2). Since resulting goods are not always destroyed, there is no guarantee for the trade secret owner that such goods will no reappear in the market.

*(iv) Damages*

Compensation for the prejudice suffered from the misappropriation of a trade secret is available in all jurisdictions<sup>16</sup>. Damages claims are mainly based on tort or contract and only in a few cases specific provisions on damages are included in either the unfair competition laws (see for example Spain) or in the specific provisions applying to trade secret misappropriation ( Italy and Sweden).

Damages based on tort cover both accruing damages ("*damnum emergens*") and loss of profits ("*lucrum cessans*"). Loss of profits, however, is in most cases very difficult to prove, since the misappropriated information is an intangible asset<sup>17</sup>. This helps explaining the often low compensation obtained<sup>18</sup>. A claim for unjust enrichment is available in some countries

---

<sup>15</sup> In Denmark (and similarly in Poland), the statutory non-disclosure and non-use obligations survive termination of the employment contract for a period of three years. In Italy, as in many other European countries, non-compete agreements (or clauses) are commonly used to prevent use or disclosure after the contract of employment ceases, albeit offering more limited restrictions than those which exist during the period of employment (to be enforceable non-compete clauses must generally be limited in time and space, identify the activities which the former employee cannot engage in and provide for a monetary compensation). In Sweden, damages for breach of confidentiality obligations after termination of employment are only available where there are "extraordinary circumstances". In Ireland and the United Kingdom there is a distinction between general (low grade) confidential information that the employee is not entitled to disclose whilst employed but can use and disclose thereafter and "real trade secrets" which he cannot disclose or use without authority at any time. The distinction depends on a number of factors including whether the employer impressed the secrecy of the relevant information upon the employee; and whether the "secret" can be readily isolated from other information which the employee is free to use.

<sup>16</sup> In Bulgaria, damage compensation is the sole final remedy available to the owner of a trade secret.

<sup>17</sup> According to Baker & McKenzie, there are often evidentiary problems in proving the loss incurred by the owner of a trade secret. In some countries, damages are awarded only if the claimant is able to demonstrate that he had suffered some loss. Other countries allow courts to award damages on an equitable basis - taking into account all the circumstances of the case - if the claimant has not been able to provide sufficient evidence on the amount of damages

<sup>18</sup> According to Baker & McKenzie, damages vary on a case-by-case basis but the average figures collected during the study "seem not to be particularly encouraging". This study mentions a few cases in Italy and Sweden, where courts awarded high amounts of damages: in Italy, in two cases of trade secrets infringement the Court of Milan awarded damages for EUR 1,100,000.00 and EUR 10,000,000.00, respectively. In Sweden, courts have awarded damages for SEK 7/10,000,000.00 and 48,000,000.00. However, the study reports that these appear to be exceptional cases. In the Force India Formula One Team Ltd. case, only €25000 were awarded by a UK court to the claimant. The plaintiff had claimed compensation in excess of £13 million (which was based on the assumption that it succeeded in the entirety of its claims for breach of confidence, which it did not). However, the judge did not accept the plaintiff argument that the relevant information was of great

only, such as among others, Belgium, Estonia, Finland and Spain (for further details please see [Table 3](#) below). In some other countries (for example, Austria, Germany, Italy, Ireland, Lithuania, Poland, Sweden and the United Kingdom) the claimant has the right to claim the account of profits obtained by the infringer from its wrongdoing. In most of the cases, however, the account of profits is alternative to the loss of profits or is considered a criterion to calculate said loss. In Italy, the owner of trade secrets may claim the restitution of the infringer's profit in addition to the loss of profits to the extent that the infringer's profits exceed the claimant's loss. In Greece, account of profits and unjust enrichment are alternative ways to calculate the loss of profits. Similarly in The Netherlands loss or profits excludes account of profits.

**Table 3 – Available damages options**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Accruing damage ( <i>damnum emergens</i> )	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Loss of revenues ( <i>lucrum cessans</i> )	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Moral damages			✓					✓					✓		✓					✓		✓	✓			✓	
Punitive damages														✓													✓
Other monetary compensation					✓																✓						
Account of profits	✓			✓	✓	✓		✓	✓		✓		✓	✓	✓	✓		✓		✓	✓			✓			✓
Fair royalty	✓					✓	✓	✓	✓				✓		✓					✓							✓
Unjust enrichment		✓			✓			✓	✓	✓	✓							✓			✓	✓	✓		✓	✓	
<i>Ex aequo et bono</i> global account		✓	✓					✓			✓		✓		✓	✓	✓		✓	✓	✓	✓	✓				
Cumulation of these options	✓	✓			✓		✓		✓	✓					✓	✓		✓	✓	✓	✓			✓	✓	✓	

If damages are claimed on contract, liquidated damages (if provided by the agreement) can also be claimed in addition to damages. Contractual liability, however, is often limited to the damages which were foreseeable at the time of conclusion of the contract.

The available options are in principle all cumulative (exceptions are Austria, Cyprus, Estonia, Finland, France, Germany, Hungary, Ireland, Luxembourg, Portugal, Romania and United Kingdom) provided that the total amount awarded by the court does not exceed the actual claimant's loss. Furthermore, in countries where courts are allowed to award an "*ex aequo et bono*" global amount in cases where damages cannot be alternatively calculated, such criteria are of course to be considered as alternative to all the other available damage options.

Since most of the EU Member States do not have specific criteria for the calculation of damages, they apply the general criteria of tort liability (i.e., *damnum emergens* and *lucrum cessans*). The license analogy has been indicated as a possible criterion for the calculation of damages<sup>19</sup>, among EU Member States in Austria, Denmark, Germany, Greece, Hungary, Italy, The Netherlands and United Kingdom.

## (B) CRIMINAL LAW

### (B.1) Criminal law protection in national law: summary

value and considered that the misuse of the information was limited in nature, purpose and benefit. As a result, the judge considered that €25000 was the figure the parties would have negotiated had they been in the position of a willing licensor and willing licensee acting reasonable as at the date of the breach of confidence.

<sup>19</sup> This method of calculation is used regarding infringements of intellectual property rights, pursuant to Article 13(1)(b) of Directive 2004/48/EC. This Article provides for the rules on abstract calculation of damages (i.e. calculated on the basis of royalties which could have been due should a licence have existed) as an alternative to the general *damnum emergens* and *lucrum cessans* criteria.



Criminal protection of trade secrets against misappropriation differs from Member State to Member State on several levels, although almost all of them have provisions in this respect. Since there is a lack of a common/shared definition of the scope of trade secrets, the actual extent of the protection provided by states may vary depending on the aims pursued by the provisions implemented for this purpose.

Only a few Member states (i.e., Bulgaria, Ireland, Malta and U.K.) have not established any specific criminal framework with respect to trade secrets violations. However, even in those Member States, the conduct of the infringer may be punished under other related criminal offences (see below). In some cases, where no specific criminal provision has been implemented, penal sanctions of trade secrets misappropriation apply under unfair competition laws or commercial laws. Sweden is the only EU Member state that has implemented a specific law on trade secrets (the Swedish Act on the Protection of Trade Secrets), even though some relevant provisions are also contained in the Criminal Code<sup>20</sup>. Table 4 below summarises the criminal provisions in force:

<i>Table 4 – Criminal provisions applying to trade secrets misappropriation<sup>21</sup></i>																											
	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Criminal code	✓	✓		✓		✓	✓	✓	✓	✓		✓	✓		✓	✓	✓	✓		✓		✓	✓	✓	✓	✓	
Unfair competition / commercial law	✓				✓	✓	✓		✓												✓		✓				
Specific law on trade secrets																								✓			

### **(B.2) Differences in the conducts considered as crimes**

#### *(i) Unauthorised disclosure/use of trade secrets*

Many of the countries seem to limit the scope of trade secrets to the information that a company has a reasonable and objective interest to keep confidential, in accordance with an objective criterion (e.g., Austria, Belgium, France, Germany, Hungary, Italy, Lithuania, Luxembourg, Netherlands, Slovakia, Spain, Sweden). Nonetheless, in some cases the relevant protection is afforded to any information having economic value that the owner deems it opportune for his benefit to keep secret according to a subjective criterion and that are subject to reasonable measures for protection of confidentiality (e.g., this broader interpretation seems to be prevailing in Czech Republic, Finland, Greece, Poland, Romania and Slovenia).

- In Austria the offender to be held criminally liable for trade secrets violations must have acted at least with conditional intent. In Belgium, Estonia, Finland, France the conduct may be punished even if the offender acted with negligence.
- Cyprus does not establish any specific requirement that the offender must meet to be charged with criminal liability for trade secret violations. Nor is there any stated obligation on the claimant to keep information confidential.
- In the Czech Republic the offender must act deliberately to commit the offence. As the relevant conduct is defined as an act of unfair competition, the offender must qualify as a competitor or someone participating in the competitive process. The concept of competition has nevertheless been construed very broadly, including even indirect or potential competitors.

<sup>20</sup> In particular, the Act on the Swedish Protection of Trade Secrets establishes two different offences: business espionage and the unauthorized dealing with trade secrets. Other complimentary or more general offences, such as, for instance, unauthorized access to computer systems or breach of faith against principal are regulated under the Criminal Code.

<sup>21</sup> Baker & McKenzie study.

- In Denmark the offences provided for under the Criminal Code require intent. Only upon certain circumstances if the employee causes a substantial risk of dissemination of confidential information by negligence he or she may be charged with criminal liability pursuant to Section 19 of the Marketing Practices Act. without having acted with intent.
- Germany requires that the infringer acts with intent and, specifically, for the purpose of competition, for personal gain, for benefit of a third party or causing damage to the owner of the secret.
- In Greece the offender must act (with intent) for purpose of competition, that means that two criteria have to be met: (i) the conduct of the offender must be suitable to serve the purpose of competition; (ii) he or she must act with the “intention of competition”, i.e. enhance his or third parties’ competitiveness.
- As to Hungary and Italy, the offender may be punished only if he or she acts with intent.
- In Latvia the employer is obliged to identify in writing the information considered to be commercial secrets. In any case, the offender requires the offender to have acted for use or disclosure by himself or another person, therefore intent is required for the offence to occur.
- Lithuania requires that the offender, in case of business espionage, acted with the intent to unlawfully obtain a trade secret, whereas, in the case of violation of trade secrets, with the intent to get a financial gain or to injure the owner by the disclosure to third parties or the use of the information.

As almost all EU Member states require that the offender acted with intent, it emerges that whoever commits a trade secrets infringement must have clearly the knowledge that the business information constituted trade secrets, even if there is no express obligation to keep such information confidential.

- In Luxembourg, Netherlands and Portugal the offender must act with the intent to reach a competitive advantage or to cause harm to the owner.
- Also Poland requires intent, as the offender must breach an obligation of confidentiality that must be prior established by the owner of the secret, either directly or indirectly.
- Under Romanian and Slovak law the offender must act with intent, but no specific purpose is required.
- The same applies in Slovenia, where if the conduct reaches certain outcome, the offender may be charged with the more severe correspondent penalties.
- Spain also requires intent, even if the purposes to be pursued vary depending on the type of offence considered (for instance, commercial advantage).
- The Swedish Act on the Protection of Trade Secret does not pose any requirement as to the purpose that the offender acts for. It only requires that he acted wilfully and without authorization.

#### *(ii) Related offences*

In Belgium a person who commits the offence under Section 309 of Criminal Code (unauthorized disclosure of trade secrets) may also be charged with theft or misappropriation (provided that he qualifies as an employee with the company). Similarly, Section 491 applies

when a person is entrusted as a data processor/handler manufacturing secrets that are physically stored breaches his duty of confidence.

In Bulgaria, for instance, the offence of business bribery is punishable and applicable to, any individual who discloses to third parties information that he knows in return for something.

In France there is a wide range of crimes that may arise in connection to trade secrets violations:

- First, the offence of theft may occur when the conduct at stake consists in the fraudulent appropriation of third parties' data carriers containing confidential information. Such an offence has been found by the Court of cassation to apply even in connection to disclosure of trade secrets. Theft is punished by imprisonment up to three years and a fine of Euro 45,000.00.
- Additionally, the offence of breach of trust may be committed where an individual with the company misappropriates documents containing confidential information entrusted to them for temporary use. In such a case, the offender shall be punished by imprisonment up to three years or a fine of Euro 375,000.00.
- Also, other provisions of the Criminal Code punish the act of supplying secret information to foreign powers by imprisonment up to fifteen years and a fine of Euro 225,000.00.

In Germany cases of industrial espionage may result in theft or misappropriation.

In Greece the infringement of trade secret may constitute, among other offences, a breach of trust under Section 390 of the Criminal Code. In such a case, the offender shall be punished by imprisonment up to ten years and a fine up to Euro 15,000.00.

Depending on the circumstances, violations of trade secrets may result, further to civil lawsuits, in a number of offences, including but not limited to insider trading, unauthorized access to computer systems and a breach of privacy.

As to Italy, the conduct of the offender who commits an unauthorized use or disclosure of trade secrets may also constitute theft or misappropriation.

In Latvia acts of unauthorized disclosure or acquisition of trade secrets may constitute unfair competition practices where repeated within a one-year period and, thus, result in a punishment by imprisonment of up to two years and a fine, in addition to disqualification penalties.

Violations of trade secrets may constitute fraud or bribery in Lithuania or theft in Luxembourg. In Netherlands the conducts may also result in the theft of secret documents or hacking of computer systems. In Portugal the related offences include computer and communications fraud. Slovakia, in addition to breach of trade secrets, criminalizes the misuse of participation in economic competition through unfair acts.

In Slovenia the same act may be punished under the crime of "disclosure of and unauthorized access to trade secrets" as well as, for instance, the offence of abuse of insider information. Spain provides an extensive regulation of trade secrets infringements: however, pursuant to Section 278.3 of the Criminal Code the specific provisions apply without prejudice to the penalties that may arise for appropriating or destroying the computer media, i.e. for the offences of theft or misappropriation.

In Sweden, further to the offences provided for under the act on the Protection of Trade Secrets, other criminal provisions may apply, including unauthorized access to computer

systems, unlawful dispossession, unlawful use, espionage, unlawful dealing with secret information and negligent dealing with confidential information.

Offences in any way related to trade secrets violations have significant importance in the legal systems that do not establish any specific provision in this respect:

- In Bulgaria violations of trade secrets may be punished only indirectly. The relevant offences in this respect include the disclosure of service/office secrets, the business bribe and computer crimes.
- Under Irish law, for instance, trade secrets infringements may result in: (i) disclosure of personal data obtained without authority; (ii) unauthorised accessing of data; (iii) unlawful use of a computer; (iv) theft or (v) criminal infringements of intellectual property rights.
- Under Maltese criminal law, in the absence of provisions specifically concerning trade secrets, one could be charged with misappropriation and fraudulent gains as a result of his conduct.
- In the U.K. the criminal provisions that may apply in connection to trade secrets infringement cases include theft, fraud, conspiracy to defraud as well as, upon certain circumstances, some of the offences provided for under the Computer Misuse Act (such as unauthorized access to information contained on a computer) and the Data Protection Act (although it is very unlikely that personal data qualify as trade secrets).

### (iii) Qualified offences

Certain Member States also establish qualified offences when the revelation or use of confidential information is committed by a person acting in a particular capacity (e.g., as civil servant, public official, or as person handling confidential information by reason of his job, e.g. lawyers, officers). Please note that this does not mean that for each of the offences a specific provision is established. Separate provisions may have been implemented (e.g. Italy) or, like in Estonia, the same provision may apply to professional and official secrets, also covering trade secrets. See [Table 5](#):

<i>Table 5 – Qualified offences<sup>22</sup></i>																											
	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Breach of professional secrecy	✓	✓		✓				✓	✓						✓				✓	✓		✓	✓	✓	✓	✓	
Breach of official secret	✓		✓	✓				✓	✓		✓				✓							✓	✓				
Other breach of confidence										✓				✓													
Separate provisions	Y	Y	N	N	N/A		N/A	N	N		Y	N		Y	N				N/A	N		Y	Y			N	

### (iv) Threshold for the applicability of criminal penalties

In the Czech Republic only violations resulting in a damage of at least Euro 2,000.00 may give rise to criminal liability. The offender must cause harm to a competitor or a consumer equivalent to such an amount or provide someone else than the owner of the secret with a benefit of the same amount. The offender does not necessarily need to be a legal person or an enterprise.

A *de minimis* threshold applies in Lithuania, where for the offender to be prosecuted it is required that the conduct caused a damage of at least EUR 5,648.00.

<sup>22</sup> Baker & McKenzie study.

Something like a *de minimis* threshold is established in Poland, where the conduct must have caused substantial damage to the owner, although no quantification of this concept is provided for in the law.

Slovakia establishes that for the offender to be prosecuted a significant damage (more than EUR 26,600.00) must be caused by his conduct to another competitor. It also provides for a more severe penalty in cases where the conduct causes a large scale damage (over EUR 133,000.00).

Also under Estonian and Finnish criminal law a general safe harbor clause applies, preventing prosecution in case the offence is found to be of minor harm.

In Austria the offender will not be prosecuted if his conduct is justified by a compelling public or private interest.

No safe harbor seems to exist in Latvia and Sweden. In Cyprus disclosure of trade secrets is allowed, for instance, when protection of health and safety of citizens is affected, i.e. where compelling public interests are at stake or to prove the violations of statutory provisions.

Similarly, no safe harbor or *de minimis* threshold applies in Denmark, Finland, Italy, Luxembourg, Slovenia. Germany does not provide for any safe harbor; however, disclosure of trade secrets is justified when committed to avert an imminent danger to life, limb, freedom, honour, property or other prevailing legal interests. In Greece trade secrets are not protected in case a witness is examined to represent certain circumstances before the Court, excluding state secrets. In Hungary Section 300(2) of Criminal Code expressly sets forth some safe harbors that justify infringement of trade secrets. These clauses include:

- (i) fulfilment of duties prescribed in a separate act governing the publication of information and information to be disclosed in the public interest;
- (ii) fulfilment of duties subject to statutory reporting obligations, even in the case the report was filed in good faith and proved to be unfounded.

In the Netherlands a specific provision sets out an exemption for those who disclosed in good faith a trade secret assuming that the disclosure was in the public interest. Portugal and Romania consider the consent of the owner to the disclosure of a secret as a safe harbor clause. In addition to that, Romanian law permits the disclosure of trade secrets where compelling public interests are at stake. Spain does not consider information about illegal activities carried out by the owner to be a trade secret: therefore, its revelation would not determine any prosecution.

Generally speaking, the risk of dissemination of confidential information does not amount to a criminal offence (except for Slovakia, Slovenia). The conduct carried out by the infringer must result in an actual violation of the interest protected under the relevant provisions. In contrast, most legal systems (including Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Italy, Latvia, Lithuania, Slovakia, Slovenia) provide criminal protection against the intent to commit a trade secret violation. The acts carried out with the purpose of disclosing or using confidential business information which reach a certain threshold in the realisation of the offence are likely to trigger criminal liability.

### ***(B.3) Differences in the penalties***

The conducts which normally give rise to violations of trade secrets include the access to confidential information, the use or the disclosure thereof or the illicit acquisition for exploitation by the offender or third parties. These conducts are generally punished regardless

of the fact that the offender qualifies as a competitor and may be committed either by (past) employees of the company or by external persons (such as consultants, contractors, agents).

It is quite frequent, however, that the violation of trade secrets committed by an employee of the company owning the confidential business information results in a more severe punishment than that provided for the same offence in other cases (i.e., in Belgium, Germany, Greece and Spain).

Table 6 below provides a summary of the main conducts concerning trade secrets violation and the related punishment provided for under the legal systems.

**Table 6 – Criminal penalties applying to trade secrets misappropriation<sup>23</sup>**

Country	Offender	Conduct	Penalties
Austria	Whoever	Disclosure or exploitation of trade or business secrets	Up to six months imprisonment; up to one year if the conduct is committed with the purpose to obtain a pecuniary advantage or to cause harm to the owner or monetary penalties
		Spying out trade or business secrets for their exploitation by somebody else or disclosure	Up to two years imprisonment OR monetary penalties
		Spying out trade or business secrets for their exploitation abroad	Up to three years imprisonment AND monetary penalties
Belgium	Whoever	Communicating in bad faith manufacturing secrets appropriated during the (past) employment with the owner	From three months up to three years imprisonment AND monetary fine from Euro 50 to 2,000.00
Bulgaria		There is no specific criminal provision concerning violation of trade secrets. However, depending on the characteristics of the conduct, the offender may be charged with more general offences, such as business bribe or computer crimes	
Cyprus	Whoever	Disclosure of trade secrets	Imprisonment up to one year OR monetary fine up to Euro 1,275.00
		Disclosure of information protected by professional secrecy involving trade secrets	Imprisonment up to six months AND/OR monetary fine up to Euro 1,700.00
Czech Republic	Whoever	Acts of unfair competition infringing trade secrets and causing damage in or in excess of Euro 2,000.00 to other competitors/consumers or providing someone with unjustified benefit in the same or greater amount	Monetary fine up to Euro 1.5 Million*
Denmark	Whoever	Unauthorized misuse or appropriation of trade secrets	Imprisonment up to 1 year and 6 months OR monetary fine
		Serious violations such as appropriation of trade secrets in a contract of service or in the performance of assignments	Imprisonment up to six years
Estonia	Whoever	Unauthorized disclosure or use of business secret learned by reason of the professional or official duties with the purpose of causing damage	Imprisonment up to one year OR monetary fine
Finland	Whoever	Disclosure or use of trade secrets known by reason of the employment, position or other lawful activities to obtain financial benefit or to injure the owner	Imprisonment up to two years OR monetary fine
		Misuse of trade secrets obtained or revealed through an unlawful act	Imprisonment up to two years OR monetary fine
		Business espionage: Unlawfully obtaining information regarding trade secrets	Imprisonment up to two years OR monetary fine
France	Whoever	Revelation of manufacturing secrets	Imprisonment up to two years AND monetary fine of Euro 30,000.00
		Theft (for instance, of carriers or materials containing trade secrets)	Imprisonment up to three years AND monetary fine of Euro 45,000.00
Germany	Employees	Unauthorized communication of trade or business secrets that the offender was granted access to for the purpose of obtaining financial advantage or injuring the owner	Imprisonment up to three years OR monetary fine
	Whoever	Unauthorized acquiring or securing trade or business secrets or using thereof	Imprisonment up to three years OR monetary fine. Imprisonment up to five years if aggravating circumstances occur
Greece	Whoever	Copying, printing, using, disclosing or in any way	Imprisonment from three months up to

		violating data or computer programs constituting secrets of an enterprise	one year. Imprisonment from one year to five years if the offender is in the service of the owner and the secrets are of great financial significance
	Employees	Unauthorized communication to third parties of secrets that the offender has known by reason of his employment to obtain financial advantage or to cause a damage to the owner; Unauthorized use of the information so obtained	Imprisonment up to six months AND monetary fine up to Euro 8.80
Hungary	Whoever	Making available to unauthorized persons secrets for financial advantage or to cause damage to others; Using the secrets so obtained	Imprisonment up to three years
Ireland	Not applicable		
Italy	Whoever	Disclosure or use of any information concerning scientific discoveries or inventions or industrial applications that is intended to remain secret known by the offender by reason of his status, function, job or art, to obtain a profit	Imprisonment up to two years
Latvia	Whoever	Revelation of non-disclosable information other than a state secret; Unauthorized acquisition and disclosure of commercial secrets	Imprisonment up to five years OR monetary fine
Lithuania	Whoever	Unlawful acquisition of commercial secrets or communication to third persons; Disclosure of information that the offender was entrusted with by reason of his employment	Imprisonment up to two years AND/OR disqualification penalties
Luxembourg	Employees	Use or disclosure, during the employment or within two years after its expiration, trade or manufacturing secrets known by reason of the job to obtain financial advantage or to cause damage to the owner	Imprisonment from three months to three years AND monetary fine from Euro 251 to 12,500.00
Malta	Not applicable		
Netherlands	Employee	Intentional disclosure of confidential information that may harm the owner	Imprisonment up to six months AND/OR monetary fine up to Euro 19,500.00
Poland	Whoever	Disclosure or exploitation of trade secret in breach of confidential duties that causes substantial damage to the owner; Use of information illegally acquired or disclosure to third persons	Imprisonment from one month to two years AND monetary fine up to Euro 260,000.00*
Portugal	Whoever	Use or disclosure to third parties of secrets that the offender knows by reason of his status, job, profession or art	Imprisonment up to one year OR monetary fine
Romania	Whoever	Disclosure, acquisition or use of trade secrets without the consent of the owner, as a result of an action of commercial or industrial espionage	Imprisonment from six months up to two years OR monetary fine from Euro 570 to 5,000.00*
		Disclosure of data or information not intended to be publicly known by a person who knows it by reason of his employment, provided that the offence is likely to cause damages	Imprisonment from two up to seven years; Imprisonment from six months to five years if the disclosure is made by another person
Slovakia	Whoever	Spying out trade secrets with the intention to disclose them to unauthorized persons	Imprisonment from six months up to three years; Imprisonment from seven to twelve years if aggravating circumstances occur
Slovenia	Whoever	Disclosure of trade secrets; Providing unauthorized third parties with access to trade secrets; Collection of trade secrets with the purpose of delivering them to unauthorized persons; Unlawful obtaining of trade secrets with the purpose of delivering them to unauthorized persons	Imprisonment up to three years; Imprisonment up to five years if the information is of particular importance
Spain	Whoever	Acquiring data, documents, media and other objects to discover trade secrets; Disclosure, revelation or communication to third parties of the discovered information	Imprisonment from two up to four years AND monetary fine; Imprisonment from three to five years AND monetary fine in case the secrets are disclosed
		Diffusion, disclosure or communication of trade secrets in breach of duties of confidentiality	Imprisonment from two up to four years AND monetary fine, in case the information is disclosed in breach of confidentiality
Sweden	Whoever	Unauthorized access of trade secrets as business espionage	Imprisonment up to two years OR monetary fine; Imprisonment up to six years in case of information of significant importance
		Acquiring trade secrets knowing that the person who made it available accessed the trade secret through acts of business espionage	Imprisonment up to two years OR monetary fine; Imprisonment up to four years in case of information of significant importance

U.K.	Not applicable		
* Monetary penalties are expressed in local currency and converted to Euro for the reader's convenience			

Generally, punishment of the offender is by imprisonment, even though he or she may also be charged, either in addition to that or alternatively, with monetary penalties: see Table 7 with penalties that shall apply for the main offence (for instance, unauthorized disclosure/use of trade secrets).

**Table 7 – Penalties<sup>24</sup>**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Imprisonment OR monetary penalties	✓			✓	A	✓	✓	✓		✓	✓							✓		✓		✓	✓	✓			
Imprisonment AND monetary penalties		✓							✓	✓		✓					✓			✓	✓						
Imprisonment ONLY													✓		✓	✓									✓	✓	
Monetary penalties ONLY																											
Other penalties					✓											✓							✓				

Hungary, Italy, Lithuania, Slovakia and Slovenia only provide for the imprisonment of the offender whereas in Czech Republic only monetary penalties and, where possible, forfeiture of property shall apply. Lithuania, as well as Romania, also provide for disqualification penalties in addition to imprisonment, such as deprivation of the right to be employed in certain positions or to engage in certain activities. This is a very significant solution, as it directly impacts on the opportunity for the offender to be entrusted with certain responsibilities in his future employment.

With respect to the extent of punishment, the Czech Republic is the state where the heaviest fines apply: under Czech law, the infringer shall be punished with a fine up to 1.5 Million Euro. In contrast, Czech law does not provide for imprisonment in case of trade secrets violations.

In most of states trade secrets infringements are punished with imprisonment up to a term of two-three years. There are a few exceptions: in Denmark the offender may be charged with up to six years imprisonment, provided that serious violations have taken place; in Slovenia imprisonment may be up to five years when the acts carried out by the offender concerns information of particular importance. Under the Swedish Act on the Protection of Trade Secrets, terms of imprisonment of up to six years are foreseen for cases of business espionage and up to four years for the unlawful acquisition of trade secrets of significant importance.

### (C) THE SPECIFIC CASE OF IMPORTS OF GOODS INTO THE EU

In the specific case of goods imported from third countries which would have been manufactured using misappropriated trade secrets of EU companies, there is no specific administrative procedure before customs authorities to block them.

The EU Regulation on customs enforcement of intellectual property rights<sup>25</sup> provides for such administrative customs procedures<sup>26</sup>: the holder of an intellectual property right can ask

<sup>24</sup> Baker & McKenzie study.

<sup>25</sup> Regulation (EC) No 1383/2003 of 22 July 2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights, OJ L 196, 2.8.2003, p.7. The Commission made a proposal in 2011 for a new Regulation concerning customs enforcement of intellectual property rights (COM(2011)285). Negotiations on this text before the European Parliament and the Council are on-going.



customs authorities to block imports of goods infringing and intellectual property right. Once the imports blocked, the holder of the intellectual property right has to file a case before a civil court which will decide on the existence (or not) of the infringement. However, this EU rules only applies as regards formal intellectual property rights and do not extent to trade secrets misappropriation claims<sup>27</sup>. Hence, national customs authorities do not process claims for misappropriation of trade secrets.

This situation differs from that in the United States. In the United States, it is possible to engage administrative proceedings before the US International Trade Commission (ITC) in order to block imported goods manufactured using misappropriated trade secrets<sup>28</sup>. Section 337 of the Tariffs Act<sup>29</sup> gives power to the US ITC to deal with claims involving infringements of intellectual property rights but also other forms of unfair competition involving imported products, such as misappropriation of trade secrets. The US ITC has investigative powers. The procedure includes trial proceedings before administrative law judges and review by the US ITC. In terms of remedies, the primary remedy available in Section 337 investigations is an exclusion order that directs US Customs to stop infringing goods from entering the US. In addition, the US ITC may issue cease and desist orders against named importers and other persons engaged in unfair acts that violate Section 337.

Therefore, in order to block goods imported from third countries which would have been manufactured using misappropriated trade secrets of EU companies, the EU owner of the trade secrets in question would need to first go to court in order to have the misappropriation of the trade secrets declared and to obtain an injunction against the third party in question which could be enforced by customs authorities. Compared to formal intellectual property rights, there is therefore an inversion of the burden of proof.

#### **(D) THE PROCEDURAL RULES BEFORE NATIONAL COURTS**

Procedural rules in national law are not always adapted to litigation in trade secrets. Secrecy of information is often at risk during civil proceedings and the absence of protection from (further) disclosure of information as a consequence of court proceedings is a considerable deterrent from starting a legal action<sup>30</sup>.

##### ***(D.1) The insufficient protection of confidential information in national proceedings***

When litigating to defend a trade secret, these procedural rules can result in disclosure of confidential information to the other party or to the public. There are three main situations.

(1) The need to describe the misappropriated trade secret in the application, so that the judge can understand it, could imply that, if the plaintiff does not know the extent of the information misappropriated by the defendant, he could disclose to the defendant (since the application is served to him) more confidential information than actually needed to defend his case<sup>31</sup>.

(2) The general rules on the production of evidence could also have the effect of having to disclose information otherwise considered confidential. In common law countries, the pre-trial duty of (full) discovery rules applies; in continental countries, the defendant may ask for

---

<sup>26</sup> Indeed, administrative customs procedures of this type would be a matter of EU law.

<sup>27</sup> Unless of course the claim encompasses both an intellectual property right infringement (e.g. a patent) as well as a trade secrets misappropriation claim.

<sup>28</sup> See generally [http://www.usitc.gov/intellectual\\_property/](http://www.usitc.gov/intellectual_property/)

<sup>29</sup> For the text of Section 337 of the Tariffs Act, see: [http://www.usitc.gov/intellectual\\_property/documents/statute.pdf](http://www.usitc.gov/intellectual_property/documents/statute.pdf)

<sup>30</sup> Baker & McKenzie study.

<sup>31</sup> See for instance, Hogan Lovells (2012), §57 regarding Belgium, at p.12.

certain documents/evidence to be presented by the other party when such evidence lies in the control of that party – which could imply further disclosure of trade secrets. It should be noted that this plays both ways: bad faith plaintiffs could try this way (and therefore abusing the litigation rules) to obtain confidential information from defendants<sup>32</sup>.

(3) The inherent publicity of judicial proceedings (civil proceedings in all EU Member States are public) could also result in the disclosure of trade secrets, in this case to the public:

- Firstly, hearings are often public. While national procedural laws normally include general provisions which allow Courts to exclude the public from the hearing for reasons relating to security, public order and decency, there do not necessarily apply to trade secrets litigation. In some EU Member States (notably Bulgaria<sup>33</sup>, Estonia<sup>34</sup>, Hungary<sup>35</sup>, Germany<sup>36</sup>, The Netherlands, Poland, Romania, Slovakia, Slovenia), a party has the right to request the court to order that the entire proceeding or a part thereof be heard in private to preserve the secrecy of the trade secret. However, according to Baker & McKenzie (2013), this seems to rarely happen in practice and there would be no case law on this point<sup>37</sup>. In the United Kingdom the parties may agree or apply to the Court to ensure that certain information to be revealed during the pre-trial disclosure procedure remains confidential. The parties may enter into a contractual agreement whereby the parties agree that certain information may remain confidential or only be disclosed to legal counsel or where the parties do not reach such agreement, a party may unilaterally apply to the Court requesting that confidential information is not disclosed to the other party during the proceeding. Requests for restriction of disclosure are at the discretion of the Court.
- Judicial decisions may describe the misappropriated trade secret in question when explaining the reasons for the decision<sup>38</sup>; and in some countries other judicial documents (including applications) may be accessed by third parties. According to Baker & McKenzie (2013), in most countries, pleadings and in general court documents are public and potentially accessible by anyone. Courts have a general duty to adopt adequate measures to safeguard the secret information of a party, for example, by restricting access to those documents which contain trade secrets only to

<sup>32</sup> General procedural rules will normally allow the defendant to refuse to provide a document if it includes a trade secret or a confidential information of the defendant.

<sup>33</sup> In Bulgaria private hearing is specifically provided for cases related to “protection of trade, manufacturing, invention or tax-related secrets” if public disclosure may impair a party’s legitimate interest. When publicity is precluded, only the parties, their attorneys, experts and witnesses are allowed to enter into the court room and are subject to a statutory obligation not to disclose subject matter and content of the relevant proceeding (breach of such obligation entails liability for compensation).

<sup>34</sup> In Estonia (similarly in Finland and Lithuania), in-camera examination can be ordered for the protection of trade secrets if the interest in a public hearing is not deemed to be greater than the commercial interest in protecting the secret.

<sup>35</sup> In Hungary, when the Court orders in-camera examination, the parties are also prohibited from making copies of the minutes of the hearing or of any document containing a trade secret. Examination of documents containing trade secrets is subject to a declaration of non-disclosure and special review procedures are established by the Judge.

<sup>36</sup> In Germany, besides the exclusion of the public if trade secrets are to be discussed, legal practice has developed the so called “Düsseldorf Procedure” (originally developed for patent law claims but likely applicable to trade secrets cases), which consists in a procedure where Courts order independent proceedings for the preservation of evidence as an interim injunction handed to the defendant together with the statement of claims so that there is no chance to destroy evidence. Evidence is then examined exclusively by authorized experts and attorneys bound to confidentiality. The parties do not have access to the confidential information.

<sup>37</sup> Baker & McKenzie (2013) study.

<sup>38</sup> See for instance, Hogan Lovells (2012), §57 regarding Belgium, at p.12.

the other party's attorney or to the court's expert (in certain cases the confidential information can be put under closed seals), or not disclosing certain information in the court's final decision (by blanking out the relevant information in the decision and other court's documents). However, according to that study, such measures have proved to be of limited effect to prevent the actual leak of confidential information during proceedings<sup>39</sup>.

#### ***(D.2) The example of antitrust proceedings protecting confidential information***

There are specific rules protecting secrecy of confidential information during antitrust proceedings in the Member States. All of them have measures aimed at protecting business secrets/confidential information from being disclosed during proceedings before national competition authorities, even if the procedural steps needed to obtain protection of secret information varies, to a certain extent, from jurisdiction to jurisdiction. In particular, the involved undertakings have the right to indicate the information that, in their opinion, shall not be divulged<sup>40</sup>. Similar provisions exist at EU level for the antitrust proceedings before the European Commission.

#### **(E) THE SPECIFIC CASE OF TRADE SECRETS WHICH ARE DISCLOSED TO PUBLIC AUTHORITIES PURSUANT TO REGULATORY OBLIGATIONS: EU RULES**

Several EU rules are addressing the specific case of trade secrets which are disclosed to public authorities – normally because of regulatory obligations.

#### ***(E.1) The protection of confidential information in public procurement cases***

Industry often expresses the fear that valuable confidential information (i.e. a trade secret) which is disclosed to a public authorities as part of a tender procedure for public procurement could not be sufficiently protected against misappropriation.

This concern is addressed by EU legislation. Current EU rules provide for protection in this regard: "*Without prejudice to the provisions of this Directive, in particular those concerning the obligations relating to the advertising of awarded contracts and to the information to candidates and tenderers [...] the contracting authority shall not disclose information forwarded to it by economic operators which they have designated as confidential; such information includes, in particular technical or trade secrets and the confidential aspects of tenders.*"<sup>41</sup>

This protection is also integrated in the 2011 Commission proposal for a new directive on public procurement<sup>42</sup>:

- Article 18 of that proposal<sup>43</sup> requires the contracting authority not to disclose information forwarded to it by economic operators which they have designated as

---

<sup>39</sup> Baker & McKenzie study.

<sup>40</sup> According to Baker & McKenzie (2013), however, the secrecy of information may not be sufficient to prevent disclosure when such information is relevant to prove the infringement or for the right of defence of the parties (Bulgaria, Estonia, Germany, Greece, Italy, Luxembourg, Portugal). See Baker & McKenzie study.

<sup>41</sup> Article 6 of Directive 2004/18/EC of the European Parliament and the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts.

<sup>42</sup> Commission proposal for a Directive of the European Parliament and of the Council on public procurement, COM(2011) 896 final, Brussels, 20.12.2011. Negotiations before the European Parliament and the Council are on-going.

<sup>43</sup> "Article 18  
Confidentiality

confidential, including, but not limited to, technical or trade secrets and the confidential aspects of tenders. In addition, Article 19(2) of the proposal requires the contracting authorities to ensure, in all communication, exchange and storage of information, that the integrity of data and the confidentiality of tenders are preserved.

- Other provisions in the proposal also require the contracting authorities not to reveal to the other participants in the tender solutions proposed or other confidential information communicated by a candidate participating in the "competitive procedure with negotiation"<sup>44</sup> or in the "competitive dialogue"<sup>45</sup> without its agreement. Such agreement shall not take the form of a general waiver but shall be given with reference to the intended communication of specific solutions or other specific confidential information

The underlying rationale was explained by an English Court of Appeal judge as follows: "*...it is plain that there is a strong public interest in the maintenance of valuable commercial confidential information ... If the penalty for contracting with public authorities were to be the potential loss of such confidential information, then public authorities and the public interest would be the losers, and the result would be potentially anticompetitive.*"<sup>46</sup>

### ***(E.2) The protection of confidentiality of trade secrets disclosed to EU institutions and agencies***

EU institutions have a general policy of transparency and allow third parties to access to the documents they hold, under certain conditions. Given that businesses may disclose confidential business information to EU institutions in the context of specific procedures (e.g. a complaint against a Member State for failure to apply EU law etc) the risk exists that such confidential business information could be disclosed to a third party. This issue is of particular importance when businesses transfer trade secrets to EU regulatory agencies, such as the European Medicines Agency, the European Chemical Agency or the three European financial authorities.

This concern has been considered when adopting the EU general rules<sup>47</sup> dealing with access to documents held by a European institution. Regulation (EC) No 1049/2001<sup>48</sup> provides for the protection of business secrets when the information has been forwarded to a EU institution or body. Article 4(2) states in particular that "*the institutions shall refuse access to a document where disclosure would undermine the protection of the commercial interests of a natural or legal person, including intellectual property*").

---

1. Unless otherwise provided in this Directive or in the national law concerning access to information, and without prejudice to the obligations relating to the advertising of awarded contracts and to the information to candidates and tenderers set out in Articles 48 and 53 of this Directive, the contracting authority shall not disclose information forwarded to it by economic operators which they have designated as confidential, including, but not limited to, technical or trade secrets and the confidential aspects of tenders.

2. Contracting authorities may impose on economic operators requirements aimed at protecting the confidential nature of information which the contracting authorities make available throughout the procurement procedure."

<sup>44</sup> Cf. Article 27(4) of the proposal.

<sup>45</sup> Cf. Article 28(3) of the proposal.

<sup>46</sup> Veolia vs. Nottinghamshire CC [2010] EWCA 1214 per Rix LJ.

<sup>47</sup> There are specific rules for the access to file in competition cases, see above.

<sup>48</sup> Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. OJ L 145, 31.5.2001, p. 43

EU rules also provide for professional secrecy obligations for their staff. In the case of the EU regulatory agencies, they are under the obligation of professional secrecy and respect of confidentiality of the information when cooperating with other authorities<sup>49</sup>.

***(E.3) The protection of confidentiality of trade secrets disclosed to national supervisory/regulatory agencies***

EU rules also deal with the preservation of confidentiality of information (including business secrets) by national regulatory authorities<sup>50</sup>.

***(E.4) Rules on the non-disclosure of trade secrets to supervisory/regulatory authorities by intermediaries***

Financial intermediaries and some regulated professionals (e.g. lawyers, auditors) often know trade secrets owned by their customers. This is why (inter alia) they are subject to professional secrecy rules, which is a guarantee to their customers.

A specific issue may arise when public authorities require those intermediaries or regulated professionals to disclose to them, in the context of their supervisory functions, confidential information which is sensitive for their customers.

EU rules have addressed this issue and exceptions to the principle of respecting professional secrecy have been established in exceptional circumstances. For instance, the EU anti-money laundering rules<sup>51</sup> require financial intermediaries and regulated professions to disclose to specific authorities (so-called financial intelligence units) data regarding situations suspected of involve money laundering.

---

<sup>49</sup> See for instance Article 70 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), OJ L 331, 15.10.2010, p. 12.

"[...]

2.

*Without prejudice to cases covered by criminal law, any confidential information received by persons referred to in paragraph 1 whilst performing their duties may not be divulged to any person or authority whatsoever, except in summary or aggregate form, such that individual financial institutions cannot be identified.*

*Moreover, the obligation under paragraph 1 and the first subparagraph of this paragraph shall not prevent the Authority and the national supervisory authorities from using the information for the enforcement of the acts referred to in Article 1(2), and in particular for legal procedures for the adoption of decisions.*

3.

*Paragraphs 1 and 2 shall not prevent the Authority from exchanging information with national supervisory authorities in accordance with this Regulation and other Union legislation applicable to financial institutions.*

*That information shall be subject to the conditions of professional secrecy referred to in paragraphs 1 and 2. The Authority shall lay down in its internal rules of procedure the practical arrangements for implementing the confidentiality rules referred to in paragraphs 1 and 2."*

Recital 62 of that Regulation says:

*"It is essential that business secrets and other confidential information be protected. The confidentiality of information made available to the Authority and exchanged in the network should be subject to stringent and effective confidentiality rules."*

<sup>50</sup> See for instance Article 25 of Directive 2004/109/EC of the European Parliament and of the Council of 15 December 2004 on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC, OJ L 390, 31.12.2004, p.38.

<sup>51</sup> Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, p.15.

In other cases, EU rules underlined the need to protect the business secrets of clients. A recent Commission legislative proposal indirectly addressed the protection of business secrets in the specific circumstance where an EU auditor would be required by a third country public authority, for their supervisory purposes<sup>52</sup>, to disclose to it audit working papers containing business secrets of the audited entity. In accordance with this proposal, the EU auditor could only transfer the audit working papers to the third country authority provided that "*the protection of the commercial interests of the audited entity, including its industrial and intellectual property is not undermined*"<sup>53</sup>.

---

<sup>52</sup> E.g. the audited entity may be an EU subsidiary of an audited entity of that third country.

<sup>53</sup> Cf. European Commission Proposal of 30 November 2011 for a Directive of the European Parliament and of the council amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts, COM(2011) 778 final. See Article 1(23), introducing a point (ba) in Article 47(2) of Directive 2006/43/EC.



## LEGISLATIVE FRAMEWORK IN EU MEMBER STATES ON THE PROTECTION OF TRADE SECRETS AGAINST MISAPPROPRIATION

*N.B. Unless otherwise stated, the information contained in this annex is based on: (a) the results of a study recently conducted by Hogan Lovells for the Commission on this matter (available at: [http://ec.europa.eu/internal\\_market/iprenforcement/documents/index\\_en.htm#maincontentSec2](http://ec.europa.eu/internal_market/iprenforcement/documents/index_en.htm#maincontentSec2)) and (b) the preliminary results of another study being carried out for the Commission (by Baker & McKenzie, final results expected for 1<sup>st</sup> quarter 2013).*

### INTRODUCTION

Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)<sup>1</sup> requires its signatories to protect "undisclosed information" (see Box 1).

#### **Box 1 - Article 39 of the TRIPS**

*"1. In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967)<sup>2</sup>, Members shall protect undisclosed information in accordance with paragraph 2 and the data submitted to governments or governmental agencies in accordance with paragraph 3.*

*2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices<sup>10</sup> so as long as such information:*

- (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;*
- (b) has commercial value because it is secret; and*
- (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.*

*3. Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use."*

<sup>10</sup> For the purpose of this provision, "a manner contrary to honest commercial practices" shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition.

There is no specific EU law directly dealing with the misappropriation of trade secrets by third parties (i.e. the case referred to in paragraph 2 of Article 39 of the TRIPS). Therefore, the protection of trade secrets against misappropriation by third parties is primarily addressed by national legislation.

National laws in this area provide for different types of protection. Table 1 provides an overview per country of this protection, which is explained the following sections of this Annex.

<sup>1</sup> The TRIPS is a multilateral agreement which must be joined to by all the members of the World Trade Organisation (WTO).

<sup>2</sup> Cf. The Stockholm Act of the Paris Convention for the Protection of Industrial Property, 14 July 1967.



**Table 1 – Main protection against trade secrets misappropriation by national law**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Trade secrets specific law																								✓			
Trade secret protection in intellectual property code															✓							✓					
Unfair competition law (civil and criminal provisions)	✓					✓	✓	✓			✓							✓			✓		✓				
Unfair competition law (civil provisions only)		✓	✓					✓		✓	✓		✓			✓	✓								✓	✓	
Unfair competition law (criminal provisions only)				✓					✓													✓					
Common law (breach of confidence)														✓												✓	
Criminal law other than unfair competition	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Tort law		✓				✓			✓			✓			✓		✓			✓							
Contract law ONLY																				✓							
Labour law																											

Most Member States

However, there are EU rules concerning the treatment of confidential information submitted to public authorities pursuant to legal obligations (i.e. corresponding to the case described in paragraph 3 of Article 39 of the TRIPS). See below [Section \(E\)](#).

#### (A) CIVIL/COMMERCIAL LAW<sup>3</sup>

##### (A.1) Civil/commercial law protection in national law: summary

###### (i) Summary

All EU Member States offer some, more or less extensive, form of protection against the misappropriation of trade secrets, albeit this is achieved in different ways.

Some Member States have specific provisions in their civil/commercial law providing protection against the misappropriation of trade secrets

- Sweden has an Act specifically directed against the misappropriation of trade secrets.
- In Italy and Portugal, specific provisions on the protection of trade secrets are included in their respective codes of industrial property – although this does not mean that trade secrets are intellectual property rights.

Other Member States have more general legislation which can be applied.

- Most of them deal with the issue via their law of unfair competition (either civil or criminal provisions, or both): Austria, Belgium, Bulgaria, Czech Republic, Germany, Denmark, Estonia, Greece, Spain, Finland, Hungary, Latvia, Lithuania, Poland, Romania, Slovenia, Slovakia.
- Tort law (or liability for non-contractual responsibility) is used in some countries, either as the main means to address trade secrets misappropriation (Luxembourg, Netherlands) or supplementing the protection offered by unfair competition law (Belgium, Greece).

<sup>3</sup>

Understood as opposed to criminal law. It therefore includes: contract law, labour law, unfair competition law, tort law, intellectual property law.

Almost all jurisdictions have general provisions included in their labour laws or civil codes to prevent employees disclosing their employers' trade secrets, at least during the employment relationship. Contract law can be used to protect trade secrets in all of them, but only Malta seems to exclusively rely on contract law to protect trade secrets.

Common law countries (Ireland, United Kingdom) have developed case law (cf. regarding breach of confidence) in the absence of legislation.

*(ii) Civil rules in Member States<sup>4</sup>*

AT (Austria): Austria's Unfair Competition Act provides civil (and criminal) sanctions against trade or business secret misuse by employees and those who exploit such information without consent for the purposes of competition. Other legislation such as the Patents Act and the Criminal Code also provides legal remedies in particular circumstances, such as disclosure of inventions by employees or in cases of industrial espionage. In addition, the Austrian courts have held that obtaining trade or business secrets by breach of confidence (in the course of contractual negotiations) falls within the Unfair Competition Act.

BE (Belgium): There is no one piece of legislation on the protection of trade secrets as such in Belgium but there are several provisions of Belgian law which can be used against the misuse or disclosure of trade secrets. Trade secret owners generally rely on the general law of tort (Article 1382 of the Belgian Civil Code), unfair competition and specific provisions in Belgian labour law.

BG (Bulgaria): There is no specific legislation on trade secrets in Bulgaria but various laws including the Law on Protection of Competition and the Law on Access to Public Information contain general provisions which may be used to protect trade secrets. In fact, there are over 60 such statutory and non-statutory provisions (including criminal liability under the Criminal Code).

CY (Cyprus): There is no specific legislation governing trade secret misuse in Cyprus but there are a number of different laws which mention trade, business and professional secrets. For example, the Commercial Descriptions Law, the General Product Safety Law and the Competition Law. However, liability is criminal; there is no civil liability for trade secret misuse.

CZ (Czech Republic): The Czech Commercial Code defines a trade secret and provides remedies for trade secret infringement. The TRIPS Agreement is directly applicable in Czech law and thus the definition of a trade secret under Article 39(2) of the TRIPS Agreement also applies in Czech law. The basis of trade secret protection in the Czech Commercial Code, however, is the civil law of unfair competition.

DE (Germany): There are a number of provisions in German legislation protecting trade secrets. The most important statutory provisions for the protection of trade secrets are found in the Act against Unfair Competition. These provisions apply to employees and to third parties. Many of the statutes protecting trade secrets under the criminal law also have civil law provisions. These provisions allow for damages and injunctive relief if one of the relevant criminal law provisions is violated. Civil law remedies are also available under the Civil Code (tort law). German contract law also provides effective protection where there is a contractual obligation to maintain the secrecy of trade secrets.

DK (Denmark): In Denmark there is no statutory definition of trade secrets; however case law has clarified the types of information that are protectable to include both technical and

<sup>4</sup> See generally Hogan Lovells (2012).

commercial information. Several statutes, both civil and criminal, are used to protect the rights of trade secret owners as well as legal principles derived from contract law, competition law, employment law and unfair competition law. Most notably, the Criminal Code and the Marketing Practices Act contain provisions protecting trade secrets.

EE (Estonia): Estonian legislation provides specific provisions on the protection of trade secrets, most notably in the Competition Act, the Commercial Code, the Employment Contracts Act and the Penal Code. The Competition Act includes an illustrative list of information considered to constitute trade secrets. The Supreme Court has also held that in addition to this definition, the definition of trade secrets provided in the TRIPS Agreement can also be used to interpret the term "trade secrets" under Estonian law.

EL (Greece): Greek Unfair Competition Law provides specific provisions on the protection of trade secrets. More general protection is found in the Greek Civil Code which includes general tort provisions.

ES (Spain): Trade secrets are mainly protected in Spain under the Unfair Competition Act and the Criminal Code. The Act contains provisions specifically aimed at trade secrets. There are also other laws which deal with trade secret protection indirectly, for example, the laws establishing the obligations of directors and other employees.

FI (Finland): There are a number of Acts which include provisions for the protection of trade secrets, most importantly the Unfair Business Practices Act, the Employment Contracts Act and the Criminal Code. ~~Unlike its neighbour, Sweden, Finland does not have one piece of legislation directed specifically to the protection of trade secrets. Although trade secrets are not considered to be typical intellectual property rights, the broad definition of intellectual property rights under the Finnish law encompasses their the protection of trade secrets under the Unfair Business Practices Act, trade secrets are not considered to be intellectual property rights.~~

Comment [LHu3]: some modifications

FR (France): The only specific trade secrets legislation in French law is that protecting "manufacturing secrets" in the Intellectual Property Code. Other provisions of civil law (tort law) protect trade secrets more generally. The Labour Code also provides criminal liability for trade secret violations by employees or former employees. When parties are bound by a contractual obligation not to disclose secret information, an action lies for breach of contract.

HU (Hungary): Hungarian law provides specific provisions on the protection of trade secrets. The Civil Code and Unfair Competition Act in particular provide specific protection. Provisions also exist in the Labour Code and in various financial/banking laws.

IE (Ireland): There is no specific legislation in Ireland directed to the protection of trade secrets. However, proceedings may be brought under laws relating to breach of confidence, data protection, criminal damage and specific sectorial pieces of legislation. As in England, Irish law has the equitable principle that a person who has received information in confidence cannot take unfair advantage of it. Generally, Irish law imposes a duty of confidentiality in both non-employment cases and employment cases. In both situations, there must be an obligation of confidence and once it is established that such an obligation exists then the person to whom the information is given has a duty to act in good faith and only use the information for the intended purpose. Again, as in England, an obligation to keep information confidential may either be imposed by contract; implied because of the circumstances of the disclosure or implied because of the special relationship between the parties.

IT (Italy): Specific provisions on the protection of trade secrets are contained in the Italian Code of Industrial Property (IPC). Secret information may only be protected if the requirements set out in the IPC are met. There are also general tortious obligations and unfair

competition provisions in the Civil Code which can be employed to compensate for trade secrets misuse.

LT (Lithuania): Lithuanian legislation provides specific provisions on the protection of trade secrets, most importantly in the Civil Code, the Law on Competition, the Labour Code and the Criminal Code. Under the Civil Code, anyone unlawfully acquiring a commercial secret is liable to compensate the owner for the damage caused. There are also express provisions in the Labour Code regarding disclosure by employees who disclose a commercial secret in breach of their employment contract.

LU (Luxembourg): There are no specific legal provisions protecting trade secrets in Luxembourg. However, trade secrets can be protected by unfair competition law, criminal law, tort law and contractual law.

LV (Latvia): Latvia has a number of pieces of legislation which provide specific provisions on the protection of commercial secrets. The Commercial Law is the main Act regulating commercial activities. It defines "commercial secrets" and provides express protection for them. The Labour Law also includes provisions regarding use of commercial secrets by employees. Latvia also has an Unfair Competition Act which expressly provides that the acquisition, use or disclosure of commercial secrets of another competitor without their consent is a form of unfair competition.

MT (Malta): There is no specific legislation on the protection of trade secrets in Malta. Trade secrets may be protected contractually, by express or implied terms, and, an employee is presumed to be under an obligation not to disclose confidential information. If no contract exists there will be no civil law right to protect a trade secret.

NL (Netherlands): There are no specific provisions on the protection of trade secrets in Dutch legislation. In the Netherlands, the protection of trade secrets is based on the general principle of tort law i.e. an unlawful act. In 1919, the Dutch Supreme Court held that the provision in the Dutch Civil Code on unlawful acts could be used to secure protection against trade secret infringement. Contract law also provides some protection in contractual relationships if there are confidentiality obligations in the contract.

PL (Poland): There are specific provisions on the protection of trade secrets in Polish legislation, notably in the Unfair Competition Act. A number of other Acts mention trade secrets, for example, the Civil Code, the Labour Code, the Act on Competition and Consumer Protection, the Code of Commercial Companies and Partnerships etc. The Labour Code includes express provisions requiring employees to maintain the confidentiality of information the disclosure of which could cause damage to their employer.

PT (Portugal): The Portuguese Industrial Property Code has specific provisions relating to the protection of trade secrets. The Industrial Property Code is directed towards unlawful acts against competitors. A violation is punished, not as a crime, but as a misdemeanour. The Labour Code also contains provisions which stipulate that an employee may not disclose information, while employed, relating to his employer's organisation, production methods and company business.

RO (Romania): There is specific legislation in Romania on the protection of trade secrets. Provisions regulating protection of trade secrets have been included in the Law for the Prevention of Unfair Competition ("Law on Unfair Competition") and specify that the unfair use of a competitor's trade secrets is regarded as contrary to honest commercial practices. Trade.

SE (Sweden): Sweden is the only country in the EU to have an Act specifically protecting trade secrets. The Act provides a definition of trade secrets, penalises trade secret espionage and contains provisions on civil liability.

SI (Slovenia): Trade secrets are specifically protected in Slovenia by a number of pieces of legislation, in particular, the Companies Act, the Employment Relationship Act, the Protection of Competition Act, the Penal Code and the Code of Obligations.

SK (Slovakia): Civil protection of trade secrets in the Slovak Republic is regulated by the Commercial Code. The relevant fields of protection are civil law, commercial law, intellectual property law, non-contractual liability and unfair competition law.

UK (United Kingdom): There is no legislation providing specific protection for trade secrets. Trade secrets are protected by contract and/or by the law of equity.

***(A.2) Differences in the scope of protection: the trade secret and the misappropriation***

The absence of homogenous pieces of legislation in this area implies that there is no uniform understanding of what a trade secret is and what misappropriation is:

- In Italy, Portugal and Sweden, there is a specific statutory definition of trade secrets in the applicable legislation.
- A statutory definition of trade secrets is also available in the unfair competition provisions of the Czech Republic, Lithuania and the Slovak Republic.
- In the Czech Republic, Greece, the Netherlands and Spain, the TRIPS definition has been expressly acknowledged and adopted<sup>5</sup>.
- In some cases, definitions of trade secrets can be found in other pieces of laws, for other purposes (e.g. Freedom of Information Act in the UK).

In principle information which meets the requirements of Article 39(2) of the TRIPS<sup>6</sup> would be protectable in all EU Member States. Also, no restrictions seem to exist regarding the type of information which could be protectable and in all EU Member States both technical (e.g. know-how etc.) and commercial secrets (e.g. business strategies etc.). However, the absence of specific definition results in risk of inconsistent interpretation as to what is protectable as trade secrets and consequently, a different protection depending on the type of action initiated by the trade secret owner<sup>7</sup>. Also, differences in courts practices are reported<sup>8</sup>.

Concerning the question of misappropriation, the main divergences relate to the situation of the third party who obtain the secret information in good faith<sup>9</sup>: see below on remedies.

***(A3) Differences in the remedies: injunctions, destruction of goods and compensation for prejudice suffered***

***(i) General***

<sup>5</sup> Cf. Baker & McKenzie study.

<sup>6</sup> In essence, information which is secret, has commercial value (because it is secret) and has been subject to reasonable steps to keep it secret.

<sup>7</sup> Baker & McKenzie study.

<sup>8</sup> Baker & McKenzie study.

<sup>9</sup> To be sure, no Member State grants any action against a third party who autonomously developed the same information.

The remedies available in civil/commercial law proceedings for the misappropriation of trade secrets do vary and appear to depend on the origin of the action (e.g. based on tort, contract law, unfair competition law etc.); see Table 2 for a summary view.

Table 2 – Available civil remedies

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Injunctions (cease and desist orders): ordinary action	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Injunctions (cease and desist orders): interim relief	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Return/destruction of trade secrets / goods produced using misappropriated trade secrets: ordinary action	✓	✓			✓	✓	✓		✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Return/destruction of trade secrets / goods produced using misappropriated trade secrets: interim relief	✓	✓			✓				✓			✓	✓	✓	✓		✓		✓				✓				✓
Seizure of trade secrets / goods produced using misappropriated trade secrets: ordinary action		✓			✓		✓		✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Seizure of trade secrets / goods produced using misappropriated trade secrets: interim relief		✓				✓			✓	✓		✓	✓		✓		✓		✓	✓	✓	✓				✓	✓
Withdrawal from the market of goods produced using misappropriated trade secrets: ordinary action		✓			✓		✓		✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Withdrawal from the market of goods produced using misappropriated trade secrets: interim relief		✓			✓				✓	✓		✓	✓		✓		✓		✓			✓	✓	✓			✓
Damages	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Publication of decisions: ordinary action		✓	✓				✓		✓		✓	✓	✓		✓	✓			✓	✓	✓		✓			✓	✓
Publication of decisions: interim relief		✓										✓			✓												
Restraint measures (e.g. penalty for future breach of the Court's order): ordinary action	✓	✓	✓	✓					✓		✓	✓		✓	✓	✓			✓					✓			
Restraint measures (e.g. penalty for future breach of the Court's order): interim relief		✓	✓						✓		✓	✓		✓	✓	✓								✓			

Comment [LHu4]: addition

The above remedies are, in general, all cumulatively available to the trade secret owner, with few exceptions. For example, in Belgium, damages are available but not for cease-and-desist claims brought under the Unfair Competition Act (in the form of expedite action). In Bulgaria, it appears that final injunctions are not available (at least cease-and-desist orders in the strict sense of the word) with damages being the usual final remedy. In Latvia, although potentially available, it is not clear which remedies can effectively be used as there is no case law as to whether remedies provided in the Civil Procedure Code for intellectual property rights apply also to trade secrets (trade secrets are not expressly included among the definition of intellectual property). In Italy damages may only be awarded in ordinary proceedings. In Luxembourg, while injunctions are granted by the President of the Commercial Court, damage claims shall be brought before the District Courts.

(ii) Injunctions (cease and desist orders)

In general, injunctions (cease and desist orders) are available in all EU Member States. In all Member States, injunctions (i.e. cease and desist orders) are usually available also as interim relief remedy (i.e. during preliminary and summary proceedings where the claimant's requests are summarily examined by the Court and measures are granted within a very short time limit).

Therefore, there is civil law redress in order to block the commercialisation of goods (or services) which have been manufactured (or designed) using misappropriated trade secrets (so-called "resulting goods/services"). However, this redress varies from Member State to Member State and there is no guarantee that the "resulting goods/services" will be stopped everywhere in the EU. Cease and desist orders against the use of misappropriated trade secrets by third parties (i.e. beyond a contractual relationship) are not always available:

- (i) when trade secrets are protected under unfair competition rules, the trade secret owner needs to sue a competitor but cannot sue a person having the secret with a view to sell it to another third party or to exploit it for other purposes than competing with the original owner of the secret;
- (ii) solutions diverge regarding the possibility to obtain a cease and desist order against negligent third parties or third parties who obtained the misappropriated trade secrets in good faith but before the trade secrets had reached the public domain. In some EU Member States, remedies are potentially available regardless of the recipient's good or bad faith (Austria<sup>10</sup>, Czech Republic, Denmark, Estonia, Finland, Germany, Ireland, Latvia, Lithuania, and Portugal) and injunctions can be obtained also against a third party who obtained the secret in good faith – however, the third party is likely not to be held liable for damages, unless the use of the secret information continues even after the recipient has been informed of the confidential nature of the information. In others, this is not possible<sup>11</sup>; and
- (iii) cease and desist orders may be limited in time even if the trade secret has not yet reached the public domain. Belgium<sup>12</sup>, Cyprus, Denmark<sup>13</sup>, Greece, The Netherlands<sup>14</sup>, Poland and Slovenia, which do not allow unlimited injunctions. In Common Law countries, injunctions are equitable remedies and, as such, courts are free to determine terms and duration of the restrictions.

Concerning the situation of employees, the Baker & McKenzie study finds that though in general, whilst employed, employees have a (statutory) duty of loyalty (including non-disclosure and non-compete obligations) towards the employer, a common practice in most jurisdictions is to provide for non-use and non-disclosure, as well as non-compete clauses in contracts of employment. However, the position differs as to what can be done in relation to

<sup>10</sup> In Austria, damage claims are also available in cases of default; accordingly damage compensation could be awarded also in case of the third party's slight negligence.

<sup>11</sup> For instance, in the United Kingdom a duty of confidentiality may be implied by the circumstances (the duty of confidentiality is easy to identify in case of an employment contract or a non-disclosure agreement, but it could prove to be very difficult to demonstrate where a person has obtained the confidential information in absence of any relationship between the owner and the recipient), but a person who innocently receives a confidential information will not be under a duty of confidentiality until he is made aware the information is confidential.

<sup>12</sup> In Belgium, courts refuse to grant final injunctions against future trade secrets misappropriation because, contrary to intellectual property rights, trade secret protection can potentially last forever and thus courts are not willing to grant the owner of a trade secret a broader protection than most intellectual property right holders.

<sup>13</sup> In Denmark, although depending on a case by case analysis, final injunctions are usually granted for a period of two to three years from termination of the cooperative relationship.

<sup>14</sup> In Greece and The Netherlands, injunctions are considered temporary in nature.



an ex-employee who uses or discloses secrets after leaving employment. The balance between the interests of the employer and the employee is indeed assessed differently in the relevant countries. In general, post-employment, an employee cannot be prevented from using the skill and knowledge gained during the employment, provided that said knowledge does not consist of trade secrets or confidential information that the employee wilfully memorised or (mis)appropriated with the purpose to misuse them after termination of the employment relationship<sup>15</sup>.

*(iii) Destruction of the goods produced using the misappropriate trade secrets or the restitution of the misappropriated information*

Compared to injunctions, other measures such as the destruction of the goods produced using the misappropriate trade secrets or the restitution of the misappropriated information are not available everywhere and are available in interim proceedings in certain countries only (see [Table A6.2](#)). Since resulting goods are not always destroyed, there is no guarantee for the trade secret owner that such goods will no reappear in the market.

*(iv) Damages*

Compensation for the prejudice suffered from the misappropriation of a trade secret is available in all jurisdictions<sup>16</sup>. Damages claims are mainly based on tort or contract and only in a few cases specific provisions on damages are included in either the unfair competition laws (see for example Spain) or in the specific provisions applying to trade secret misappropriation (Italy and Sweden).

Damages based on tort cover both accruing damages ("*damnum emergens*") and loss of profits ("*lucrum cessans*"). Loss of profits, however, is in most cases very difficult to prove, since the misappropriated information is an intangible asset<sup>17</sup>. This helps explaining the often low compensation obtained<sup>18</sup>. A claim for unjust enrichment is available in some countries

<sup>15</sup> In Denmark (and similarly in Poland), the statutory non-disclosure and non-use obligations survive termination of the employment contract for a period of three years. In Italy, as in many other European countries, non-compete agreements (or clauses) are commonly used to prevent use or disclosure after the contract of employment ceases, albeit offering more limited restrictions than those which exist during the period of employment (to be enforceable non-compete clauses must generally be limited in time and space, identify the activities which the former employee cannot engage in and provide for a monetary compensation). In Sweden, damages for breach of confidentiality obligations after termination of employment are only available where there are "extraordinary circumstances". In Ireland and the United Kingdom there is a distinction between general (low grade) confidential information that the employee is not entitled to disclose whilst employed but can use and disclose thereafter and "real trade secrets" which he cannot disclose or use without authority at any time. The distinction depends on a number of factors including whether the employer impressed the secrecy of the relevant information upon the employee; and whether the "secret" can be readily isolated from other information which the employee is free to use.

<sup>16</sup> In Bulgaria, damage compensation is the sole final remedy available to the owner of a trade secret.

<sup>17</sup> According to Baker & McKenzie, there are often evidentiary problems in proving the loss incurred by the owner of a trade secret. In some countries, damages are awarded only if the claimant is able to demonstrate that he had suffered some loss. Other countries allow courts to award damages on an equitable basis - taking into account all the circumstances of the case - if the claimant has not been able to provide sufficient evidence on the amount of damages

<sup>18</sup> According to Baker & McKenzie, damages vary on a case-by-case basis but the average figures collected during the study "seem not to be particularly encouraging". This study mentions a few cases in Italy and Sweden, where courts awarded high amounts of damages: in Italy, in two cases of trade secrets infringement the Court of Milan awarded damages for EUR 1,100,000.00 and EUR 10,000,000.00, respectively. In Sweden, courts have awarded damages for SEK 7/10,000,000.00 and 48,000,000.00. However, the study reports that these appear to be exceptional cases.

In the Force India Formula One Team Ltd. case, only €25000 were awarded by a UK court to the claimant. The plaintiff had claimed compensation in excess of £13 million (which was based on the

only, such as among others, Belgium, Estonia, Finland and Spain (for further details please see Table 3 below). In some other countries (for example, Austria, Germany, Italy, Ireland, Lithuania, Poland, Sweden and the United Kingdom) the claimant has the right to claim the account of profits obtained by the infringer from its wrongdoing. In most of the cases, however, the account of profits is alternative to the loss of profits or is considered a criterion to calculate said loss. In Italy, the owner of trade secrets may claim the restitution of the infringer's profit in addition to the loss of profits to the extent that the infringer's profits exceed the claimant's loss. In Greece, account of profits and unjust enrichment are alternative ways to calculate the loss of profits. Similarly in The Netherlands loss or profits excludes account of profits.

**Table 3 – Available damages options**

	AT	BE	BG	CY	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Accruing damage ( <i>damnum emergens</i> )	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Loss of revenues ( <i>lucrum cessans</i> )	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Moral damages			✓					✓				✓	✓						✓		✓	✓			✓	
Punitive damages													✓													✓
Other monetary compensation					✓															✓						
Account of profits	✓			✓	✓		✓	✓		✓		✓	✓	✓		✓		✓	✓			✓				✓
Fair royalty	✓				✓	✓		✓		✓		✓	✓						✓							✓
Unjust enrichment		✓			✓			✓	✓	✓						✓					✓	✓	✓	✓	✓	✓
<i>Ex aequo et bono</i> global account		✓	✓					✓		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cumulation of these options		✓	✓		✓			✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓

Comment [LHu5]: addition

Comment [LHu6]: addition

If damages are claimed on contract, liquidated damages (if provided by the agreement) can also be claimed in addition to damages. Contractual liability, however, is often limited to the damages which were foreseeable at the time of conclusion of the contract.

The available options are in principle all cumulative (exceptions are Austria, Cyprus, Estonia, Finland, France, Germany, Hungary, Ireland, Luxembourg, Portugal, Romania and United Kingdom) provided that the total amount awarded by the court does not exceed the actual claimant's loss. Furthermore, in countries where courts are allowed to award an "*ex aequo et bono*" global amount in cases where damages cannot be alternatively calculated, such criteria are of course to be considered as alternative to all the other available damage options.

Since most of the EU Member States do not have specific criteria for the calculation of damages, they apply the general criteria of tort liability (i.e., *damnum emergens* and *lucrum cessans*). The license analogy has been indicated as a possible criterion for the calculation of damages<sup>19</sup>, among EU Member States in Austria, Denmark, Germany, Greece, Hungary, Italy, The Netherlands and United Kingdom.

## (B) CRIMINAL LAW

assumption that it succeeded in the entirety of its claims for breach of confidence, which it did not). However, the judge did not accept the plaintiff argument that the relevant information was of great value and considered that the misuse of the information was limited in nature, purpose and benefit. As a result, the judge considered that €25000 was the figure the parties would have negotiated had they been in the position of a willing licensor and willing licensee acting reasonable as at the date of the breach of confidence.

<sup>19</sup> This method of calculation is used regarding infringements of intellectual property rights, pursuant to Article 13(1)(b) of Directive 2004/48/EC. This Article provides for the rules on abstract calculation of damages (i.e. calculated on the basis of royalties which could have been due should a licence have existed) as an alternative to the general *damnum emergens* and *lucrum cessans* criteria.

### (B.1) Criminal law protection in national law: summary

Criminal protection of trade secrets against misappropriation differs from Member State to Member State on several levels, although almost all of them have provisions in this respect. Since there is a lack of a common/shared definition of the scope of trade secrets, the actual extent of the protection provided by states may vary depending on the aims pursued by the provisions implemented for this purpose.

Only a few Member states (i.e., Bulgaria, Ireland, Malta and U.K.) have not established any specific criminal framework with respect to trade secrets violations. However, even in those Member States, the conduct of the infringer may be punished under other related criminal offences (see below). In some cases, where no specific criminal provision has been implemented, penal sanctions of trade secrets misappropriation apply under unfair competition laws or commercial laws. Sweden is the only EU Member state that has implemented a specific law on trade secrets (the Swedish Act on the Protection of Trade Secrets), even though some relevant provisions are also contained in the Criminal Code<sup>20</sup>.

Table 4 below summarises the criminal provisions in force:

Table 4 – Criminal provisions applying to trade secrets misappropriation <sup>21</sup>																											
	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Criminal code	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Unfair competition commercial law	✓			✓	✓	✓	✓	✓	✓	✓	✓										✓		✓				
Specific law on trade secrets																								✓			

Comment [LHu7]: addition

Comment [LHu8]: addition

### (B.2) Differences in the conducts considered as crimes

#### (i) Unauthorised disclosure/use of trade secrets

Many of the countries seem to limit the scope of trade secrets to the information that a company has a reasonable and objective interest to keep confidential, in accordance with an objective criterion (e.g., Austria, Belgium, France, Germany, Hungary, Italy, Lithuania, Luxembourg, Netherlands, Slovakia, Spain, Sweden). Nonetheless, in some cases the relevant protection is afforded to any information having economic value that the owner deems it opportune for his benefit to keep secret according to a subjective criterion and that are subject to reasonable measures for protection of confidentiality (e.g., this broader interpretation seems to be prevailing in Czech Republic, Finland, Greece, Poland, Romania and Slovenia).

- In Austria the offender to be held criminally liable for trade secrets violations must have acted at least with conditional intent. In Belgium, Estonia, ~~Finland~~, France the conduct may be punished even if the offender acted with negligence.
- Cyprus does not establish any specific requirement that the offender must meet to be charged with criminal liability for trade secret violations. Nor is there any stated obligation on the claimant to keep information confidential.
- In the Czech Republic the offender must act deliberately to commit the offence. As the relevant conduct is defined as an act of unfair competition, the offender must qualify as a competitor or someone participating in the competitive process. The

Comment [LHu9]: deletion

<sup>20</sup> In particular, the Act on the Swedish Protection of Trade Secrets establishes two different offences: business espionage and the unauthorized dealing with trade secrets. Other complimentary or more general offences, such as, for instance, unauthorized access to computer systems or breach of faith against principal are regulated under the Criminal Code.

<sup>21</sup> Baker & McKenzie study.

concept of competition has nevertheless been construed very broadly, including even indirect or potential competitors.

- In Denmark the offences provided for under the Criminal Code require intent. Only upon certain circumstances if the employee causes a substantial risk of dissemination of confidential information by negligence he or she may be charged with criminal liability pursuant to Section 19 of the Marketing Practices Act. without having acted with intent.

Germany requires that the infringer acts with intent and, specifically, for the purpose of competition, for personal gain, for benefit of a third party or causing damage to the owner of the secret.

Formatted: Tired 0

- Finland requires that the infringer acts intentionally and in order to obtain financial benefit for himself or herself or another, or to injure another, unlawfully discloses the business secret of another or unlawfully utilises such a business secret.

Formatted: Bullets and Numbering

Comment [LHu10]: addition

- In Greece the offender must act (with intent) for purpose of competition, that means that two criteria have to be met: (i) the conduct of the offender must be suitable to serve the purpose of competition; (ii) he or she must act with the "intention of competition", i.e. enhance his or third parties' competitiveness.
- As to Hungary and Italy, the offender may be punished only if he or she acts with intent.
- In Latvia the employer is obliged to identify in writing the information considered to be commercial secrets. In any case, the offender requires the offender to have acted for use or disclosure by himself or another person, therefore intent is required for the offence to occur.
- Lithuania requires that the offender, in case of business espionage, acted with the intent to unlawfully obtain a trade secret, whereas, in the case of violation of trade secrets, with the intent to get a financial gain or to injure the owner by the disclosure to third parties or the use of the information.

As almost all EU Member states require that the offender acted with intent, it emerges that whoever commits a trade secrets infringement must have clearly the knowledge that the business information constituted trade secrets, even if there is no express obligation to keep such information confidential.

- In Luxembourg, Netherlands and Portugal the offender must act with the intent to reach a competitive advantage or to cause harm to the owner.
- Also Poland requires intent, as the offender must breach an obligation of confidentiality that must be prior established by the owner of the secret, either directly or indirectly.
- Under Romanian and Slovak law the offender must act with intent, but no specific purpose is required.
- The same applies in Slovenia, where if the conduct reaches certain outcome, the offender may be charged with the more severe correspondent penalties.
- Spain also requires intent, even if the purposes to be pursued vary depending on the type of offence considered (for instance, commercial advantage).

- The Swedish Act on the Protection of Trade Secret does not pose any requirement as to the purpose that the offender acts for. It only requires that he acted wilfully and without authorization.

*(ii) Related offences*

In Belgium a person who commits the offence under Section 309 of Criminal Code (unauthorized disclosure of trade secrets) may also be charged with theft or misappropriation (provided that he qualifies as an employee with the company). Similarly, Section 491 applies when a person is entrusted as a data processor/handler manufacturing secrets that are physically stored breaches his duty of confidence.

In Bulgaria, for instance, the offence of business bribery is punishable and applicable to, any individual who discloses to third parties information that he knows in return for something.

In France there is a wide range of crimes that may arise in connection to trade secrets violations:

- First, the offence of theft may occur when the conduct at stake consists in the fraudulent appropriation of third parties' data carriers containing confidential information. Such an offence has been found by the Court of cassation to apply even in connection to disclosure of trade secrets. Theft is punished by imprisonment up to three years and a fine of Euro 45,000.00.
- Additionally, the offence of breach of trust may be committed where an individual with the company misappropriates documents containing confidential information entrusted to them for temporary use. In such a case, the offender shall be punished by imprisonment up to three years or a fine of Euro 375,000.00.
- Also, other provisions of the Criminal Code punish the act of supplying secret information to foreign powers by imprisonment up to fifteen years and a fine of Euro 225,000.00.

In Germany cases of industrial espionage may result in theft or misappropriation.

In Greece the infringement of trade secret may constitute, among other offences, a breach of trust under Section 390 of the Criminal Code. In such a case, the offender shall be punished by imprisonment up to ten years and a fine up to Euro 15,000.00.

Depending on the circumstances, violations of trade secrets may result, further to civil lawsuits, in a number of offences, including but not limited to insider trading, unauthorized access to computer systems and a breach of privacy.

As to Italy, the conduct of the offender who commits an unauthorized use or disclosure of trade secrets may also constitute theft or misappropriation.

In Latvia acts of unauthorized disclosure or acquisition of trade secrets may constitute unfair competition practices where repeated within a one-year period and, thus, result in a punishment by imprisonment of up to two years and a fine, in addition to disqualification penalties.

Violations of trade secrets may constitute fraud or bribery in Lithuania or theft in Luxembourg. In Netherlands the conducts may also result in the theft of secret documents or hacking of computer systems. In Portugal the related offences include computer and communications fraud. Slovakia, in addition to breach of trade secrets, criminalizes the misuse of participation in economic competition through unfair acts.

In Slovenia the same act may be punished under the crime of “disclosure of and unauthorized access to trade secrets” as well as, for instance, the offence of abuse of insider information. Spain provides an extensive regulation of trade secrets infringements: however, pursuant to Section 278.3 of the Criminal Code the specific provisions apply without prejudice to the penalties that may arise for appropriating or destroying the computer media, i.e. for the offences of theft or misappropriation.

In Sweden, further to the offences provided for under the act on the Protection of Trade Secrets, other criminal provisions may apply, including unauthorized access to computer systems, unlawful dispossession, unlawful use, espionage, unlawful dealing with secret information and negligent dealing with confidential information.

Offences in any way related to trade secrets violations have significant importance in the legal systems that do not establish any specific provision in this respect:

- In Bulgaria violations of trade secrets may be punished only indirectly. The relevant offences in this respect include the disclosure of service/office secrets, the business bribe and computer crimes.
- Under Irish law, for instance, trade secrets infringements may result in: (i) disclosure of personal data obtained without authority; (ii) unauthorised accessing of data; (iii) unlawful use of a computer; (iv) theft or (v) criminal infringements of intellectual property rights.
- Under Maltese criminal law, in the absence of provisions specifically concerning trade secrets, one could be charged with misappropriation and fraudulent gains as a result of his conduct.
- In the U.K. the criminal provisions that may apply in connection to trade secrets infringement cases include theft, fraud, conspiracy to defraud as well as, upon certain circumstances, some of the offences provided for under the Computer Misuse Act (such as unauthorized access to information contained on a computer) and the Data Protection Act (although it is very unlikely that personal data qualify as trade secrets).

### (iii) Qualified offences

Certain Member States also establish qualified offences when the revelation or use of confidential information is committed by a person acting in a particular capacity (e.g., as civil servant, public official, or as person handling confidential information by reason of his job, e.g. lawyers, officers). Please note that this does not mean that for each of the offences a specific provision is established. Separate provisions may have been implemented (e.g. Italy) or, like in Estonia, the same provision may apply to professional and official secrets, also covering trade secrets. See Table 5:

Table 5 – Qualified offences <sup>22</sup>																											
	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Breach of professional secrecy	✓	✓	✓					✓	✓						✓				✓	✓		✓	✓	✓	✓	✓	
Breach of official secret	✓		✓	✓				✓	✓		✓				✓							✓	✓				
Other breach of confidence									✓					✓													
Separate provisions	Y	Y	N	N	N/A		N/A	N	N		Y	N		Y	N				N/A	N		Y	Y			N	

### (iv) Threshold for the applicability of criminal penalties

In the Czech Republic only violations resulting in a damage of at least Euro 2,000.00 may give rise to criminal liability. The offender must cause harm to a competitor or a consumer equivalent to such an amount or provide someone else than the owner of the secret with a benefit of the same amount. The offender does not necessarily need to be a legal person or an enterprise.

A *de minimis* threshold applies in Lithuania, where for the offender to be prosecuted it is required that the conduct caused a damage of at least EUR 5,648.00.

Something like a *de minimis* threshold is established in Poland, where the conduct must have caused substantial damage to the owner, although no quantification of this concept is provided for in the law.

Slovakia establishes that for the offender to be prosecuted a significant damage (more than EUR 26,600.00) must be caused by his conduct to another competitor. It also provides for a more severe penalty in cases where the conduct causes a large scale damage (over EUR 133,000.00).

Also under Estonian and Finnish criminal law a general safe harbor clause applies, preventing prosecution in case the offence is found to be of minor harm.

Comment [LHu11]: deletion

In Austria the offender will not be prosecuted if his conduct is justified by a compelling public or private interest.

No safe harbor seems to exist in Latvia and Sweden. In Cyprus disclosure of trade secrets is allowed, for instance, when protection of health and safety of citizens is affected, i.e. where compelling public interests are at stake or to prove the violations of statutory provisions.

Similarly, no safe harbor or *de minimis* threshold applies in Denmark, Finland, Italy, Luxembourg, Slovenia. Germany does not provide for any safe harbor; however, disclosure of trade secrets is justified when committed to avert an imminent danger to life, limb, freedom, honour, property or other prevailing legal interests. In Greece trade secrets are not protected in case a witness is examined to represent certain circumstances before the Court, excluding state secrets. In Hungary Section 300(2) of Criminal Code expressly sets forth some safe harbors that justify infringement of trade secrets. These clauses include:

- (i) fulfilment of duties prescribed in a separate act governing the publication of information and information to be disclosed in the public interest;
- (ii) fulfilment of duties subject to statutory reporting obligations, even in the case the report was filed in good faith and proved to be unfounded.

In the Netherlands a specific provision sets out an exemption for those who disclosed in good faith a trade secret assuming that the disclosure was in the public interest. Portugal and Romania consider the consent of the owner to the disclosure of a secret as a safe harbor clause. In addition to that, Romanian law permits the disclosure of trade secrets where compelling public interests are at stake. Spain does not consider information about illegal activities carried out by the owner to be a trade secret: therefore, its revelation would not determine any prosecution.

Generally speaking, the risk of dissemination of confidential information does not amount to a criminal offence (except for Slovakia, Slovenia). The conduct carried out by the infringer must result in an actual violation of the interest protected under the relevant provisions. In contrast, most legal systems (including Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Italy, Latvia, Lithuania, Slovakia, Slovenia) provide criminal protection against the intent to commit a trade secret violation. The acts carried out with the

purpose of disclosing or using confidential business information which reach a certain threshold in the realisation of the offence are likely to trigger criminal liability.

### (B.3) Differences in the penalties

The conducts which normally give rise to violations of trade secrets include the access to confidential information, the use or the disclosure thereof or the illicit acquisition for exploitation by the offender or third parties. These conducts are generally punished regardless of the fact that the offender qualifies as a competitor and may be committed either by (past) employees of the company or by external persons (such as consultants, contractors, agents).

It is quite frequent, however, that the violation of trade secrets committed by an employee of the company owning the confidential business information results in a more severe punishment than that provided for the same offence in other cases (i.e., in Belgium, Germany, Greece and Spain).

Table 6 below provides a summary of the main conducts concerning trade secrets violation and the related punishment provided for under the legal systems.

**Table 6 – Criminal penalties applying to trade secrets misappropriation<sup>23</sup>**

Country	Offender	Conduct	Penalties
Austria	Whoever	Disclosure or exploitation of trade or business secrets	Up to six months imprisonment; up to one year if the conduct is committed with the purpose to obtain a pecuniary advantage or to cause harm to the owner or monetary penalties
		Spying out trade or business secrets for their exploitation by somebody else or disclosure	Up to two years imprisonment OR monetary penalties
		Spying out trade or business secrets for their exploitation abroad	Up to three years imprisonment AND monetary penalties
Belgium	Whoever	Communicating in bad faith manufacturing secrets appropriated during the (past) employment with the owner	From three months up to three years imprisonment AND monetary fine from Euro 50 to 2,000.00
Bulgaria		There is no specific criminal provision concerning violation of trade secrets. However, depending on the characteristics of the conduct, the offender may be charged with more general offences, such as business bribe or computer crimes	
Cyprus	Whoever	Disclosure of trade secrets	Imprisonment up to one year OR monetary fine up to Euro 1,275.00
		Disclosure of information protected by professional secrecy involving trade secrets	Imprisonment up to six months AND/OR monetary fine up to Euro 1,700.00
Czech Republic	Whoever	Acts of unfair competition infringing trade secrets and causing damage in or in excess of Euro 2,000.00 to other competitors/consumers or providing someone with unjustified benefit in the same or greater amount	Monetary fine up to Euro 1.5 Million*
Denmark	Whoever	Unauthorized misuse or appropriation of trade secrets	Imprisonment up to 1 year and 6 months OR monetary fine
		Serious violations such as appropriation of trade secrets in a contract of service or in the performance of assignments	Imprisonment up to six years
Estonia	Whoever	Unauthorized disclosure or use of business secret learned by reason of the professional or official duties with the purpose of causing damage	Imprisonment up to one year OR monetary fine
Finland	Whoever	Violation of a business secret: Disclosure or use of trade secrets known by reason of the employment, position or other lawful activities to obtain financial benefit or to injure the owner	Imprisonment up to two years OR monetary fine
		Misuse of trade secrets obtained or revealed through an unlawful act	Imprisonment up to two years OR monetary fine
		Business espionage: Unlawfully obtaining information regarding trade secrets	Imprisonment up to two years OR monetary fine
France	Whoever	Revelation of manufacturing secrets	Imprisonment up to two years AND

Comment [LHu12]: addition



			monetary fine of Euro 30,000.00
		Theft (for instance, of carriers or materials containing trade secrets)	Imprisonment up to three years AND monetary fine of Euro 45,000.00
Germany	Employees	Unauthorized communication of trade or business secrets that the offender was granted access to for the purpose of obtaining financial advantage or injuring the owner	Imprisonment up to three years OR monetary fine
	Whoever	Unauthorized acquiring or securing trade or business secrets or using thereof	Imprisonment up to three years OR monetary fine. Imprisonment up to five years if aggravating circumstances occur
Greece	Whoever	Copying, printing, using, disclosing or in any way violating data or computer programs constituting secrets of an enterprise	Imprisonment from three months up to one year. Imprisonment from one year to five years if the offender is in the service of the owner and the secrets are of great financial significance
	Employees	Unauthorized communication to third parties of secrets that the offender has known by reason of his employment to obtain financial advantage or to cause a damage to the owner; Unauthorized use of the information so obtained	Imprisonment up to six months AND monetary fine up to Euro 8.80
Hungary	Whoever	Making available to unauthorized persons secrets for financial advantage or to cause damage to others; Using the secrets so obtained	Imprisonment up to three years
Ireland	Not applicable		
Italy	Whoever	Disclosure or use of any information concerning scientific discoveries or inventions or industrial applications that is intended to remain secret known by the offender by reason of his status, function, job or art, to obtain a profit	Imprisonment up to two years
Latvia	Whoever	Revelation of non-disclosable information other than a state secret; Unauthorized acquisition and disclosure of commercial secrets	Imprisonment up to five years OR monetary fine
Lithuania	Whoever	Unlawful acquisition of commercial secrets or communication to third persons; Disclosure of information that the offender was entrusted with by reason of his employment	Imprisonment up to two years AND/OR disqualification penalties
Luxembourg	Employees	Use or disclosure, during the employment or within two years after its expiration, trade or manufacturing secrets known by reason of the job to obtain financial advantage or to cause damage to the owner	Imprisonment from three months to three years AND monetary fine from Euro 251 to 12,500.00
Malta	Not applicable		
Netherlands	Employee	Intentional disclosure of confidential information that may harm the owner	Imprisonment up to six months AND/OR monetary fine up to Euro 19,500.00
Poland	Whoever	Disclosure or exploitation of trade secret in breach of confidential duties that causes substantial damage to the owner; Use of information illegally acquired or disclosure to third persons	Imprisonment from one month to two years AND monetary fine up to Euro 260,000.00*
Portugal	Whoever	Use or disclosure to third parties of secrets that the offender knows by reason of his status, job, profession or art	Imprisonment up to one year OR monetary fine
Romania	Whoever	Disclosure, acquisition or use of trade secrets without the consent of the owner, as a result of an action of commercial or industrial espionage	Imprisonment from six months up to two years OR monetary fine from Euro 570 to 5,000.00*
		Disclosure of data or information not intended to be publicly known by a person who knows it by reason of his employment, provided that the offence is likely to cause damages	Imprisonment from two up to seven years; Imprisonment from six months to five years if the disclosure is made by another person
Slovakia	Whoever	Spying out trade secrets with the intention to disclose them to unauthorized persons	Imprisonment from six months up to three years; Imprisonment from seven to twelve years if aggravating circumstances occur
Slovenia	Whoever	Disclosure of trade secrets; Providing unauthorized third parties with access to trade secrets; Collection of trade secrets with the purpose of delivering them to unauthorized persons; Unlawful obtainment of trade secrets with the purpose of delivering them to unauthorized persons	Imprisonment up to three years; Imprisonment up to five years if the information is of particular importance
Spain	Whoever	Acquiring data, documents, media and other objects to discover trade secrets; Disclosure, revelation or communication to third parties of the discovered information	Imprisonment from two up to four years AND monetary fine; Imprisonment from three to five years AND monetary fine in case the secrets are disclosed

		Diffusion, disclosure or communication of trade secrets in breach of duties of confidentiality	Imprisonment from two up to four years AND monetary fine, in case the information is disclosed in breach of confidentiality
Sweden	Whoever	Unauthorized access of trade secrets as business espionage	Imprisonment up to two years OR monetary fine; Imprisonment up to six years in case of information of significant importance
		Acquiring trade secrets knowing that the person who made it available accessed the trade secret through acts of business espionage	Imprisonment up to two years OR monetary fine; Imprisonment up to four years in case of information of significant importance
U.K.	Not applicable		

\* Monetary penalties are expressed in local currency and converted to Euro for the reader's convenience

Generally, punishment of the offender is by imprisonment, even though he or she may also be charged, either in addition to that or alternatively, with monetary penalties: see Table 7 with penalties that shall apply for the main offence (for instance, unauthorized disclosure/use of trade secrets).

**Table 7 – Penalties<sup>24</sup>**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Imprisonment OR monetary penalties	✓			✓		✓	✓	✓		✓	✓							✓				✓	✓	✓			
Imprisonment AND monetary penalties		✓								✓	✓		✓					✓			✓	✓					
Imprisonment ONLY														✓		✓	✓									✓	✓
Monetary penalties ONLY					✓																						
Other penalties					✓											✓							✓				

Hungary, Italy, Lithuania, Slovakia and Slovenia only provide for the imprisonment of the offender whereas in Czech Republic only monetary penalties and, where possible, forfeiture of property shall apply. Lithuania, as well as Romania, also provide for disqualification penalties in addition to imprisonment, such as deprivation of the right to be employed in certain positions or to engage in certain activities. This is a very significant solution, as it directly impacts on the opportunity for the offender to be entrusted with certain responsibilities in his future employment.

With respect to the extent of punishment, the Czech Republic is the state where the heaviest fines apply: under Czech law, the infringer shall be punished with a fine up to 1.5 Million Euro. In contrast, Czech law does not provide for imprisonment in case of trade secrets violations.

In most of states trade secrets infringements are punished with imprisonment up to a term of two-three years. There are a few exceptions: in Denmark the offender may be charged with up to six years imprisonment, provided that serious violations have taken place; in Slovenia imprisonment may be up to five years when the acts carried out by the offender concerns information of particular importance. Under the Swedish Act on the Protection of Trade Secrets, terms of imprisonment of up to six years are foreseen for cases of business espionage and up to four years for the unlawful acquisition of trade secrets of significant importance.

### (C) THE SPECIFIC CASE OF IMPORTS OF GOODS INTO THE EU

In the specific case of goods imported from third countries which would have been manufactured using misappropriated trade secrets of EU companies, there is no specific administrative procedure before customs authorities to block them.

The EU Regulation on customs enforcement of intellectual property rights<sup>25</sup> provides for such administrative customs procedures<sup>26</sup>: the holder of an intellectual property right can ask customs authorities to block imports of goods infringing and intellectual property right. Once the imports blocked, the holder of the intellectual property right has to file a case before a civil court which will decide on the existence (or not) of the infringement. However, this EU rules only applies as regards formal intellectual property rights and do not extent to trade secrets misappropriation claims<sup>27</sup>. Hence, national customs authorities do not process claims for misappropriation of trade secrets.

This situation differs from that in the United States. In the United States, it is possible to engage administrative proceedings before the US International Trade Commission (ITC) in order to block imported goods manufactured using misappropriated trade secrets<sup>28</sup>. Section 337 of the Tariffs Act<sup>29</sup> gives power to the US ITC to deal with claims involving infringements of intellectual property rights but also other forms of unfair competition involving imported products, such as misappropriation of trade secrets. The US ITC has investigative powers. The procedure includes trial proceedings before administrative law judges and review by the US ITC. In terms of remedies, the primary remedy available in Section 337 investigations is an exclusion order that directs US Customs to stop infringing goods from entering the US. In addition, the US ITC may issue cease and desist orders against named importers and other persons engaged in unfair acts that violate Section 337.

Therefore, in order to block goods imported from third countries which would have been manufactured using misappropriated trade secrets of EU companies, the EU owner of the trade secrets in question would need to first go to court in order to have the misappropriation of the trade secrets declared and to obtain an injunction against the third party in question which could be enforced by customs authorities. Compared to formal intellectual property rights, there is therefore an inversion of the burden of proof.

#### **(D) THE PROCEDURAL RULES BEFORE NATIONAL COURTS**

Procedural rules in national law are not always adapted to litigation in trade secrets. Secrecy of information is often at risk during civil proceedings and the absence of protection from (further) disclosure of information as a consequence of court proceedings is a considerable deterrent from starting a legal action<sup>30</sup>.

##### ***(D.1) The insufficient protection of confidential information in national proceedings***

<sup>25</sup> Regulation (EC) No 1383/2003 of 22 July 2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights, OJ L 196, 2.8.2003, p.7. The Commission made a proposal in 2011 for a new Regulation concerning customs enforcement of intellectual property rights (COM(2011)285). Negotiations on this text before the European Parliament and the Council are on-going.

<sup>26</sup> Indeed, administrative customs procedures of this type would be a matter of EU law.

<sup>27</sup> Unless of course the claim encompasses both an intellectual property right infringement (e.g. a patent) as well as a trade secrets misappropriation claim.

<sup>28</sup> See generally [http://www.usitc.gov/intellectual\\_property/](http://www.usitc.gov/intellectual_property/)

<sup>29</sup> For the text of Section 337 of the Tariffs Act, see:

<sup>30</sup> [http://www.usitc.gov/intellectual\\_property/documents/statute.pdf](http://www.usitc.gov/intellectual_property/documents/statute.pdf)

Baker & McKenzie study.

When litigating to defend a trade secret, these procedural rules can result in disclosure of confidential information to the other party or to the public. There are three main situations.

(1) The need to describe the misappropriated trade secret in the application, so that the judge can understand it, could imply that, if the plaintiff does not know the extent of the information misappropriated by the defendant, he could disclose to the defendant (since the application is served to him) more confidential information than actually needed to defend his case<sup>31</sup>.

(2) The general rules on the production of evidence could also have the effect of having to disclose information otherwise considered confidential. In common law countries, the pre-trial duty of (full) discovery rules applies; in continental countries, the defendant may ask for certain documents/evidence to be presented by the other party when such evidence lies in the control of that party – which could imply further disclosure of trade secrets. It should be noted that this plays both ways: bad faith plaintiffs could try this way (and therefore abusing the litigation rules) to obtain confidential information from defendants<sup>32</sup>.

(3) The inherent publicity of judicial proceedings (civil proceedings in all EU Member States are public) could also result in the disclosure of trade secrets, in this case to the public:

- Firstly, hearings are often public. While national procedural laws normally include general provisions which allow Courts to exclude the public from the hearing for reasons relating to security, public order and decency, there do not necessarily apply to trade secrets litigation. In some EU Member States (notably Bulgaria<sup>33</sup>, Estonia<sup>34</sup>, Hungary<sup>35</sup>, Germany<sup>36</sup>, The Netherlands, Poland, Romania, Slovakia, Slovenia), a party has the right to request the court to order that the entire proceeding or a part thereof be heard in private to preserve the secrecy of the trade secret. However, according to Baker & McKenzie (2013), this seems to rarely happen in practice and there would be no case law on this point<sup>37</sup>. In the United Kingdom the parties may agree or apply to the Court to ensure that certain information to be revealed during the pre-trial disclosure procedure remains confidential. The parties may enter into a contractual agreement whereby the parties agree that certain information may remain confidential or only be disclosed to legal counsel or where the parties do not reach

<sup>31</sup> See for instance, Hogan Lovells (2012), §57 regarding Belgium, at p.12.

<sup>32</sup> General procedural rules will normally allow the defendant to refuse to provide a document if it includes a trade secret or a confidential information of the defendant.

<sup>33</sup> In Bulgaria private hearing is specifically provided for cases related to “protection of trade, manufacturing, invention or tax-related secrets” if public disclosure may impair a party’s legitimate interest. When publicity is precluded, only the parties, their attorneys, experts and witnesses are allowed to enter into the court room and are subject to a statutory obligation not to disclose subject matter and content of the relevant proceeding (breach of such obligation entails liability for compensation).

<sup>34</sup> In Estonia (similarly in Finland and Lithuania), in-camera examination can be ordered for the protection of trade secrets if the interest in a public hearing is not deemed to be greater than the commercial interest in protecting the secret.

<sup>35</sup> In Hungary, when the Court orders in-camera examination, the parties are also prohibited from making copies of the minutes of the hearing or of any document containing a trade secret. Examination of documents containing trade secrets is subject to a declaration of non-disclosure and special review procedures are established by the Judge.

<sup>36</sup> In Germany, besides the exclusion of the public if trade secrets are to be discussed, legal practice has developed the so called “Düsseldorf Procedure” (originally developed for patent law claims but likely applicable to trade secrets cases), which consists in a procedure where Courts order independent proceedings for the preservation of evidence as an interim injunction handed to the defendant together with the statement of claims so that there is no chance to destroy evidence. Evidence is then examined exclusively by authorized experts and attorneys bound to confidentiality. The parties do not have access to the confidential information.

<sup>37</sup> Baker & McKenzie (2013) study.

such agreement, a party may unilaterally apply to the Court requesting that confidential information is not disclosed to the other party during the proceeding. Requests for restriction of disclosure are at the discretion of the Court.

- Judicial decisions may describe the misappropriated trade secret in question when explaining the reasons for the decision<sup>38</sup>; and in some countries other judicial documents (including applications) may be accessed by third parties. According to Baker & McKenzie (2013), in most countries, pleadings and in general court documents are public and potentially accessible by anyone. Courts have a general duty to adopt adequate measures to safeguard the secret information of a party, for example, by restricting access to those documents which contain trade secrets only to the other party's attorney or to the court's expert (in certain cases the confidential information can be put under closed seals), or not disclosing certain information in the court's final decision (by blanking out the relevant information in the decision and other court's documents). However, according to that study, such measures have proved to be of limited effect to prevent the actual leak of confidential information during proceedings<sup>39</sup>.

#### ***(D.2) The example of antitrust proceedings protecting confidential information***

There are specific rules protecting secrecy of confidential information during antitrust proceedings in the Member States. All of them have measures aimed at protecting business secrets/confidential information from being disclosed during proceedings before national competition authorities, even if the procedural steps needed to obtain protection of secret information varies, to a certain extent, from jurisdiction to jurisdiction. In particular, the involved undertakings have the right to indicate the information that, in their opinion, shall not be divulged<sup>40</sup>. Similar provisions exist at EU level for the antitrust proceedings before the European Commission.

#### **(E) THE SPECIFIC CASE OF TRADE SECRETS WHICH ARE DISCLOSED TO PUBLIC AUTHORITIES PURSUANT TO REGULATORY OBLIGATIONS: EU RULES**

Several EU rules are addressing the specific case of trade secrets which are disclosed to public authorities – normally because of regulatory obligations.

##### ***(E.1) The protection of confidential information in public procurement cases***

Industry often expresses the fear that valuable confidential information (i.e. a trade secret) which is disclosed to a public authorities as part of a tender procedure for public procurement could not be sufficiently protected against misappropriation.

This concern is addressed by EU legislation. Current EU rules provide for protection in this regard: "*Without prejudice to the provisions of this Directive, in particular those concerning the obligations relating to the advertising of awarded contracts and to the information to candidates and tenderers [...] the contracting authority shall not disclose information forwarded to it by economic operators which they have designated as confidential; such*

<sup>38</sup> See for instance, Hogan Lovells (2012), §57 regarding Belgium, at p.12.

<sup>39</sup> Baker & McKenzie study.

<sup>40</sup> According to Baker & McKenzie (2013), however, the secrecy of information may not be sufficient to prevent disclosure when such information is relevant to prove the infringement or for the right of defence of the parties (Bulgaria, Estonia, Germany, Greece, Italy, Luxembourg, Portugal). See Baker & McKenzie study.

information includes, in particular technical or trade secrets and the confidential aspects of tenders."<sup>41</sup>

This protection is also integrated in the 2011 Commission proposal for a new directive on public procurement<sup>42</sup>:

- Article 18 of that proposal<sup>43</sup> requires the contracting authority not to disclose information forwarded to it by economic operators which they have designated as confidential, including, but not limited to, technical or trade secrets and the confidential aspects of tenders. In addition, Article 19(2) of the proposal requires the contracting authorities to ensure, in all communication, exchange and storage of information, that the integrity of data and the confidentiality of tenders are preserved.
- Other provisions in the proposal also require the contracting authorities not to reveal to the other participants in the tender solutions proposed or other confidential information communicated by a candidate participating in the "competitive procedure with negotiation"<sup>44</sup> or in the "competitive dialogue"<sup>45</sup> without its agreement. Such agreement shall not take the form of a general waiver but shall be given with reference to the intended communication of specific solutions or other specific confidential information

The underlying rationale was explained by an English Court of Appeal judge as follows: "...it is plain that there is a strong public interest in the maintenance of valuable commercial confidential information ... If the penalty for contracting with public authorities were to be the potential loss of such confidential information, then public authorities and the public interest would be the losers, and the result would be potentially anticompetitive."<sup>46</sup>

**(E.2) The protection of confidentiality of trade secrets disclosed to EU institutions and agencies**

EU institutions have a general policy of transparency and allow third parties to access to the documents they hold, under certain conditions. Given that businesses may disclose confidential business information to EU institutions in the context of specific procedures (e.g. a complaint against a Member State for failure to apply EU law etc) the risk exists that such confidential business information could be disclosed to a third party. This issue is of particular importance when businesses transfer trade secrets to EU regulatory agencies, such

<sup>41</sup> Article 6 of Directive 2004/18/EC of the European Parliament and the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts.

<sup>42</sup> Commission proposal for a Directive of the European Parliament and of the Council on public procurement, COM(2011) 896 final, Brussels, 20.12.2011. Negotiations before the European Parliament and the Council are on-going.

<sup>43</sup> "Article 18  
Confidentiality

1. Unless otherwise provided in this Directive or in the national law concerning access to information, and without prejudice to the obligations relating to the advertising of awarded contracts and to the information to candidates and tenderers set out in Articles 48 and 53 of this Directive, the contracting authority shall not disclose information forwarded to it by economic operators which they have designated as confidential, including, but not limited to, technical or trade secrets and the confidential aspects of tenders.

2. Contracting authorities may impose on economic operators requirements aimed at protecting the confidential nature of information which the contracting authorities make available throughout the procurement procedure."

<sup>44</sup> Cf. Article 27(4) of the proposal.

<sup>45</sup> Cf. Article 28(3) of the proposal.

<sup>46</sup> Veolia vs. Nottinghamshire CC [2010] EWCA 1214 per Rix LJ.

as the European Medicines Agency, the European Chemical Agency or the three European financial authorities.

This concern has been considered when adopting the EU general rules<sup>47</sup> dealing with access to documents held by a European institution. Regulation (EC) No 1049/2001<sup>48</sup> provides for the protection of business secrets when the information has been forwarded to a EU institution or body. Article 4(2) states in particular that *"the institutions shall refuse access to a document where disclosure would undermine the protection of the commercial interests of a natural or legal person, including intellectual property"*).

EU rules also provide for professional secrecy obligations for their staff. In the case of the EU regulatory agencies, they are under the obligation of professional secrecy and respect of confidentiality of the information when cooperating with other authorities<sup>49</sup>.

***(E.3) The protection of confidentiality of trade secrets disclosed to national supervisory/regulatory agencies***

EU rules also deal with the preservation of confidentiality of information (including business secrets) by national regulatory authorities<sup>50</sup>.

***(E.4) Rules on the non-disclosure of trade secrets to supervisory/regulatory authorities by intermediaries***

Financial intermediaries and some regulated professionals (e.g. lawyers, auditors) often know trade secrets owned by their customers. This is why (inter alia) they are subject to professional secrecy rules, which is a guarantee to their customers.

<sup>47</sup> There are specific rules for the access to file in competition cases, see above.

<sup>48</sup> Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. OJ L 145, 31.5.2001, p. 43

<sup>49</sup> See for instance Article 70 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), OJ L 331, 15.10.2010, p. 12.

"[...]

2.

*Without prejudice to cases covered by criminal law, any confidential information received by persons referred to in paragraph 1 whilst performing their duties may not be divulged to any person or authority whatsoever, except in summary or aggregate form, such that individual financial institutions cannot be identified.*

*Moreover, the obligation under paragraph 1 and the first subparagraph of this paragraph shall not prevent the Authority and the national supervisory authorities from using the information for the enforcement of the acts referred to in Article 1(2), and in particular for legal procedures for the adoption of decisions.*

3.

*Paragraphs 1 and 2 shall not prevent the Authority from exchanging information with national supervisory authorities in accordance with this Regulation and other Union legislation applicable to financial institutions.*

*That information shall be subject to the conditions of professional secrecy referred to in paragraphs 1 and 2. The Authority shall lay down in its internal rules of procedure the practical arrangements for implementing the confidentiality rules referred to in paragraphs 1 and 2."*

Recital 62 of that Regulation says:

*"It is essential that business secrets and other confidential information be protected. The confidentiality of information made available to the Authority and exchanged in the network should be subject to stringent and effective confidentiality rules."*

<sup>50</sup> See for instance Article 25 of Directive 2004/109/EC of the European Parliament and of the Council of 15 December 2004 on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC, OJ L 390, 31.12.2004, p.38.

A specific issue may arise when public authorities require those intermediaries or regulated professionals to disclose to them, in the context of their supervisory functions, confidential information which is sensitive for their customers.

EU rules have addressed this issue and exceptions to the principle of respecting professional secrecy have been established in exceptional circumstances. For instance, the EU anti-money laundering rules<sup>51</sup> require financial intermediaries and regulated professions to disclose to specific authorities (so-called financial intelligence units) data regarding situations suspected of involve money laundering.

In other cases, EU rules underlined the need to protect the business secrets of clients. A recent Commission legislative proposal indirectly addressed the protection of business secrets in the specific circumstance where an EU auditor would be required by a third country public authority, for their supervisory purposes<sup>52</sup>, to disclose to it audit working papers containing business secrets of the audited entity. In accordance with this proposal, the EU auditor could only transfer the audit working papers to the third country authority provided that "*the protection of the commercial interests of the audited entity, including its industrial and intellectual property is not undermined*"<sup>53</sup>.

---

<sup>51</sup> Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, p.15.

<sup>52</sup> E.g. the audited entity may be an EU subsidiary of an audited entity of that third country.

<sup>53</sup> Cf. European Commission Proposal of 30 November 2011 for a Directive of the European Parliament and of the council amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts, COM(2011) 778 final. See Article 1(23), introducing a point (ba) in Article 47(2) of Directive 2006/43/EC.







PREMIER MINISTRE

Le 28 janvier 2013

## NOTE DE LA DELEGATION FRANCAISE

### OBSERVATIONS SUR LE DOCUMENT INTITULÉ “*LEGISLATIVE FRAMEWORK IN EU MEMBER STATES ON THE PROTECTION OF TRADE SECRETS AGAINST MISAPPROPRIATION*”

#### 1. Introduction générale

1. D’une part, le tableau figurant en introduction est à compléter comme suit :

*Table 1 – Main protection against trade secrets misappropriation by national law*

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK	
Trade secrets specific law																								✓				
Trade secret protection in intellectual property code												✓			✓							✓						
Unfair competition law (civil and criminal provisions)	✓				✓	✓	✓											✓			✓		✓					
Unfair competition law (civil provisions only)		✓	✓					✓		✓	✓	✓	✓				✓	✓							✓	✓		
Unfair competition law (criminal provisions only)				✓					✓													✓						
Common law (breach of confidence)														✓												✓		
Criminal law other than unfair competition	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	
Tort law		✓				✓			✓			✓			✓		✓			✓								
Contract law ONLY																				✓								
Labour law																												
	Most Member States																											

Most Member States

En effet, il convient d’ajouter, dans le tableau, la référence à la France pour :

- la protection des « secrets de fabrique » visée à l’article L. 621-1 du Code de la propriété intellectuelle (« *Trade secret protection in intellectual property code* ») ;
- pour la protection relevant de la concurrence déloyale (« *Unfair competition law (civil provisions only)* ») basée sur l’article 1382 du Code civil.

2. D’autre part, il convient également d’ajouter la référence à la France parmi les Etats prévoyant une protection des secrets d’affaire par la protection par « unfair competition (either civil or criminal provisions, or both) » ainsi que d’ajouter la référence à la France parmi les Etats prévoyant la protection par la responsabilité délictuelle en supplément de la



protection par la concurrence déloyale. Sur ce dernier point, il s'agit d'une appréciation jurisprudentielle de l'article 1382 du code civil sur la responsabilité délictuelle : la jurisprudence sanctionne la violation du secret des affaires sur ce fondement.

La partie A.1 (i) est donc à compléter comme suit :

« (A.1) Civil/commercial law protection in national law : summary

(i) summary

*Some Member States have specific provisions in their civil/commercial law providing protection against the misappropriation of trade secrets*

- *Sweden has an Act specifically directed against the misappropriation of trade secrets.*
- *In Italy and Portugal, specific provisions on the protection of trade secrets are included in their respective codes of industrial property – although this does not mean that trade secrets are intellectual property rights. **France: manufacturing secrets in the code of intellectual property***

*Other Member States have more general legislation which can be applied.*

- *Most of them deal with the issue via their law of unfair competition (either civil or criminal provisions, or both): Austria, Belgium, Bulgaria, Czech Republic, Germany, Denmark, Estonia, **France**, Greece, Spain, Finland, Hungary, Latvia, Lithuania, Poland, Romania, Slovenia, Slovakia.*
- *Tort law (or liability for non-contractual responsibility) is used in some countries, either as the main means to address trade secrets misappropriation (Luxembourg, Netherlands) or supplementing the protection offered by unfair competition law (Belgium, **France**, Greece).*

## **2. Développements relatifs au secret de fabrique (page 4)**

La partie A.1 (ii) est à modifier comme suit afin de refléter davantage le double mécanisme de l'action en concurrence déloyale et de la responsabilité délictuelle :

« FR (France) : ~~The only specific trade secrets legislation in French law is that protecting "manufacturing secrets" in the Intellectual Property Code. Other provisions of civil law (tort law) protect trade secrets more generally. The Labour Code also provides criminal liability for trade secret violations by employees or former employees. When parties are bound by a contractual obligation not to disclose secret information, an action lies for breach of contract. There are a number of references to trade secrets in French law and case law but no statutory definition of trade secrets. Trade secret owners generally rely on the unfair competition law (against competitor) and the general law of tort (against any third party) which correspond to the same reference of the French Civil Code, namely Article 1382. However the only specific trade secrets legislation is dealing with protecting "manufacturing secrets" in the Intellectual Property Code in link with the Labour Code, which provides criminal liability for trade secret violations by employees or former~~



.....

*employees. When parties are bound by a contractual obligation not to disclose secret information, an action lies for breach of contract. »*

S'agissant du secret de fabrique (article L621-1 du code de la propriété intellectuelle), la violation de ce secret est sanctionnée pénalement. La violation de ce secret doit émaner d'un salarié ou d'un directeur. Seule sa révélation est punie (ou la tentative de révélation), excluant ainsi un détournement du secret à des fins personnelles. Il faut prouver son intention frauduleuse.

En l'absence de définition légale du secret de fabrique, la jurisprudence a précisé les contours de cette notion : le procédé de fabrication en cause doit être mis en œuvre par un industriel, être original, offrir un intérêt pratique et commercial, et avoir été gardé secret à l'égard des concurrents.

### ***3. Définition du secret des affaires (partie A.2) Differencies in the scope of protection : the trade secret and the misappropriation***

En France, si la notion de secret des affaires est fréquemment employée dans des textes législatifs et réglementaires éparses, et par la jurisprudence, elle n'est pourtant pas définie.

Le seul texte comportant une précision – par la négative – sur les documents couverts par le secret des affaires est l'article R463-14 du Code de Commerce, dans le cadre des règles régissant la procédure devant l'Autorité de la concurrence<sup>1</sup> :

« Les informations, documents ou parties de documents pour lesquels une demande de protection au titre du secret des affaires n'a pas été présentée sont réputés ne pas mettre en jeu le secret des affaires. Il en est de même des éléments portant sur les ventes, parts de marché, offres ou données similaires de plus de cinq ans au moment où il est statué sur la demande, sauf si, dans des cas exceptionnels, le rapporteur général en décide autrement. »

La seule définition du secret des affaires émanant d'une autorité officielle est celle de la Commission d'Accès aux Documents Administratifs (CADA).

La loi n°78-753 du 17 juillet 1978 portant diverses mesures d'aménagement des relations entre l'administration et le public dispose que les autorités sont tenues de communiquer les documents administratifs aux personnes qui en font la demande sous réserve de la liste des documents qui ne sont communicables qu'à l'intéressé (II) et notamment ceux dont la communication porterait atteinte à la protection de la vie privée, au secret médical et au secret en matière commerciale et industrielle.

Dans un avis n°20062458, du 15 juin 2006, la CADA a précisé que le secret en matière industrielle et commerciale couvrait trois types de mentions :

- « Les mentions protégées par le secret des procédés, qui recouvre les techniques de fabrication telle que la description des matériels utilisés et du personnel employé ;

---

<sup>1</sup> devant l'Autorité de la Concurrence, en application des articles L.463-4 et R.463-4 du Code de Commerce, une partie peut former une demande de protection du secret des affaires impliquant l'établissement d'une version non confidentielle et d'un résumé des pièces destinés à être communiqués à l'adversaire.



- Les mentions protégées par le secret des informations économiques et financières, catégorie dans laquelle entrent les informations qui ont trait à la situation économique d'une entreprise, à sa santé financière ou à l'état de son crédit, comme par exemple, le chiffre d'affaires, les effectifs et généralement, toutes les informations de nature à révéler son niveau d'activité ;
- Les mentions protégées par le secret des stratégies commerciales, catégorie dans laquelle entrent les informations sur les prix et les pratiques commerciales telles que la liste des fournisseurs, le montant des remises consenties etc. »

La notion de secret en matière industrielle et commerciale est donc très proche de celle de secret des affaires.

On peut citer également la loi dite « loi de blocage » du 26 juillet 1968 (modifiée le 16 juillet 1980)<sup>2</sup> qui avait été adoptée pour protéger les entreprises françaises contre les actions judiciaires engagées à l'étranger et qui avaient pour effet de collecter des renseignements économiques stratégiques pour ces entreprises. Aux termes de l'article 1bis de cette loi :

*« Sous réserve des traités ou accords internationaux et des lois et règlements en vigueur, il est interdit à toute personne de demander, de rechercher ou de communiquer, par écrit, oralement ou sous toute autre forme, des documents ou renseignements d'ordre économique, commercial, industriel, financier ou technique tendant à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères ou dans le cadre de celles-ci. »*

#### **4. Mesures de réparation (partie A3) Differences in the remedies : injonctions, destruction of goods and compensation for prejudice suffered)**

Au point iv) *Damages*, le document indique : « *Loss of profits, however, is in most cases very difficult to prove, since the misappropriated information is an intangible asset. This helps explaining the often low compensation obtained* ».

En France, le préjudice est souvent difficile à établir. Ainsi, :

- dans l'affaire Valéo (TGI Versailles, 18 déc. 2007), le préjudice subi par la partie civile a été évalué à 7 000 euros ;
- voir aussi TGI Clermont-Ferrand, chambre correctionnelle, 21 juin 2010 (10 000 euros à titre de dommages et intérêts ;
- ou encore TGI Clermont-Ferrand, chambre correctionnelle, 26 septembre 2011 (rejet des demandes au titre du préjudice matériel, 3 000 euros en réparation du préjudice moral) ;
- voir toutefois TGI Nanterre, chambre correctionnelle, 10 novembre 2011 Greenpeace c/EDF (500.000 € à titre de dommages et intérêts) ;
- ou encore Cour de Cassation, chambre Criminelle, 4 mars 2008, pourvoi n° 07-84002 (100.000 euros à titre de dommages et intérêts).

<sup>2</sup> Loi n° 68-678 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.





Le tableau « *Table 3 – available damages options* » pourrait être complété pour mentionner l'allocation de dommages et intérêts en réparation du préjudice moral, en France.

<i>Table 3 – Available damages options</i>																											
	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LI	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Accruing damage ( <i>damnum emergens</i> )	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Loss of revenues ( <i>lucrum cessans</i> )	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Moral damages			✓						✓			✓			✓					✓		✓				✓	
Punitive damages													✓		✓												✓
Other monetary compensation					✓																✓						
Account of profits	✓			✓		✓		✓	✓		✓		✓	✓	✓	✓		✓		✓	✓			✓			✓
Fair royalty	✓					✓	✓		✓				✓		✓					✓							✓
Unjust enrichment		✓			✓			✓	✓	✓	✓							✓		✓	✓	✓			✓	✓	
<i>Ex aequo et bono</i> global account		✓	✓					✓			✓		✓		✓	✓	✓		✓	✓		✓	✓				
Cumulation of these options	✓	✓			✓		✓		✓	✓					✓	✓		✓	✓	✓				✓	✓	✓	

##### 5. Observations sur l'aspect penal (*partie (B.2) Differences in the conducts considered as crimes*)

S'agissant du point (i) *Unauthorised disclosure/use of trade secrets*, le document indique: "In (...) France, the conduct may be punished even if the offender acted with negligence".

Cette affirmation n'est pas tout à fait exacte dans la mesure où les dispositions du code pénal sur le fondement desquelles la violation du secret des affaires est sanctionnée en France couvrent des délits intentionnels (vol (article 311-1 du code pénal), abus de confiance (article 314-1), escroquerie (article 313-1), loi Godfrain sur les intrusions informatiques (article 323-1), livraison d'informations à une puissance étrangère de nature à porter atteinte aux intérêts fondamentaux de la nation (article 411-6)).

Seul l'article 413-10 du code pénal portant sur le secret défense prévoit que la personne dépositaire peut agir par imprudence ou négligence.

En outre, au point ii) *related offences*, il convient de modifier ce paragraphe comme suit : "Additionally, the offence of breach of trust may be committed where **an individual** misappropriates documents containing confidential information entrusted **to him** for temporary or specific use (...)".

Par ailleurs, s'agissant du point (iii) *qualified offences* : en France, des dispositions distinctes prévoient la violation du secret professionnel (article 226-13 du code pénal), ou encore la violation du secret défense (article 413-10 du même code).



Le tableau 5 est donc complété comme suit :

Table 5 – Qualified offences																											
	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Breach of professional secrecy	✓	✓		✓				✓	✓			✓			✓				✓	✓		✓	✓	✓	✓	✓	
Breach of official secret	✓		✓	✓				✓	✓			✓	✓		✓							✓	✓				
Other breach of confidence										✓				✓													
Separate provisions	Y	Y	N	N	N/A		N/A	N	N		Y	N		Y	N				N/A	N		Y	Y			N	

Enfin, concernant la partie B3.) « *differences in the penalties* » et en particulier le tableau 6 « *criminal penalties applying to trade secret misappropriation* », il convient de préciser que la violation du secret de fabrique ne concerne que le salaire ou le directeur.

Pour les autres infractions, la rédaction pourrait être précisée comme suit : “*theft (carries or materials containing trade secrets), breach of trust, imprisonment up to three years and monetary fine of euro 375.000*”.

## 6. Protection procédurale du secret des affaires (partie D) procedural rules before national courts)

### “D.1. the insufficient protection of confidential information in national proceedings”

Le rapport ne mentionne rien au regard de la protection du secret des affaires dans le cadre des procédures dites *in futurum* (article 145 du code de procédure civile) ou encore de saisie-contrefaçon. On précisera à cet égard que la Cour de Cassation juge que le secret des affaires n'est pas en soi un obstacle à l'application de l'article 145 dès lors que le juge constate que les mesures qu'il ordonne (pouvant aboutir à la révélation d'un secret des affaires) procèdent d'un motif légitime et sont nécessaires à la protection des droits de la partie qui les a sollicitées. Lorsque le juge rejette la demande, il prend non pas en compte le risque d'une violation du secret des affaires mais l'absence d'un motif légitime.

Le secret professionnel constitue quant à lui un empêchement légitime opposable.

### “D.2 ) the example of antitrust proceedings protecting confidential information”

Il convient d'ajouter la référence à la France dans la liste des pays figurant en note de bas de page n°40 dès lors qu'en application de l'article R 463-15 du code de commerce, des pièces contenant des informations relevant du secret des affaires peuvent être nécessaires à l'exercice des droits de la défense ou pour les besoins du débat devant l'Autorité de la concurrence.



998

## LEGISLATIVE FRAMEWORK IN EU MEMBER STATES ON THE PROTECTION OF TRADE SECRETS AGAINST MISAPPROPRIATION

*N.B. Unless otherwise stated, the information contained in this annex is based on: (a) the results of a study recently conducted by Hogan Lovells for the Commission on this matter (available at: [http://ec.europa.eu/internal\\_market/iprenforcement/documents/index\\_en.htm#maincontentSec2](http://ec.europa.eu/internal_market/iprenforcement/documents/index_en.htm#maincontentSec2)) and (b) the preliminary results of another study being carried out for the Commission (by Baker & McKenzie, final results expected for 1<sup>st</sup> quarter 2013).*

### INTRODUCTION

Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)<sup>1</sup> requires its signatories to protect "undisclosed information" (see Box 1).

#### **Box 1 - Article 39 of the TRIPS**

*"1. In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967)<sup>2</sup>, Members shall protect undisclosed information in accordance with paragraph 2 and the data submitted to governments or governmental agencies in accordance with paragraph 3.*

*2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices<sup>10</sup> so as long as such information:*

- (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;*
- (b) has commercial value because it is secret; and*
- (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.*

*3. Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use."*

<sup>10</sup> For the purpose of this provision, "a manner contrary to honest commercial practices" shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition.

There is no specific EU law directly dealing with the misappropriation of trade secrets by third parties (i.e. the case referred to in paragraph 2 of Article 39 of the TRIPS). Therefore, the protection of trade secrets against misappropriation by third parties is primarily addressed by national legislation.

National laws in this area provide for different types of protection. Table 1 provides an overview per country of this protection, which is explained the following sections of this Annex.

<sup>1</sup> The TRIPS is a multilateral agreement which must be joined to by all the members of the World Trade Organisation (WTO).

<sup>2</sup> Cf. The Stockholm Act of the Paris Convention for the Protection of Industrial Property, 14 July 1967.

**Table 1 – Main protection against trade secrets misappropriation by national law**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Trade secrets specific law																								✓			
Trade secret protection in intellectual property code															✓							✓					
Unfair competition law (civil and criminal provisions)	✓				✓	✓	✓											✓			✓		✓				
Unfair competition law (civil provisions only)		✓	✓					✓		✓	✓		✓			✓	✓								✓	✓	
Unfair competition law (criminal provisions only)				✓					✓													✓					
Common law (breach of confidence)														✓												✓	
Criminal law other than unfair competition	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tort law		✓				✓			✓				✓		✓		✓				✓						
Contract law ONLY																				✓							
Labour law																											
									</																		

Most Member States

However, there are EU rules concerning the treatment of confidential information submitted to public authorities pursuant to legal obligations (i.e. corresponding to the case described in paragraph 3 of Article 39 of the TRIPS). See below Section (E).

#### **(A) CIVIL/COMMERCIAL LAW<sup>3</sup>**

##### **(A.1) Civil/commercial law protection in national law: summary**

###### **(i) Summary**

All EU Member States offer some, more or less extensive, form of protection against the misappropriation of trade secrets, albeit this is achieved in different ways.

Some Member States have specific provisions in their civil/commercial law providing protection against the misappropriation of trade secrets

- Sweden has an Act specifically directed against the misappropriation of trade secrets.
- In Italy and Portugal, specific provisions on the protection of trade secrets are included in their respective codes of industrial property – although this does not mean that trade secrets are intellectual property rights.

Other Member States have more general legislation which can be applied.

- Most of them deal with the issue via their law of unfair competition (either civil or criminal provisions, or both): Austria, Belgium, Bulgaria, Czech Republic, Germany, Denmark, Estonia, Greece, Spain, Finland, Hungary, Latvia, Lithuania, Poland, Romania, Slovenia, Slovakia.
- Tort law (or liability for non-contractual responsibility) is used in some countries, either as the main means to address trade secrets misappropriation (Luxembourg, Netherlands) or supplementing the protection offered by unfair competition law (Belgium, Greece).

<sup>3</sup>

Understood as opposed to criminal law. It therefore includes: contract law, labour law, unfair competition law, tort law, intellectual property law.

Almost all jurisdictions have general provisions included in their labour laws or civil codes to prevent employees disclosing their employers' trade secrets, at least during the employment relationship. Contract law can be used to protect trade secrets in all of them, but only Malta seems to exclusively rely on contract law to protect trade secrets.

Common law countries (Ireland, United Kingdom) have developed case law (cf. regarding breach of confidence) in the absence of legislation.

*(ii) Civil rules in Member States<sup>4</sup>*

AT (Austria): Austria's Unfair Competition Act provides civil (and criminal) sanctions against trade or business secret misuse by employees and those who exploit such information without consent for the purposes of competition. Other legislation such as the Patents Act and the Criminal Code also provides legal remedies in particular circumstances, such as disclosure of inventions by employees or in cases of industrial espionage. In addition, the Austrian courts have held that obtaining trade or business secrets by breach of confidence (in the course of contractual negotiations) falls within the Unfair Competition Act.

BE (Belgium): There is no one piece of legislation on the protection of trade secrets as such in Belgium but there are several provisions of Belgian law which can be used against the misuse or disclosure of trade secrets. Trade secret owners generally rely on the general law of tort (Article 1382 of the Belgian Civil Code), unfair competition and specific provisions in Belgian labour law.

BG (Bulgaria): There is no specific legislation on trade secrets in Bulgaria but various laws including the Law on Protection of Competition and the Law on Access to Public Information contain general provisions which may be used to protect trade secrets. In fact, there are over 60 such statutory and non-statutory provisions (including criminal liability under the Criminal Code).

CY (Cyprus): There is no specific legislation governing trade secret misuse in Cyprus but there are a number of different laws which mention trade, business and professional secrets. For example, the Commercial Descriptions Law, the General Product Safety Law and the Competition Law. However, liability is criminal; there is no civil liability for trade secret misuse.

CZ (Czech Republic): The Czech Commercial Code defines a trade secret and provides remedies for trade secret infringement. The TRIPS Agreement is directly applicable in Czech law and thus the definition of a trade secret under Article 39(2) of the TRIPS Agreement also applies in Czech law. The basis of trade secret protection in the Czech Commercial Code, however, is the civil law of unfair competition.

DE (Germany): There are a number of provisions in German legislation protecting trade secrets. The most important statutory provisions for the protection of trade secrets are found in the Act against Unfair Competition. These provisions apply to employees and to third parties. Many of the statutes protecting trade secrets under the criminal law also have civil law provisions. These provisions allow for damages and injunctive relief if one of the relevant criminal law provisions is violated. Civil law remedies are also available under the Civil Code (tort law). German contract law also provides effective protection where there is a contractual obligation to maintain the secrecy of trade secrets.

DK (Denmark): In Denmark there is no statutory definition of trade secrets; however case law has clarified the types of information that are protectable to include both technical and

---

<sup>4</sup> See generally Hogan Lovells (2012).



commercial information. Several statutes, both civil and criminal, are used to protect the rights of trade secret owners as well as legal principles derived from contract law, competition law, employment law and unfair competition law. Most notably, the Criminal Code and the Marketing Practices Act contain provisions protecting trade secrets.

EE (Estonia): Estonian legislation provides specific provisions on the protection of trade secrets, most notably in the Competition Act, the Commercial Code, the Employment Contracts Act and the Penal Code. The Competition Act includes an illustrative list of information considered to constitute trade secrets. The Supreme Court has also held that in addition to this definition, the definition of trade secrets provided in the TRIPS Agreement can also be used to interpret the term "trade secrets" under Estonian law.

EL (Greece): Greek Unfair Competition Law provides specific provisions on the protection of trade secrets. More general protection is found in the Greek Civil Code which includes general tort provisions.

ES (Spain): Trade secrets are mainly protected in Spain under the Unfair Competition Act and the Criminal Code. The Act contains provisions specifically aimed at trade secrets. There are also other laws which deal with trade secret protection indirectly, for example, the laws establishing the obligations of directors and other employees.

FI (Finland): There are a number of Acts which include provisions for the protection of trade secrets, most importantly the Unfair Business Practices Act, the Employment Contracts Act and the Criminal Code. Unlike its neighbour, Sweden, Finland does not have one piece of legislation directed specifically to the protection of trade secrets. Although trade secrets are not considered to be typical intellectual property rights, the broad definition of intellectual property rights under Finnish law encompasses their protection under the Unfair Business Practices Act.

FR (France): The only specific trade secrets legislation in French law is that protecting "manufacturing secrets" in the Intellectual Property Code. Other provisions of civil law (tort law) protect trade secrets more generally. The Labour Code also provides criminal liability for trade secret violations by employees or former employees. When parties are bound by a contractual obligation not to disclose secret information, an action lies for breach of contract.

HU (Hungary): Hungarian law provides specific provisions on the protection of trade secrets. The main general rules are established in the Civil Code as part of the moral rights section. Besides, rules on the the protection of know-how are currently laid down separately in the Civil Code, within the general provisions on the protection of intellectual property. The unfair competition law aspects of trade secret protection (based on the definition of trade secrets enshrined in the Civil Code) are regulated in the Unfair Competition Act.

~~The Civil Code and Unfair Competition Act in particular provide specific protection.~~ Provisions also exist in the Labour Code and in various financial/banking laws.

IE (Ireland): There is no specific legislation in Ireland directed to the protection of trade secrets. However, proceedings may be brought under laws relating to breach of confidence, data protection, criminal damage and specific sectorial pieces of legislation. As in England, Irish law has the equitable principle that a person who has received information in confidence cannot take unfair advantage of it. Generally, Irish law imposes a duty of confidentiality in both non-employment cases and employment cases. In both situations, there must be an obligation of confidence and once it is established that such an obligation exists then the person to whom the information is given has a duty to act in good faith and only use the information for the intended purpose. Again, as in England, an obligation to keep information

confidential may either be imposed by contract; implied because of the circumstances of the disclosure or implied because of the special relationship between the parties.

IT (Italy): Specific provisions on the protection of trade secrets are contained in the Italian Code of Industrial Property (IPC). Secret information may only be protected if the requirements set out in the IPC are met. There are also general tortious obligations and unfair competition provisions in the Civil Code which can be employed to compensate for trade secrets misuse.

LT (Lithuania): Lithuanian legislation provides specific provisions on the protection of trade secrets, most importantly in the Civil Code, the Law on Competition, the Labour Code and the Criminal Code. Under the Civil Code, anyone unlawfully acquiring a commercial secret is liable to compensate the owner for the damage caused. There are also express provisions in the Labour Code regarding disclosure by employees who disclose a commercial secret in breach of their employment contract.

LU (Luxembourg): There are no specific legal provisions protecting trade secrets in Luxembourg. However, trade secrets can be protected by unfair competition law, criminal law, tort law and contractual law.

LV (Latvia): Latvia has a number of pieces of legislation which provide specific provisions on the protection of commercial secrets. The Commercial Law is the main Act regulating commercial activities. It defines "commercial secrets" and provides express protection for them. The Labour Law also includes provisions regarding use of commercial secrets by employees. Latvia also has an Unfair Competition Act which expressly provides that the acquisition, use or disclosure of commercial secrets of another competitor without their consent is a form of unfair competition.

MT (Malta): There is no specific legislation on the protection of trade secrets in Malta. Trade secrets may be protected contractually, by express or implied terms, and, an employee is presumed to be under an obligation not to disclose confidential information. If no contract exists there will be no civil law right to protect a trade secret.

NL (Netherlands): There are no specific provisions on the protection of trade secrets in Dutch legislation. In the Netherlands, the protection of trade secrets is based on the general principle of tort law i.e. an unlawful act. In 1919, the Dutch Supreme Court held that the provision in the Dutch Civil Code on unlawful acts could be used to secure protection against trade secret infringement. Contract law also provides some protection in contractual relationships if there are confidentiality obligations in the contract.

PL (Poland): There are specific provisions on the protection of trade secrets in Polish legislation, notably in the Unfair Competition Act. A number of other Acts mention trade secrets, for example, the Civil Code, the Labour Code, the Act on Competition and Consumer Protection, the Code of Commercial Companies and Partnerships etc. The Labour Code includes express provisions requiring employees to maintain the confidentiality of information the disclosure of which could cause damage to their employer.

PT (Portugal): The Portuguese Industrial Property Code has specific provisions relating to the protection of trade secrets. The Industrial Property Code is directed towards unlawful acts against competitors. A violation is punished, not as a crime, but as a misdemeanour. The Labour Code also contains provisions which stipulate that an employee may not disclose information, while employed, relating to his employer's organisation, production methods and company business.

RO (Romania): There is specific legislation in Romania on the protection of trade secrets. Provisions regulating protection of trade secrets have been included in the Law for the Prevention of Unfair Competition ("Law on Unfair Competition") and specify that the unfair use of a competitor's trade secrets is regarded as contrary to honest commercial practices. Trade.

SE (Sweden): Sweden is the only country in the EU to have an Act specifically protecting trade secrets. The Act provides a definition of trade secrets, penalises trade secret espionage and contains provisions on civil liability.

SI (Slovenia): Trade secrets are specifically protected in Slovenia by a number of pieces of legislation, in particular, the Companies Act, the Employment Relationship Act, the Protection of Competition Act, the Penal Code and the Code of Obligations.

SK (Slovakia): Civil protection of trade secrets in the Slovak Republic is regulated by the Commercial Code. The relevant fields of protection are civil law, commercial law, intellectual property law, non-contractual liability and unfair competition law.

UK (United Kingdom): There is no legislation providing specific protection for trade secrets. Trade secrets are protected by contract and/or by the law of equity.

***(A.2) Differences in the scope of protection: the trade secret and the misappropriation***

The absence of homogenous pieces of legislation in this area implies that there is no uniform understanding of what a trade secret is and what misappropriation is:

- In Italy, Portugal and Sweden, there is a specific statutory definition of trade secrets in the applicable legislation.
- A statutory definition of trade secrets is also available in the unfair competition provisions of the Czech Republic, Lithuania and the Slovak Republic.
- In the Czech Republic, Greece, the Netherlands and Spain, the TRIPS definition has been expressly acknowledged and adopted<sup>5</sup>.
- In some cases, definitions of trade secrets can be found in other pieces of laws, for other purposes (e.g. Freedom of Information Act in the UK).

**Comment [JA2]:** The Hungarian Civil Code is also providing for a definition of trade secrets (in compliance with the relevant TRIPS provision). Moreover, the Unfair Competition Act is referring back to that definition when laying down specific rules for the protection of trade secrets in a competition law context.

In principle information which meets the requirements of Article 39(2) of the TRIPS<sup>6</sup> would be protectable in all EU Member States. Also, no restrictions seem to exist regarding the type of information which could be protectable and in all EU Member States both technical (e.g. know-how etc.) and commercial secrets (e.g. business strategies etc.). However, the absence of specific definition results in risk of inconsistent interpretation as to what is protectable as trade secrets and consequently, a different protection depending on the type of action initiated by the trade secret owner<sup>7</sup>. Also, differences in courts practices are reported<sup>8</sup>.

Concerning the question of misappropriation, the main divergences relate to the situation of the third party who obtain the secret information in good faith<sup>9</sup>: see below on remedies.

<sup>5</sup> Cf. Baker & McKenzie study.

<sup>6</sup> In essence, information which is secret, has commercial value (because it is secret) and has been subject to reasonable steps to keep it secret.

<sup>7</sup> Baker & McKenzie study.

<sup>8</sup> Baker & McKenzie study.

<sup>9</sup> To be sure, no Member State grants any action against a third party who autonomously developed the same information.

***(A3) Differences in the remedies: injunctions, destruction of goods and compensation for prejudice suffered***

***(i) General***

The remedies available in civil/commercial law proceedings for the misappropriation of trade secrets do vary and appear to depend on the origin of the action (e.g. based on tort, contract law, unfair competition law etc.): see Table 2 for a summary view.

**Table 2 – Available civil remedies**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Injunctions (cease and desist orders: ordinary action	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Injunctions (cease and desist orders: interim relief	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Return/destruction of trade secrets / goods produced using misappropriated trade secrets: ordinary action	✓	✓			✓	✓	✓			✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Return/destruction of trade secrets / goods produced using misappropriated trade secrets: interim relief	✓	✓				✓				✓		✓	✓	✓	✓		✓		✓				✓				✓
Seizure of trade secrets / goods produced using misappropriated trade secrets: ordinary action		✓			✓		✓		✓	✓		✓	✓		✓	✓		✓		✓	✓	✓		✓	✓	✓	✓
Seizure of trade secrets / goods produced using misappropriated trade secrets: interim relief		✓				✓			✓	✓		✓	✓		✓		✓		✓	✓	✓	✓				✓	✓
Withdrawal from the market of goods produced using misappropriated trade secrets: ordinary action		✓			✓		✓		✓	✓		✓	✓		✓	✓		✓		✓	✓	✓	✓	✓			
Withdrawal from the market of goods produced using misappropriated trade secrets: interim relief		✓			✓				✓	✓		✓	✓		✓		✓					✓	✓	✓			
Damages	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Publication of decisions: ordinary action		✓	✓			✓				✓	✓	✓	✓		✓		✓			✓	✓		✓			✓	✓
Publication of decisions: interim relief		✓										✓			✓												
Restraint measures (e.g. penalty for future breach of the Court's order): ordinary action	✓	✓	✓	✓					✓		✓	✓			✓	✓	✓		✓					✓			
Restraint measures (e.g. penalty for future breach of the Court's order): interim relief		✓		✓					✓			✓			✓		✓							✓			

The above remedies are, in general, all cumulatively available to the trade secret owner, with few exceptions. For example, in Belgium, damages are available but not for cease-and-desist claims brought under the Unfair Competition Act (in the form of expedite action). In Bulgaria, it appears that final injunctions are not available (at least cease-and-desist orders in the strict sense of the word) with damages being the usual final remedy. In Latvia, although potentially available, it is not clear which remedies can effectively be used as there is no case law as to whether remedies provided in the Civil Procedure Code for intellectual property rights apply also to trade secrets (trade secrets are not expressly included among the definition of intellectual property). In Italy damages may only be awarded in ordinary proceedings. In Luxembourg, while injunctions are granted by the President of the Commercial Court, damage claims shall be brought before the District Courts.

*(ii) Injunctions (cease and desist orders)*

In general, injunctions (cease and desist orders) are available in all EU Member States. In all Member States, injunctions (i.e. cease and desist orders) are usually available also as interim

relief remedy (i.e. during preliminary and summary proceedings where the claimant's requests are summarily examined by the Court and measures are granted within a very short time limit).

Therefore, there is civil law redress in order to block the commercialisation of goods (or services) which have been manufactured (or designed) using misappropriated trade secrets (so-called "resulting goods/services"). However, this redress varies from Member State to Member State and there is no guarantee that the "resulting goods/services" will be stopped everywhere in the EU. Cease and desist orders against the use of misappropriated trade secrets by third parties (i.e. beyond a contractual relationship) are not always available:

- (i) when trade secrets are protected under unfair competition rules, the trade secret owner needs to sue a competitor but cannot sue a person having the secret with a view to sell it to another third party or to exploit it for other purposes than competing with the original owner of the secret;
- (ii) solutions diverge regarding the possibility to obtain a cease and desist order against negligent third parties or third parties who obtained the misappropriated trade secrets in good faith but before the trade secrets had reached the public domain. In some EU Member States, remedies are potentially available regardless of the recipient's good or bad faith (Austria<sup>10</sup>, Czech Republic, Denmark, Estonia, Finland, Germany, Ireland, Latvia, Lithuania, and Portugal) and injunctions can be obtained also against a third party who obtained the secret in good faith – however, the third party is likely not to be held liable for damages, unless the use of the secret information continues even after the recipient has been informed of the confidential nature of the information. In others, this is not possible<sup>11</sup>; and
- (iii) cease and desist orders may be limited in time even if the trade secret has not yet reached the public domain. Belgium<sup>12</sup>, Cyprus, Denmark<sup>13</sup>, Greece, The Netherlands<sup>14</sup>, Poland and Slovenia, which do not allow unlimited injunctions. In Common Law countries, injunctions are equitable remedies and, as such, courts are free to determine terms and duration of the restrictions.

Concerning the situation of employees, the Baker & McKenzie study finds that though in general, whilst employed, employees have a (statutory) duty of loyalty (including non-disclosure and non-compete obligations) towards the employer, a common practice in most jurisdictions is to provide for non-use and non-disclosure, as well as non-compete clauses in contracts of employment. However, the position differs as to what can be done in relation to an ex-employee who uses or discloses secrets after leaving employment. The balance between the interests of the employer and the employee is indeed assessed differently in the relevant

<sup>10</sup> In Austria, damage claims are also available in cases of default; accordingly damage compensation could be awarded also in case of the third party's slight negligence.

<sup>11</sup> For instance, in the United Kingdom a duty of confidentiality may be implied by the circumstances (the duty of confidentiality is easy to identify in case of an employment contract or a non-disclosure agreement, but it could prove to be very difficult to demonstrate where a person has obtained the confidential information in absence of any relationship between the owner and the recipient), but a person who innocently receives a confidential information will not be under a duty of confidentiality until he is made aware the information is confidential.

<sup>12</sup> In Belgium, courts refuse to grant final injunctions against future trade secrets misappropriation because, contrary to intellectual property rights, trade secret protection can potentially last forever and thus courts are not willing to grant the owner of a trade secret a broader protection than most intellectual property right holders.

<sup>13</sup> In Denmark, although depending on a case by case analysis, final injunctions are usually granted for a period of two to three years from termination of the cooperative relationship.

<sup>14</sup> In Greece and The Netherlands, injunctions are considered temporary in nature.

countries. In general, post-employment, an employee cannot be prevented from using the skill and knowledge gained during the employment, provided that said knowledge does not consist of trade secrets or confidential information that the employee wilfully memorised or (mis)appropriated with the purpose to misuse them after termination of the employment relationship<sup>15</sup>.

*(iii) Destruction of the goods produced using the misappropriate trade secrets or the restitution of the misappropriated information*

Compared to injunctions, other measures such as the destruction of the goods produced using the misappropriate trade secrets or the restitution of the misappropriated information) are not available everywhere and are available in interim proceedings in certain countries only (see [Table A6.2](#)). Since resulting goods are not always destroyed, there is no guarantee for the trade secret owner that such goods will no reappear in the market.

*(iv) Damages*

Compensation for the prejudice suffered from the misappropriation of a trade secret is available in all jurisdictions<sup>16</sup>. Damages claims are mainly based on tort or contract and only in a few cases specific provisions on damages are included in either the unfair competition laws (see for example Spain) or in the specific provisions applying to trade secret misappropriation (Italy and Sweden).

Damages based on tort cover both accruing damages ("*damnum emergens*") and loss of profits ("*lucrum cessans*"). Loss of profits, however, is in most cases very difficult to prove, since the misappropriated information is an intangible asset<sup>17</sup>. This helps explaining the often low compensation obtained<sup>18</sup>. A claim for unjust enrichment is available in some countries

<sup>15</sup> In Denmark (and similarly in Poland), the statutory non-disclosure and non-use obligations survive termination of the employment contract for a period of three years. In Italy, as in many other European countries, non-compete agreements (or clauses) are commonly used to prevent use or disclosure after the contract of employment ceases, albeit offering more limited restrictions than those which exist during the period of employment (to be enforceable non-compete clauses must generally be limited in time and space, identify the activities which the former employee cannot engage in and provide for a monetary compensation). In Sweden, damages for breach of confidentiality obligations after termination of employment are only available where there are "extraordinary circumstances". In Ireland and the United Kingdom there is a distinction between general (low grade) confidential information that the employee is not entitled to disclose whilst employed but can use and disclose thereafter and "real trade secrets" which he cannot disclose or use without authority at any time. The distinction depends on a number of factors including whether the employer impressed the secrecy of the relevant information upon the employee; and whether the "secret" can be readily isolated from other information which the employee is free to use.

<sup>16</sup> In Bulgaria, damage compensation is the sole final remedy available to the owner of a trade secret.

<sup>17</sup> According to Baker & McKenzie, there are often evidentiary problems in proving the loss incurred by the owner of a trade secret. In some countries, damages are awarded only if the claimant is able to demonstrate that he had suffered some loss. Other countries allow courts to award damages on an equitable basis - taking into account all the circumstances of the case - if the claimant has not been able to provide sufficient evidence on the amount of damages

<sup>18</sup> According to Baker & McKenzie, damages vary on a case-by-case basis but the average figures collected during the study "seem not to be particularly encouraging". This study mentions a few cases in Italy and Sweden, where courts awarded high amounts of damages: in Italy, in two cases of trade secrets infringement the Court of Milan awarded damages for EUR 1,100,000.00 and EUR 10,000,000.00, respectively. In Sweden, courts have awarded damages for SEK 7/10,000,000.00 and 48,000,000.00. However, the study reports that these appear to be exceptional cases. In the Force India Formula One Team Ltd. case, only €25000 were awarded by a UK court to the claimant. The plaintiff had claimed compensation in excess of £13 million (which was based on the assumption that it succeeded in the entirety of its claims for breach of confidence, which it did not). However, the judge did not accept the plaintiff argument that the relevant information was of great

only, such as among others, Belgium, Estonia, Finland and Spain (for further details please see [Table 3](#) below). In some other countries (for example, Austria, Germany, Italy, Ireland, Lithuania, Poland, Sweden and the United Kingdom) the claimant has the right to claim the account of profits obtained by the infringer from its wrongdoing. In most of the cases, however, the account of profits is alternative to the loss of profits or is considered a criterion to calculate said loss. In Italy, the owner of trade secrets may claim the restitution of the infringer's profit in addition to the loss of profits to the extent that the infringer's profits exceed the claimant's loss. In Greece, account of profits and unjust enrichment are alternative ways to calculate the loss of profits. Similarly in The Netherlands loss or profits excludes account of profits.

**Table 3 – Available damages options**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Accruing damage ( <i>damnum emergens</i> )	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Loss of revenues ( <i>lucrum cessans</i> )	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Moral damages			✓						✓				✓	✓						✓		✓	✓			✓	
Punitive damages														✓													✓
Other monetary compensation					✓																✓						
Account of profits	✓			✓	✓	✓		✓	✓	✓	✓		✓	✓	✓			✓			✓			✓			✓
Fair royalty	✓					✓	✓	✓	✓				✓	✓	✓						✓						✓
Unjust enrichment		✓			✓			✓	✓	✓									✓		✓	✓	✓	✓	✓	✓	
<i>Ex aequo et bono</i> global account		✓	✓					✓		✓	✓		✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	
Cumulation of these options	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

If damages are claimed on contract, liquidated damages (if provided by the agreement) can also be claimed in addition to damages. Contractual liability, however, is often limited to the damages which were foreseeable at the time of conclusion of the contract.

The available options are in principle all cumulative (exceptions are Austria, Cyprus, Estonia, Finland, France, Germany, Hungary, Ireland, Luxembourg, Portugal, Romania and United Kingdom) provided that the total amount awarded by the court does not exceed the actual claimant's loss. Furthermore, in countries where courts are allowed to award an "*ex aequo et bono*" global amount in cases where damages cannot be alternatively calculated, such criteria are of course to be considered as alternative to all the other available damage options.

Since most of the EU Member States do not have specific criteria for the calculation of damages, they apply the general criteria of tort liability (i.e., *damnum emergens* and *lucrum cessans*). The license analogy has been indicated as a possible criterion for the calculation of damages<sup>19</sup>, among EU Member States in Austria, Denmark, Germany, Greece, Hungary, Italy, The Netherlands and United Kingdom.

## (B) CRIMINAL LAW

### (B.1) Criminal law protection in national law: summary

value and considered that the misuse of the information was limited in nature, purpose and benefit. As a result, the judge considered that €25000 was the figure the parties would have negotiated had they been in the position of a willing licensor and willing licensee acting reasonable as at the date of the breach of confidence.

<sup>19</sup>

This method of calculation is used regarding infringements of intellectual property rights, pursuant to Article 13(1)(b) of Directive 2004/48/EC. This Article provides for the rules on abstract calculation of damages (i.e. calculated on the basis of royalties which could have been due should a licence have existed) as an alternative to the general *damnum emergens* and *lucrum cessans* criteria.



Criminal protection of trade secrets against misappropriation differs from Member State to Member State on several levels, although almost all of them have provisions in this respect. Since there is a lack of a common/shared definition of the scope of trade secrets, the actual extent of the protection provided by states may vary depending on the aims pursued by the provisions implemented for this purpose.

Only a few Member states (i.e., Bulgaria, Ireland, Malta and U.K.) have not established any specific criminal framework with respect to trade secrets violations. However, even in those Member States, the conduct of the infringer may be punished under other related criminal offences (see below). In some cases, where no specific criminal provision has been implemented, penal sanctions of trade secrets misappropriation apply under unfair competition laws or commercial laws. Sweden is the only EU Member state that has implemented a specific law on trade secrets (the Swedish Act on the Protection of Trade Secrets), even though some relevant provisions are also contained in the Criminal Code<sup>20</sup>. Table 4 below summarises the criminal provisions in force:

Table 4 – Criminal provisions applying to trade secrets misappropriation <sup>21</sup>																											
	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Criminal code	✓	✓		✓		✓	✓	✓	✓	✓		✓	✓		✓	✓	✓	✓		✓		✓	✓	✓	✓	✓	✓
Unfair competition / commercial law	✓			✓	✓	✓	✓		✓												✓		✓				
Specific law on trade secrets																								✓			

## **(B.2) Differences in the conducts considered as crimes**

### **(i) Unauthorised disclosure/use of trade secrets**

Many of the countries seem to limit the scope of trade secrets to the information that a company has a reasonable and objective interest to keep confidential, in accordance with an objective criterion (e.g., Austria, Belgium, France, Germany, Hungary, Italy, Lithuania, Luxembourg, Netherlands, Slovakia, Spain, Sweden). Nonetheless, in some cases the relevant protection is afforded to any information having economic value that the owner deems it opportune for his benefit to keep secret according to a subjective criterion and that are subject to reasonable measures for protection of confidentiality (e.g., this broader interpretation seems to be prevailing in Czech Republic, Finland, Greece, Poland, Romania and Slovenia).

- In Austria the offender to be held criminally liable for trade secrets violations must have acted at least with conditional intent. In Belgium, Estonia, Finland, France the conduct may be punished even if the offender acted with negligence.
- Cyprus does not establish any specific requirement that the offender must meet to be charged with criminal liability for trade secret violations. Nor is there any stated obligation on the claimant to keep information confidential.
- In the Czech Republic the offender must act deliberately to commit the offence. As the relevant conduct is defined as an act of unfair competition, the offender must qualify as a competitor or someone participating in the competitive process. The concept of competition has nevertheless been construed very broadly, including even indirect or potential competitors.

<sup>20</sup> In particular, the Act on the Swedish Protection of Trade Secrets establishes two different offences: business espionage and the unauthorized dealing with trade secrets. Other complimentary or more general offences, such as, for instance, unauthorized access to computer systems or breach of faith against principal are regulated under the Criminal Code.

<sup>21</sup> Baker & McKenzie study.

- In Denmark the offences provided for under the Criminal Code require intent. Only upon certain circumstances if the employee causes a substantial risk of dissemination of confidential information by negligence he or she may be charged with criminal liability pursuant to Section 19 of the Marketing Practices Act. without having acted with intent.
- Germany requires that the infringer acts with intent and, specifically, for the purpose of competition, for personal gain, for benefit of a third party or causing damage to the owner of the secret.
- In Greece the offender must act (with intent) for purpose of competition, that means that two criteria have to be met: (i) the conduct of the offender must be suitable to serve the purpose of competition; (ii) he or she must act with the “intention of competition”, i.e. enhance his or third parties’ competitiveness.
- As to Hungary and Italy, the offender may be punished only if he or she acts with intent.
- In Latvia the employer is obliged to identify in writing the information considered to be commercial secrets. In any case, the offender requires the offender to have acted for use or disclosure by himself or another person, therefore intent is required for the offence to occur.
- Lithuania requires that the offender, in case of business espionage, acted with the intent to unlawfully obtain a trade secret, whereas, in the case of violation of trade secrets, with the intent to get a financial gain or to injure the owner by the disclosure to third parties or the use of the information.

As almost all EU Member states require that the offender acted with intent, it emerges that whoever commits a trade secrets infringement must have clearly the knowledge that the business information constituted trade secrets, even if there is no express obligation to keep such information confidential.

- In Luxembourg, Netherlands and Portugal the offender must act with the intent to reach a competitive advantage or to cause harm to the owner.
- Also Poland requires intent, as the offender must breach an obligation of confidentiality that must be prior established by the owner of the secret, either directly or indirectly.
- Under Romanian and Slovak law the offender must act with intent, but no specific purpose is required.
- The same applies in Slovenia, where if the conduct reaches certain outcome, the offender may be charged with the more severe correspondent penalties.
- Spain also requires intent, even if the purposes to be pursued vary depending on the type of offence considered (for instance, commercial advantage).
- The Swedish Act on the Protection of Trade Secret does not pose any requirement as to the purpose that the offender acts for. It only requires that he acted wilfully and without authorization.

*(ii) Related offences*

In Belgium a person who commits the offence under Section 309 of Criminal Code (unauthorized disclosure of trade secrets) may also be charged with theft or misappropriation (provided that he qualifies as an employee with the company). Similarly, Section 491 applies

when a person is entrusted as a data processor/handler manufacturing secrets that are physically stored breaches his duty of confidence.

In Bulgaria, for instance, the offence of business bribery is punishable and applicable to, any individual who discloses to third parties information that he knows in return for something.

In France there is a wide range of crimes that may arise in connection to trade secrets violations:

- First, the offence of theft may occur when the conduct at stake consists in the fraudulent appropriation of third parties' data carriers containing confidential information. Such an offence has been found by the Court of cassation to apply even in connection to disclosure of trade secrets. Theft is punished by imprisonment up to three years and a fine of Euro 45,000.00.
- Additionally, the offence of breach of trust may be committed where an individual with the company misappropriates documents containing confidential information entrusted to them for temporary use. In such a case, the offender shall be punished by imprisonment up to three years or a fine of Euro 375,000.00.
- Also, other provisions of the Criminal Code punish the act of supplying secret information to foreign powers by imprisonment up to fifteen years and a fine of Euro 225,000.00.

In Germany cases of industrial espionage may result in theft or misappropriation.

In Greece the infringement of trade secret may constitute, among other offences, a breach of trust under Section 390 of the Criminal Code. In such a case, the offender shall be punished by imprisonment up to ten years and a fine up to Euro 15,000.00.

Depending on the circumstances, violations of trade secrets may result, further to civil lawsuits, in a number of offences, including but not limited to insider trading, unauthorized access to computer systems and a breach of privacy.

As to Italy, the conduct of the offender who commits an unauthorized use or disclosure of trade secrets may also constitute theft or misappropriation.

In Latvia acts of unauthorized disclosure or acquisition of trade secrets may constitute unfair competition practices where repeated within a one-year period and, thus, result in a punishment by imprisonment of up to two years and a fine, in addition to disqualification penalties.

Violations of trade secrets may constitute fraud or bribery in Lithuania or theft in Luxembourg. In Netherlands the conducts may also result in the theft of secret documents or hacking of computer systems. In Portugal the related offences include computer and communications fraud. Slovakia, in addition to breach of trade secrets, criminalizes the misuse of participation in economic competition through unfair acts.

In Slovenia the same act may be punished under the crime of "disclosure of and unauthorized access to trade secrets" as well as, for instance, the offence of abuse of insider information. Spain provides an extensive regulation of trade secrets infringements: however, pursuant to Section 278.3 of the Criminal Code the specific provisions apply without prejudice to the penalties that may arise for appropriating or destroying the computer media, i.e. for the offences of theft or misappropriation.

In Sweden, further to the offences provided for under the act on the Protection of Trade Secrets, other criminal provisions may apply, including unauthorized access to computer

systems, unlawful dispossession, unlawful use, espionage, unlawful dealing with secret information and negligent dealing with confidential information.

Offences in any way related to trade secrets violations have significant importance in the legal systems that do not establish any specific provision in this respect:

- In Bulgaria violations of trade secrets may be punished only indirectly. The relevant offences in this respect include the disclosure of service/office secrets, the business bribe and computer crimes.
- Under Irish law, for instance, trade secrets infringements may result in: (i) disclosure of personal data obtained without authority; (ii) unauthorised accessing of data; (iii) unlawful use of a computer; (iv) theft or (v) criminal infringements of intellectual property rights.
- Under Maltese criminal law, in the absence of provisions specifically concerning trade secrets, one could be charged with misappropriation and fraudulent gains as a result of his conduct.
- In the U.K. the criminal provisions that may apply in connection to trade secrets infringement cases include theft, fraud, conspiracy to defraud as well as, upon certain circumstances, some of the offences provided for under the Computer Misuse Act (such as unauthorized access to information contained on a computer) and the Data Protection Act (although it is very unlikely that personal data qualify as trade secrets).

### (iii) Qualified offences

Certain Member States also establish qualified offences when the revelation or use of confidential information is committed by a person acting in a particular capacity (e.g., as civil servant, public official, or as person handling confidential information by reason of his job, e.g. lawyers, officers). Please note that this does not mean that for each of the offences a specific provision is established. Separate provisions may have been implemented (e.g. Italy) or, like in Estonia, the same provision may apply to professional and official secrets, also covering trade secrets. See [Table 5](#):

**Table 5 – Qualified offences<sup>22</sup>**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Breach of professional secrecy	✓	✓	✓					✓	✓				✓		✓				✓	✓		✓	✓	✓	✓	✓	✓
Breach of official secret	✓		✓	✓				✓	✓		✓		✓		✓								✓	✓			
Other breach of confidence									✓				✓														
Separate provisions	Y	Y	N	N	N/A	N/A	N	N			Y	N	Y	Y	N				N/A	N		Y	Y			N	

### (iv) Threshold for the applicability of criminal penalties

In the Czech Republic only violations resulting in a damage of at least Euro 2,000.00 may give rise to criminal liability. The offender must cause harm to a competitor or a consumer equivalent to such an amount or provide someone else than the owner of the secret with a benefit of the same amount. The offender does not necessarily need to be a legal person or an enterprise.

A *de minimis* threshold applies in Lithuania, where for the offender to be prosecuted it is required that the conduct caused a damage of at least EUR 5,648.00.

**Comment [JA3]:** In the Hungarian Criminal Code, there are separate provisions covering breach of professional secrecy (Art. 177 and first phrase of Art. 300), breach of official secret (Art. 221-222/A.) and other breach of confidence (Art. 177).

It is the first one of these that is treated together (in the same provision on „breach of economic secret”) with the breach of trade secrets.

Please note that a new Criminal Code will enter into force on 1 July 2013. It will not bring about substantial changes in the criminal law protection of trade secrets, but the trade secret related offence will be treated in a separate provision from the „breach of economic secret”.

Something like a *de minimis* threshold is established in Poland, where the conduct must have caused substantial damage to the owner, although no quantification of this concept is provided for in the law.

Slovakia establishes that for the offender to be prosecuted a significant damage (more than EUR 26,600.00) must be caused by his conduct to another competitor. It also provides for a more severe penalty in cases where the conduct causes a large scale damage (over EUR 133,000.00).

Also under Estonian and Finnish criminal law a general safe harbor clause applies, preventing prosecution in case the offence is found to be of minor harm.

In Austria the offender will not be prosecuted if his conduct is justified by a compelling public or private interest.

No safe harbor seems to exist in Latvia and Sweden. In Cyprus disclosure of trade secrets is allowed, for instance, when protection of health and safety of citizens is affected, i.e. where compelling public interests are at stake or to prove the violations of statutory provisions.

Similarly, no safe harbor or *de minimis* threshold applies in Denmark, Finland, Italy, Luxembourg, Slovenia. Germany does not provide for any safe harbor; however, disclosure of trade secrets is justified when committed to avert an imminent danger to life, limb, freedom, honour, property or other prevailing legal interests. In Greece trade secrets are not protected in case a witness is examined to represent certain circumstances before the Court, excluding state secrets. In Hungary Section 300(2) of Criminal Code expressly sets forth some safe harbors that justify infringement of trade secrets. These clauses include:

- (i) fulfilment of duties prescribed in a separate act governing the publication of information and information to be disclosed in the public interest;
- (ii) fulfilment of duties subject to statutory reporting obligations, even in the case the report was filed in good faith and proved to be unfounded.

In the Netherlands a specific provision sets out an exemption for those who disclosed in good faith a trade secret assuming that the disclosure was in the public interest. Portugal and Romania consider the consent of the owner to the disclosure of a secret as a safe harbor clause. In addition to that, Romanian law permits the disclosure of trade secrets where compelling public interests are at stake. Spain does not consider information about illegal activities carried out by the owner to be a trade secret: therefore, its revelation would not determine any prosecution.

Generally speaking, the risk of dissemination of confidential information does not amount to a criminal offence (except for Slovakia, Slovenia). The conduct carried out by the infringer must result in an actual violation of the interest protected under the relevant provisions. In contrast, most legal systems (including Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Italy, Latvia, Lithuania, Slovakia, Slovenia) provide criminal protection against the intent to commit a trade secret violation. The acts carried out with the purpose of disclosing or using confidential business information which reach a certain threshold in the realisation of the offence are likely to trigger criminal liability.

### ***(B.3) Differences in the penalties***

The conducts which normally give rise to violations of trade secrets include the access to confidential information, the use or the disclosure thereof or the illicit acquisition for exploitation by the offender or third parties. These conducts are generally punished regardless

of the fact that the offender qualifies as a competitor and may be committed either by (past) employees of the company or by external persons (such as consultants, contractors, agents).

It is quite frequent, however, that the violation of trade secrets committed by an employee of the company owning the confidential business information results in a more severe punishment than that provided for the same offence in other cases (i.e., in Belgium, Germany, Greece and Spain).

Table 6 below provides a summary of the main conducts concerning trade secrets violation and the related punishment provided for under the legal systems.

**Table 6 – Criminal penalties applying to trade secrets misappropriation<sup>23</sup>**

Country	Offender	Conduct	Penalties
Austria	Whoever	Disclosure or exploitation of trade or business secrets	Up to six months imprisonment; up to one year if the conduct is committed with the purpose to obtain a pecuniary advantage or to cause harm to the owner or monetary penalties
		Spying out trade or business secrets for their exploitation by somebody else or disclosure	Up to two years imprisonment OR monetary penalties
		Spying out trade or business secrets for their exploitation abroad	Up to three years imprisonment AND monetary penalties
Belgium	Whoever	Communicating in bad faith manufacturing secrets appropriated during the (past) employment with the owner	From three months up to three years imprisonment AND monetary fine from Euro 50 to 2,000.00
Bulgaria		There is no specific criminal provision concerning violation of trade secrets. However, depending on the characteristics of the conduct, the offender may be charged with more general offences, such as business bribe or computer crimes	
Cyprus	Whoever	Disclosure of trade secrets	Imprisonment up to one year OR monetary fine up to Euro 1,275.00
		Disclosure of information protected by professional secrecy involving trade secrets	Imprisonment up to six months AND/OR monetary fine up to Euro 1,700.00
Czech Republic	Whoever	Acts of unfair competition infringing trade secrets and causing damage in or in excess of Euro 2,000.00 to other competitors/consumers or providing someone with unjustified benefit in the same or greater amount	Monetary fine up to Euro 1.5 Million*
Denmark	Whoever	Unauthorized misuse or appropriation of trade secrets	Imprisonment up to 1 year and 6 months OR monetary fine
		Serious violations such as appropriation of trade secrets in a contract of service or in the performance of assignments	Imprisonment up to six years
Estonia	Whoever	Unauthorized disclosure or use of business secret learned by reason of the professional or official duties with the purpose of causing damage	Imprisonment up to one year OR monetary fine
Finland	Whoever	Disclosure or use of trade secrets known by reason of the employment, position or other lawful activities to obtain financial benefit or to injure the owner	Imprisonment up to two years OR monetary fine
		Misuse of trade secrets obtained or revealed through an unlawful act	Imprisonment up to two years OR monetary fine
		Business espionage: Unlawfully obtaining information regarding trade secrets	Imprisonment up to two years OR monetary fine
France	Whoever	Revelation of manufacturing secrets	Imprisonment up to two years AND monetary fine of Euro 30,000.00
		Theft (for instance, of carriers or materials containing trade secrets)	Imprisonment up to three years AND monetary fine of Euro 45,000.00
Germany	Employees	Unauthorized communication of trade or business secrets that the offender was granted access to for the purpose of obtaining financial advantage or injuring the owner	Imprisonment up to three years OR monetary fine
	Whoever	Unauthorized acquiring or securing trade or business secrets or using thereof	Imprisonment up to three years OR monetary fine. Imprisonment up to five years if aggravating circumstances occur
Greece	Whoever	Copying, printing, using, disclosing or in any way	Imprisonment from three months up to

<sup>23</sup> Baker & McKenzie (2013).

		violating data or computer programs constituting secrets of an enterprise	one year. Imprisonment from one year to five years if the offender is in the service of the owner and the secrets are of great financial significance
	Employees	Unauthorized communication to third parties of secrets that the offender has known by reason of his employment to obtain financial advantage or to cause a damage to the owner; Unauthorized use of the information so obtained	Imprisonment up to six months AND monetary fine up to Euro 8.80
Hungary	Whoever	<del>Making available to unauthorized persons illegally obtaining, using, communicating or publishing trade secrets for financial advantage gain or to causing pecuniary disadvantage damage to others: Using the secrets so obtained</del>	Imprisonment up to three years
Ireland	Not applicable		
Italy	Whoever	Disclosure or use of any information concerning scientific discoveries or inventions or industrial applications that is intended to remain secret known by the offender by reason of his status, function, job or art, to obtain a profit	Imprisonment up to two years
Latvia	Whoever	Revelation of non-disclosable information other than a state secret; Unauthorized acquisition and disclosure of commercial secrets	Imprisonment up to five years OR monetary fine
Lithuania	Whoever	Unlawful acquisition of commercial secrets or communication to third persons; Disclosure of information that the offender was entrusted with by reason of his employment	Imprisonment up to two years AND/OR disqualification penalties
Luxembourg	Employees	Use or disclosure, during the employment or within two years after its expiration, trade or manufacturing secrets known by reason of the job to obtain financial advantage or to cause damage to the owner	Imprisonment from three months to three years AND monetary fine from Euro 251 to 12,500.00
Malta	Not applicable		
Netherlands	Employee	Intentional disclosure of confidential information that may harm the owner	Imprisonment up to six months AND/OR monetary fine up to Euro 19,500.00
Poland	Whoever	Disclosure or exploitation of trade secret in breach of confidential duties that causes substantial damage to the owner; Use of information illegally acquired or disclosure to third persons	Imprisonment from one month to two years AND monetary fine up to Euro 260,000.00*
Portugal	Whoever	Use or disclosure to third parties of secrets that the offender knows by reason of his status, job, profession or art	Imprisonment up to one year OR monetary fine
Romania	Whoever	Disclosure, acquisition or use of trade secrets without the consent of the owner, as a result of an action of commercial or industrial espionage	Imprisonment from six months up to two years OR monetary fine from Euro 570 to 5,000.00*
		Disclosure of data or information not intended to be publicly known by a person who knows it by reason of his employment, provided that the offence is likely to cause damages	Imprisonment from two up to seven years; Imprisonment from six months to five years if the disclosure is made by another person
Slovakia	Whoever	Spying out trade secrets with the intention to disclose them to unauthorized persons	Imprisonment from six months up to three years; Imprisonment from seven to twelve years if aggravating circumstances occur
Slovenia	Whoever	Disclosure of trade secrets; Providing unauthorized third parties with access to trade secrets; Collection of trade secrets with the purpose of delivering them to unauthorized persons; Unlawful obtainment of trade secrets with the purpose of delivering them to unauthorized persons	Imprisonment up to three years; Imprisonment up to five years if the information is of particular importance
Spain	Whoever	Acquiring data, documents, media and other objects to discover trade secrets; Disclosure, revelation or communication to third parties of the discovered information	Imprisonment from two up to four years AND monetary fine; Imprisonment from three to five years AND monetary fine in case the secrets are disclosed
		Diffusion, disclosure or communication of trade secrets in breach of duties of confidentiality	Imprisonment from two up to four years AND monetary fine, in case the information is disclosed in breach of confidentiality
Sweden	Whoever	Unauthorized access of trade secrets as business espionage	Imprisonment up to two years OR monetary fine; Imprisonment up to six years in case of information of significant importance
		Acquiring trade secrets knowing that the person who made it available accessed the trade secret through acts	Imprisonment up to two years OR monetary fine; Imprisonment up to four

		of business espionage	years in case of information of significant importance
U.K.	Not applicable		

\* Monetary penalties are expressed in local currency and converted to Euro for the reader's convenience

Generally, punishment of the offender is by imprisonment, even though he or she may also be charged, either in addition to that or alternatively, with monetary penalties: see Table 7 with penalties that shall apply for the main offence (for instance, unauthorized disclosure/use of trade secrets).

**Table 7 – Penalties<sup>24</sup>**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Imprisonment OR monetary penalties	✓				✓	✓	✓	✓	✓	✓	✓						✓			✓		✓	✓	✓			
Imprisonment AND monetary penalties		✓							✓	✓		✓					✓			✓	✓						
Imprisonment ONLY													✓		✓	✓									✓	✓	
Monetary penalties ONLY					✓																						
Other penalties					✓											✓							✓				

Hungary, Italy, Lithuania, Slovakia and Slovenia only provide for the imprisonment of the offender whereas in Czech Republic only monetary penalties and, where possible, forfeiture of property shall apply. Lithuania, as well as Romania, also provide for disqualification penalties in addition to imprisonment, such as deprivation of the right to be employed in certain positions or to engage in certain activities. This is a very significant solution, as it directly impacts on the opportunity for the offender to be entrusted with certain responsibilities in his future employment.

With respect to the extent of punishment, the Czech Republic is the state where the heaviest fines apply: under Czech law, the infringer shall be punished with a fine up to 1.5 Million Euro. In contrast, Czech law does not provide for imprisonment in case of trade secrets violations.

In most of states trade secrets infringements are punished with imprisonment up to a term of two-three years. There are a few exceptions: in Denmark the offender may be charged with up to six years imprisonment, provided that serious violations have taken place; in Slovenia imprisonment may be up to five years when the acts carried out by the offender concerns information of particular importance. Under the Swedish Act on the Protection of Trade Secrets, terms of imprisonment of up to six years are foreseen for cases of business espionage and up to four years for the unlawful acquisition of trade secrets of significant importance.

### (C) THE SPECIFIC CASE OF IMPORTS OF GOODS INTO THE EU

In the specific case of goods imported from third countries which would have been manufactured using misappropriated trade secrets of EU companies, there is no specific administrative procedure before customs authorities to block them.

The EU Regulation on customs enforcement of intellectual property rights<sup>25</sup> provides for such administrative customs procedures<sup>26</sup>: the holder of an intellectual property right can ask

<sup>24</sup> Baker & McKenzie study.

<sup>25</sup> Regulation (EC) No 1383/2003 of 22 July 2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights, OJ L 196, 2.8.2003, p.7. The Commission made a proposal in 2011 for a new



customs authorities to block imports of goods infringing and intellectual property right. Once the imports blocked, the holder of the intellectual property right has to file a case before a civil court which will decide on the existence (or not) of the infringement. However, this EU rules only applies as regards formal intellectual property rights and do not extent to trade secrets misappropriation claims<sup>27</sup>. Hence, national customs authorities do not process claims for misappropriation of trade secrets.

This situation differs from that in the United States. In the United States, it is possible to engage administrative proceedings before the US International Trade Commission (ITC) in order to block imported goods manufactured using misappropriated trade secrets<sup>28</sup>. Section 337 of the Tariffs Act<sup>29</sup> gives power to the US ITC to deal with claims involving infringements of intellectual property rights but also other forms of unfair competition involving imported products, such as misappropriation of trade secrets. The US ITC has investigative powers. The procedure includes trial proceedings before administrative law judges and review by the US ITC. In terms of remedies, the primary remedy available in Section 337 investigations is an exclusion order that directs US Customs to stop infringing goods from entering the US. In addition, the US ITC may issue cease and desist orders against named importers and other persons engaged in unfair acts that violate Section 337.

Therefore, in order to block goods imported from third countries which would have been manufactured using misappropriated trade secrets of EU companies, the EU owner of the trade secrets in question would need to first go to court in order to have the misappropriation of the trade secrets declared and to obtain an injunction against the third party in question which could be enforced by customs authorities. Compared to formal intellectual property rights, there is therefore an inversion of the burden of proof.

#### **(D) THE PROCEDURAL RULES BEFORE NATIONAL COURTS**

Procedural rules in national law are not always adapted to litigation in trade secrets. Secrecy of information is often at risk during civil proceedings and the absence of protection from (further) disclosure of information as a consequence of court proceedings is a considerable deterrent from starting a legal action<sup>30</sup>.

##### ***(D.1) The insufficient protection of confidential information in national proceedings***

When litigating to defend a trade secret, these procedural rules can result in disclosure of confidential information to the other party or to the public. There are three main situations.

(1) The need to describe the misappropriated trade secret in the application, so that the judge can understand it, could imply that, if the plaintiff does not know the extent of the information misappropriated by the defendant, he could disclose to the defendant (since the application is served to him) more confidential information than actually needed to defend his case<sup>31</sup>.

---

Regulation concerning customs enforcement of intellectual property rights (COM(2011)285). Negotiations on this text before the European Parliament and the Council are on-going.

<sup>26</sup> Indeed, administrative customs procedures of this type would be a matter of EU law.

<sup>27</sup> Unless of course the claim encompasses both an intellectual property right infringement (e.g. a patent) as well as a trade secrets misappropriation claim.

<sup>28</sup> See generally [http://www.usitc.gov/intellectual\\_property/](http://www.usitc.gov/intellectual_property/)

<sup>29</sup> For the text of Section 337 of the Tariffs Act, see:

[http://www.usitc.gov/intellectual\\_property/documents/statute.pdf](http://www.usitc.gov/intellectual_property/documents/statute.pdf)

<sup>30</sup> Baker & McKenzie study.

<sup>31</sup> See for instance, Hogan Lovells (2012), §57 regarding Belgium, at p.12.

(2) The general rules on the production of evidence could also have the effect of having to disclose information otherwise considered confidential. In common law countries, the pre-trial duty of (full) discovery rules applies; in continental countries, the defendant may ask for certain documents/evidence to be presented by the other party when such evidence lies in the control of that party – which could imply further disclosure of trade secrets. It should be noted that this plays both ways: bad faith plaintiffs could try this way (and therefore abusing the litigation rules) to obtain confidential information from defendants<sup>32</sup>.

(3) The inherent publicity of judicial proceedings (civil proceedings in all EU Member States are public) could also result in the disclosure of trade secrets, in this case to the public:

- Firstly, hearings are often public. While national procedural laws normally include general provisions which allow Courts to exclude the public from the hearing for reasons relating to security, public order and decency, there do not necessarily apply to trade secrets litigation. In some EU Member States (notably Bulgaria<sup>33</sup>, Estonia<sup>34</sup>, Hungary<sup>35</sup>, Germany<sup>36</sup>, The Netherlands, Poland, Romania, Slovakia, Slovenia), a party has the right to request the court to order that the entire proceeding or a part thereof be heard in private to preserve the secrecy of the trade secret. However, according to Baker & McKenzie (2013), this seems to rarely happen in practice and there would be no case law on this point<sup>37</sup>. In the United Kingdom the parties may agree or apply to the Court to ensure that certain information to be revealed during the pre-trial disclosure procedure remains confidential. The parties may enter into a contractual agreement whereby the parties agree that certain information may remain confidential or only be disclosed to legal counsel or where the parties do not reach such agreement, a party may unilaterally apply to the Court requesting that confidential information is not disclosed to the other party during the proceeding. Requests for restriction of disclosure are at the discretion of the Court.
- Judicial decisions may describe the misappropriated trade secret in question when explaining the reasons for the decision<sup>38</sup>; and in some countries other judicial documents (including applications) may be accessed by third parties. According to Baker & McKenzie (2013), in most countries, pleadings and in general court

<sup>32</sup> General procedural rules will normally allow the defendant to refuse to provide a document if it includes a trade secret or a confidential information of the defendant.

<sup>33</sup> In Bulgaria private hearing is specifically provided for cases related to “protection of trade, manufacturing, invention or tax-related secrets” if public disclosure may impair a party’s legitimate interest. When publicity is precluded, only the parties, their attorneys, experts and witnesses are allowed to enter into the court room and are subject to a statutory obligation not to disclose subject matter and content of the relevant proceeding (breach of such obligation entails liability for compensation).

<sup>34</sup> In Estonia (similarly in Finland and Lithuania), in-camera examination can be ordered for the protection of trade secrets if the interest in a public hearing is not deemed to be greater than the commercial interest in protecting the secret.

<sup>35</sup> In Hungary, when the Court orders in-camera examination, the parties are also prohibited from making copies of the minutes of the hearing or of any document containing a trade secret. Examination of documents containing trade secrets is subject to a declaration of non-disclosure and special review procedures are established by the Judge.

<sup>36</sup> In Germany, besides the exclusion of the public if trade secrets are to be discussed, legal practice has developed the so called “Düsseldorf Procedure” (originally developed for patent law claims but likely applicable to trade secrets cases), which consists in a procedure where Courts order independent proceedings for the preservation of evidence as an interim injunction handed to the defendant together with the statement of claims so that there is no chance to destroy evidence. Evidence is then examined exclusively by authorized experts and attorneys bound to confidentiality. The parties do not have access to the confidential information.

<sup>37</sup> Baker & McKenzie (2013) study.

<sup>38</sup> See for instance, Hogan Lovells (2012), §57 regarding Belgium, at p.12.

documents are public and potentially accessible by anyone. Courts have a general duty to adopt adequate measures to safeguard the secret information of a party, for example, by restricting access to those documents which contain trade secrets only to the other party's attorney or to the court's expert (in certain cases the confidential information can be put under closed seals), or not disclosing certain information in the court's final decision (by blanking out the relevant information in the decision and other court's documents). However, according to that study, such measures have proved to be of limited effect to prevent the actual leak of confidential information during proceedings<sup>39</sup>.

#### ***(D.2) The example of antitrust proceedings protecting confidential information***

There are specific rules protecting secrecy of confidential information during antitrust proceedings in the Member States. All of them have measures aimed at protecting business secrets/confidential information from being disclosed during proceedings before national competition authorities, even if the procedural steps needed to obtain protection of secret information varies, to a certain extent, from jurisdiction to jurisdiction. In particular, the involved undertakings have the right to indicate the information that, in their opinion, shall not be divulged<sup>40</sup>. Similar provisions exist at EU level for the antitrust proceedings before the European Commission.

#### **(E) THE SPECIFIC CASE OF TRADE SECRETS WHICH ARE DISCLOSED TO PUBLIC AUTHORITIES PURSUANT TO REGULATORY OBLIGATIONS: EU RULES**

Several EU rules are addressing the specific case of trade secrets which are disclosed to public authorities – normally because of regulatory obligations.

##### ***(E.1) The protection of confidential information in public procurement cases***

Industry often expresses the fear that valuable confidential information (i.e. a trade secret) which is disclosed to a public authorities as part of a tender procedure for public procurement could not be sufficiently protected against misappropriation.

This concern is addressed by EU legislation. Current EU rules provide for protection in this regard: "*Without prejudice to the provisions of this Directive, in particular those concerning the obligations relating to the advertising of awarded contracts and to the information to candidates and tenderers [...] the contracting authority shall not disclose information forwarded to it by economic operators which they have designated as confidential; such information includes, in particular technical or trade secrets and the confidential aspects of tenders.*"<sup>41</sup>

This protection is also integrated in the 2011 Commission proposal for a new directive on public procurement<sup>42</sup>:

<sup>39</sup> Baker & McKenzie study.

<sup>40</sup> According to Baker & McKenzie (2013), however, the secrecy of information may not be sufficient to prevent disclosure when such information is relevant to prove the infringement or for the right of defence of the parties (Bulgaria, Estonia, Germany, Greece, Italy, Luxembourg, Portugal). See Baker & McKenzie study.

<sup>41</sup> Article 6 of Directive 2004/18/EC of the European Parliament and the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts.

<sup>42</sup> Commission proposal for a Directive of the European Parliament and of the Council on public procurement, COM(2011) 896 final, Brussels, 20.12.2011. Negotiations before the European Parliament and the Council are on-going.

- Article 18 of that proposal<sup>43</sup> requires the contracting authority not to disclose information forwarded to it by economic operators which they have designated as confidential, including, but not limited to, technical or trade secrets and the confidential aspects of tenders. In addition, Article 19(2) of the proposal requires the contracting authorities to ensure, in all communication, exchange and storage of information, that the integrity of data and the confidentiality of tenders are preserved.
- Other provisions in the proposal also require the contracting authorities not to reveal to the other participants in the tender solutions proposed or other confidential information communicated by a candidate participating in the "competitive procedure with negotiation"<sup>44</sup> or in the "competitive dialogue"<sup>45</sup> without its agreement. Such agreement shall not take the form of a general waiver but shall be given with reference to the intended communication of specific solutions or other specific confidential information

The underlying rationale was explained by an English Court of Appeal judge as follows: "...it is plain that there is a strong public interest in the maintenance of valuable commercial confidential information ... If the penalty for contracting with public authorities were to be the potential loss of such confidential information, then public authorities and the public interest would be the losers, and the result would be potentially anticompetitive."<sup>46</sup>

***(E.2) The protection of confidentiality of trade secrets disclosed to EU institutions and agencies***

EU institutions have a general policy of transparency and allow third parties to access to the documents they hold, under certain conditions. Given that businesses may disclose confidential business information to EU institutions in the context of specific procedures (e.g. a complaint against a Member State for failure to apply EU law etc) the risk exists that such confidential business information could be disclosed to a third party. This issue is of particular importance when businesses transfer trade secrets to EU regulatory agencies, such as the European Medicines Agency, the European Chemical Agency or the three European financial authorities.

This concern has been considered when adopting the EU general rules<sup>47</sup> dealing with access to documents held by a European institution. Regulation (EC) No 1049/2001<sup>48</sup> provides for the protection of business secrets when the information has been forwarded to a EU institution or body. Article 4(2) states in particular that "*the institutions shall refuse access to a document*

<sup>43</sup> "Article 18  
Confidentiality

1. Unless otherwise provided in this Directive or in the national law concerning access to information, and without prejudice to the obligations relating to the advertising of awarded contracts and to the information to candidates and tenderers set out in Articles 48 and 53 of this Directive, the contracting authority shall not disclose information forwarded to it by economic operators which they have designated as confidential, including, but not limited to, technical or trade secrets and the confidential aspects of tenders.

2. Contracting authorities may impose on economic operators requirements aimed at protecting the confidential nature of information which the contracting authorities make available throughout the procurement procedure."

<sup>44</sup> Cf. Article 27(4) of the proposal.

<sup>45</sup> Cf. Article 28(3) of the proposal.

<sup>46</sup> Veolia vs. Nottinghamshire CC [2010] EWCA 1214 per Rix LJ.

<sup>47</sup> There are specific rules for the access to file in competition cases, see above.

<sup>48</sup> Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. OJ L 145, 31.5.2001, p. 43

where disclosure would undermine the protection of the commercial interests of a natural or legal person, including intellectual property").

EU rules also provide for professional secrecy obligations for their staff. In the case of the EU regulatory agencies, they are under the obligation of professional secrecy and respect of confidentiality of the information when cooperating with other authorities<sup>49</sup>.

***(E.3) The protection of confidentiality of trade secrets disclosed to national supervisory/regulatory agencies***

EU rules also deal with the preservation of confidentiality of information (including business secrets) by national regulatory authorities<sup>50</sup>.

***(E.4) Rules on the non-disclosure of trade secrets to supervisory/regulatory authorities by intermediaries***

Financial intermediaries and some regulated professionals (e.g. lawyers, auditors) often know trade secrets owned by their customers. This is why (inter alia) they are subject to professional secrecy rules, which is a guarantee to their customers.

A specific issue may arise when public authorities require those intermediaries or regulated professionals to disclose to them, in the context of their supervisory functions, confidential information which is sensitive for their customers.

EU rules have addressed this issue and exceptions to the principle of respecting professional secrecy have been established in exceptional circumstances. For instance, the EU anti-money laundering rules<sup>51</sup> require financial intermediaries and regulated professions to disclose to

<sup>49</sup> See for instance Article 70 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), OJ L 331, 15.10.2010, p. 12.

"[...]

2.

*Without prejudice to cases covered by criminal law, any confidential information received by persons referred to in paragraph 1 whilst performing their duties may not be divulged to any person or authority whatsoever, except in summary or aggregate form, such that individual financial institutions cannot be identified.*

*Moreover, the obligation under paragraph 1 and the first subparagraph of this paragraph shall not prevent the Authority and the national supervisory authorities from using the information for the enforcement of the acts referred to in Article 1(2), and in particular for legal procedures for the adoption of decisions.*

3.

*Paragraphs 1 and 2 shall not prevent the Authority from exchanging information with national supervisory authorities in accordance with this Regulation and other Union legislation applicable to financial institutions.*

*That information shall be subject to the conditions of professional secrecy referred to in paragraphs 1 and 2. The Authority shall lay down in its internal rules of procedure the practical arrangements for implementing the confidentiality rules referred to in paragraphs 1 and 2."*

Recital 62 of that Regulation says:

*"It is essential that business secrets and other confidential information be protected. The confidentiality of information made available to the Authority and exchanged in the network should be subject to stringent and effective confidentiality rules."*

<sup>50</sup> See for instance Article 25 of Directive 2004/109/EC of the European Parliament and of the Council of 15 December 2004 on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC, OJ L 390, 31.12.2004, p.38.

<sup>51</sup> Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, p.15.

specific authorities (so-called financial intelligence units) data regarding situations suspected of involve money laundering.

In other cases, EU rules underlined the need to protect the business secrets of clients. A recent Commission legislative proposal indirectly addressed the protection of business secrets in the specific circumstance where an EU auditor would be required by a third country public authority, for their supervisory purposes<sup>52</sup>, to disclose to it audit working papers containing business secrets of the audited entity. In accordance with this proposal, the EU auditor could only transfer the audit working papers to the third country authority provided that "*the protection of the commercial interests of the audited entity, including its industrial and intellectual property is not undermined*"<sup>53</sup>.

---

<sup>52</sup> E.g. the audited entity may be an EU subsidiary of an audited entity of that third country.

<sup>53</sup> Cf. European Commission Proposal of 30 November 2011 for a Directive of the European Parliament and of the council amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts, COM(2011) 778 final. See Article 1(23), introducing a point (ba) in Article 47(2) of Directive 2006/43/EC.



99g

## LEGISLATIVE FRAMEWORK IN EU MEMBER STATES ON THE PROTECTION OF TRADE SECRETS AGAINST MISAPPROPRIATION

*N.B. Unless otherwise stated, the information contained in this annex is based on: (a) the results of a study recently conducted by Hogan Lovells for the Commission on this matter (available at: [http://ec.europa.eu/internal\\_market/iprenforcement/documents/index\\_en.htm#maincontentSec2](http://ec.europa.eu/internal_market/iprenforcement/documents/index_en.htm#maincontentSec2)) and (b) the preliminary results of another study being carried out for the Commission (by Baker & McKenzie, final results expected for 1<sup>st</sup> quarter 2013).*

### INTRODUCTION

Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)<sup>1</sup> requires its signatories to protect "undisclosed information" (see Box 1).

#### **Box 1 - Article 39 of the TRIPS**

*"1. In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967)<sup>2</sup>, Members shall protect undisclosed information in accordance with paragraph 2 and the data submitted to governments or governmental agencies in accordance with paragraph 3.*

*2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices<sup>10</sup> so as long as such information:*

- (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;*
- (b) has commercial value because it is secret; and*
- (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.*

*3. Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use."*

<sup>10</sup> For the purpose of this provision, "a manner contrary to honest commercial practices" shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition.

There is no specific EU law directly dealing with the misappropriation of trade secrets by third parties (i.e. the case referred to in paragraph 2 of Article 39 of the TRIPS). Therefore, the protection of trade secrets against misappropriation by third parties is primarily addressed by national legislation.

National laws in this area provide for different types of protection. Table 1 provides an overview per country of this protection, which is explained the following sections of this Annex.

<sup>1</sup> The TRIPS is a multilateral agreement which must be joined to by all the members of the World Trade Organisation (WTO).

<sup>2</sup> Cf. The Stockholm Act of the Paris Convention for the Protection of Industrial Property, 14 July 1967.



**Table 1 – Main protection against trade secrets misappropriation by national law**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Trade secrets specific law																								✓			
Trade secret protection in intellectual property code															✓							✓					
Unfair competition law (civil and criminal provisions)	✓				✓	✓	✓											✓			✓	✓					
Unfair competition law (civil provisions only)		✓	✓					✓		✓	✓		✓			✓	✓								✓	✓	
Unfair competition law (criminal provisions only)				✓					✓													✓					
Common law (breach of confidence)														✓													✓
Criminal law other than unfair competition	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
Tort law		✓				✓			✓			✓			✓		✓				✓						
Contract law ONLY																			✓								
Labour law																											Most Member States

However, there are EU rules concerning the treatment of confidential information submitted to public authorities pursuant to legal obligations (i.e. corresponding to the case described in paragraph 3 of Article 39 of the TRIPS). See below Section (E).

#### **(A) CIVIL/COMMERCIAL LAW<sup>3</sup>**

##### **(A.1) Civil/commercial law protection in national law: summary**

###### **(i) Summary**

All EU Member States offer some, more or less extensive, form of protection against the misappropriation of trade secrets, albeit this is achieved in different ways.

Some Member States have specific provisions in their civil/commercial law providing protection against the misappropriation of trade secrets

- Sweden has an Act specifically directed against the misappropriation of trade secrets.
- In Italy and Portugal, specific provisions on the protection of trade secrets are included in their respective codes of industrial property – although this does not mean that trade secrets are intellectual property rights.

Other Member States have more general legislation which can be applied.

- Most of them deal with the issue via their law of unfair competition (either civil or criminal provisions, or both): Austria, Belgium, Bulgaria, Czech Republic, Germany, Denmark, Estonia, Greece, Spain, Finland, Hungary, Latvia, Lithuania, Poland, Romania, Slovenia, Slovakia.
- Tort law (or liability for non-contractual responsibility) is used in some countries, either as the main means to address trade secrets misappropriation (Luxembourg, Netherlands) or supplementing the protection offered by unfair competition law (Belgium, Greece).

<sup>3</sup> Understood as opposed to criminal law. It therefore includes: contract law, labour law, unfair competition law, tort law, intellectual property law.

Almost all jurisdictions have general provisions included in their labour laws or civil codes to prevent employees disclosing their employers' trade secrets, at least during the employment relationship. Contract law can be used to protect trade secrets in all of them, but only Malta seems to exclusively rely on contract law to protect trade secrets.

Common law countries (Ireland, United Kingdom) have developed case law (cf. regarding breach of confidence) in the absence of legislation.

*(ii) Civil rules in Member States<sup>4</sup>*

AT (Austria): Austria's Unfair Competition Act provides civil (and criminal) sanctions against trade or business secret misuse by employees and those who exploit such information without consent for the purposes of competition. Other legislation such as the Patents Act and the Criminal Code also provides legal remedies in particular circumstances, such as disclosure of inventions by employees or in cases of industrial espionage. In addition, the Austrian courts have held that obtaining trade or business secrets by breach of confidence (in the course of contractual negotiations) falls within the Unfair Competition Act.

BE (Belgium): There is no one piece of legislation on the protection of trade secrets as such in Belgium but there are several provisions of Belgian law which can be used against the misuse or disclosure of trade secrets. Trade secret owners generally rely on the general law of tort (Article 1382 of the Belgian Civil Code), unfair competition and specific provisions in Belgian labour law.

BG (Bulgaria): There is no specific legislation on trade secrets in Bulgaria but various laws including the Law on Protection of Competition and the Law on Access to Public Information contain general provisions which may be used to protect trade secrets. In fact, there are over 60 such statutory and non-statutory provisions (including criminal liability under the Criminal Code).

CY (Cyprus): There is no specific legislation governing trade secret misuse in Cyprus but there are a number of different laws which mention trade, business and professional secrets. For example, the Commercial Descriptions Law, the General Product Safety Law and the Competition Law. However, liability is criminal; there is no civil liability for trade secret misuse.

CZ (Czech Republic): The Czech Commercial Code defines a trade secret and provides remedies for trade secret infringement. The TRIPS Agreement is directly applicable in Czech law and thus the definition of a trade secret under Article 39(2) of the TRIPS Agreement also applies in Czech law. The basis of trade secret protection in the Czech Commercial Code, however, is the civil law of unfair competition.

DE (Germany): There are a number of provisions in German legislation protecting trade secrets. The most important statutory provisions for the protection of trade secrets are found in the Act against Unfair Competition. These provisions apply to employees and to third parties. Many of the statutes protecting trade secrets under the criminal law also have civil law provisions. These provisions allow for damages and injunctive relief if one of the relevant criminal law provisions is violated. Civil law remedies are also available under the Civil Code (tort law). German contract law also provides effective protection where there is a contractual obligation to maintain the secrecy of trade secrets.

DK (Denmark): In Denmark there is no statutory definition of trade secrets; however case law has clarified the types of information that are protectable to include both technical and

---

<sup>4</sup> See generally Hogan Lovells (2012).

commercial information. Several statutes, both civil and criminal, are used to protect the rights of trade secret owners as well as legal principles derived from contract law, competition law, employment law and unfair competition law. Most notably, the Criminal Code and the Marketing Practices Act contain provisions protecting trade secrets.

EE (Estonia): Estonian legislation provides specific provisions on the protection of trade secrets, most notably in the Competition Act, the Commercial Code, the Employment Contracts Act and the Penal Code. The Competition Act includes an illustrative list of information considered to constitute trade secrets. The Supreme Court has also held that in addition to this definition, the definition of trade secrets provided in the TRIPS Agreement can also be used to interpret the term "trade secrets" under Estonian law.

EL (Greece): Greek Unfair Competition Law provides specific provisions on the protection of trade secrets. More general protection is found in the Greek Civil Code which includes general tort provisions.

ES (Spain): Trade secrets are mainly protected in Spain under the Unfair Competition Act and the Criminal Code. The Act contains provisions specifically aimed at trade secrets. There are also other laws which deal with trade secret protection indirectly, for example, the laws establishing the obligations of directors and other employees.

FI (Finland): There are a number of Acts which include provisions for the protection of trade secrets, most importantly the Unfair Business Practices Act, the Employment Contracts Act and the Criminal Code. Unlike its neighbour, Sweden, Finland does not have one piece of legislation directed specifically to the protection of trade secrets. Although trade secrets are not considered to be typical intellectual property rights, the broad definition of intellectual property rights under Finnish law encompasses their protection under the Unfair Business Practices Act.

FR (France): The only specific trade secrets legislation in French law is that protecting "manufacturing secrets" in the Intellectual Property Code. Other provisions of civil law (tort law) protect trade secrets more generally. The Labour Code also provides criminal liability for trade secret violations by employees or former employees. When parties are bound by a contractual obligation not to disclose secret information, an action lies for breach of contract.

HU (Hungary): Hungarian law provides specific provisions on the protection of trade secrets. The Civil Code and Unfair Competition Act in particular provide specific protection. Provisions also exist in the Labour Code and in various financial/banking laws.

IE (Ireland): There is no specific legislation in Ireland directed to the protection of trade secrets. However, proceedings may be brought under laws relating to breach of confidence, data protection, criminal damage and specific sectorial pieces of legislation. As in England, Irish law has the equitable principle that a person who has received information in confidence cannot take unfair advantage of it. Generally, Irish law imposes a duty of confidentiality in both non-employment cases and employment cases. In both situations, there must be an obligation of confidence and once it is established that such an obligation exists then the person to whom the information is given has a duty to act in good faith and only use the information for the intended purpose. Again, as in England, an obligation to keep information confidential may either be imposed by contract; implied because of the circumstances of the disclosure or implied because of the special relationship between the parties.

IT (Italy): Specific provisions on the protection of trade secrets are contained in the Italian Code of Industrial Property (IPC). Secret information may only be protected if the requirements set out in the IPC are met. There are also general tortious obligations and unfair

competition provisions in the Civil Code which can be employed to compensate for trade secrets misuse.

LT (Lithuania): Lithuanian legislation provides specific provisions on the protection of trade secrets, most importantly in the Civil Code, the Law on Competition, the Labour Code and the Criminal Code. Under the Civil Code, anyone unlawfully acquiring a commercial secret is liable to compensate the owner for the damage caused. There are also express provisions in the Labour Code regarding disclosure by employees who disclose a commercial secret in breach of their employment contract.

LU (Luxembourg): There are no specific legal provisions protecting trade secrets in Luxembourg. However, trade secrets can be protected by unfair competition law, criminal law, tort law and contractual law.

LV (Latvia): Latvia has a number of pieces of legislation which provide specific provisions on the protection of commercial secrets. The Commercial Law is the main Act regulating commercial activities. It defines "commercial secrets" and provides express protection for them. The Labour Law also includes provisions regarding use of commercial secrets by employees. Latvia also has an Unfair Competition Act which expressly provides that the acquisition, use or disclosure of commercial secrets of another competitor without their consent is a form of unfair competition.

MT (Malta): There is no specific legislation on the protection of trade secrets in Malta. Trade secrets may be protected contractually, by express or implied terms, and, an employee is presumed to be under an obligation not to disclose confidential information. If no contract exists there will be no civil law right to protect a trade secret.

NL (Netherlands): There are no specific provisions on the protection of trade secrets in Dutch legislation. In the Netherlands, the protection of trade secrets is based on the general principle of tort law i.e. an unlawful act. In 1919, the Dutch Supreme Court held that the provision in the Dutch Civil Code on unlawful acts could be used to secure protection against trade secret infringement. Contract law also provides some protection in contractual relationships if there are confidentiality obligations in the contract.

PL (Poland): There are specific provisions on the protection of trade secrets in Polish legislation, notably in the Unfair Competition Act. A number of other Acts mention trade secrets, for example, the Civil Code, the Labour Code, the Act on Competition and Consumer Protection, the Code of Commercial Companies and Partnerships etc. The Labour Code includes express provisions requiring employees to maintain the confidentiality of information the disclosure of which could cause damage to their employer.

PT (Portugal): The Portuguese Industrial Property Code has specific provisions relating to the protection of trade secrets. The Industrial Property Code is directed towards unlawful acts against competitors. A violation is punished, not as a crime, but as a misdemeanour. The Labour Code also contains provisions which stipulate that an employee may not disclose information, while employed, relating to his employer's organisation, production methods and company business.

RO (Romania): There is specific legislation in Romania on the protection of trade secrets. Provisions regulating protection of trade secrets have been included in the Law for the Prevention of Unfair Competition ("Law on Unfair Competition") and specify that the unfair use of a competitor's trade secrets is regarded as contrary to honest commercial practices. Trade.

SE (Sweden): Sweden is the only country in the EU to have an Act specifically protecting trade secrets. The Act provides a definition of trade secrets, penalises trade secret espionage and contains provisions on civil liability.

SI (Slovenia): Trade secrets are specifically protected in Slovenia by a number of pieces of legislation, in particular, the Companies Act, the Employment Relationship Act, the Protection of Competition Act, the Penal Code and the Code of Obligations.

SK (Slovakia): Civil protection of trade secrets in the Slovak Republic is regulated by the Commercial Code. The relevant fields of protection are civil law, commercial law, intellectual property law, non-contractual liability and unfair competition law.

UK (United Kingdom): There is no legislation providing specific protection for trade secrets. Trade secrets are protected by contract and/or by the law of equity.

***(A.2) Differences in the scope of protection: the trade secret and the misappropriation***

The absence of homogenous pieces of legislation in this area implies that there is no uniform understanding of what a trade secret is and what misappropriation is:

- In Italy, Lithuania, Portugal and Sweden, there is a specific statutory definition of trade secrets in the applicable legislation.
- A statutory definition of trade secrets is also available in the unfair competition provisions of the Czech Republic, Lithuania and the Slovak Republic.
- In the Czech Republic, Greece, the Netherlands and Spain, the TRIPS definition has been expressly acknowledged and adopted<sup>5</sup>.
- In some cases, definitions of trade secrets can be found in other pieces of laws, for other purposes (e.g. Freedom of Information Act in the UK).

**Comment [AŽ2]:** The statutory definition is provided for in Civil Code of the Republic of Lithuania.

In principle information which meets the requirements of Article 39(2) of the TRIPS<sup>6</sup> would be protectable in all EU Member States. Also, no restrictions seem to exist regarding the type of information which could be protectable and in all EU Member States both technical (e.g. know-how etc.) and commercial secrets (e.g. business strategies etc.). However, the absence of specific definition results in risk of inconsistent interpretation as to what is protectable as trade secrets and consequently, a different protection depending on the type of action initiated by the trade secret owner<sup>7</sup>. Also, differences in courts practices are reported<sup>8</sup>.

Concerning the question of misappropriation, the main divergences relate to the situation of the third party who obtain the secret information in good faith<sup>9</sup>: see below on remedies.

***(A3) Differences in the remedies: injunctions, destruction of goods and compensation for prejudice suffered***

***(i) General***

<sup>5</sup> Cf. Baker & McKenzie study.

<sup>6</sup> In essence, information which is secret, has commercial value (because it is secret) and has been subject to reasonable steps to keep it secret.

<sup>7</sup> Baker & McKenzie study.

<sup>8</sup> Baker & McKenzie study.

<sup>9</sup> To be sure, no Member State grants any action against a third party who autonomously developed the same information.

The remedies available in civil/commercial law proceedings for the misappropriation of trade secrets do vary and appear to depend on the origin of the action (e.g. based on tort, contract law, unfair competition law etc.): see Table 2 for a summary view.

**Table 2 – Available civil remedies**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Injunctions (cease and desist orders): ordinary action	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Injunctions (cease and desist orders): interim relief	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Return/destruction of trade secrets / goods produced using misappropriated trade secrets: ordinary action	✓	✓			✓	✓	✓			✓		✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Return/destruction of trade secrets / goods produced using misappropriated trade secrets: interim relief	✓	✓			✓					✓		✓	✓	✓	✓			✓		✓			✓				✓
Seizure of trade secrets / goods produced using misappropriated trade secrets: ordinary action		✓			✓		✓		✓	✓		✓	✓		✓	✓		✓		✓	✓	✓		✓	✓	✓	✓
Seizure of trade secrets / goods produced using misappropriated trade secrets: interim relief		✓				✓			✓	✓		✓	✓		✓			✓		✓	✓	✓				✓	✓
Withdrawal from the market of goods produced using misappropriated trade secrets: ordinary action		✓			✓		✓		✓	✓		✓	✓		✓	✓		✓		✓	✓	✓	✓	✓	✓		
Withdrawal from the market of goods produced using misappropriated trade secrets: interim relief		✓			✓				✓	✓		✓	✓		✓			✓					✓	✓	✓		
Damages	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Publication of decisions: ordinary action		✓	✓			✓				✓	✓	✓	✓		✓		✓			✓	✓		✓			✓	✓
Publication of decisions: interim relief		✓										✓			✓												
Restraint measures (e.g. penalty for future breach of the Court's order): ordinary action	✓	✓	✓	✓					✓		✓	✓			✓	✓	✓		✓					✓			
Restraint measures (e.g. penalty for future breach of the Court's order): interim relief		✓		✓					✓			✓			✓		✓							✓			

The above remedies are, in general, all cumulatively available to the trade secret owner, with few exceptions. For example, in Belgium, damages are available but not for cease-and-desist claims brought under the Unfair Competition Act (in the form of expedite action). In Bulgaria, it appears that final injunctions are not available (at least cease-and-desist orders in the strict sense of the word) with damages being the usual final remedy. In Latvia, although potentially available, it is not clear which remedies can effectively be used as there is no case law as to whether remedies provided in the Civil Procedure Code for intellectual property rights apply also to trade secrets (trade secrets are not expressly included among the definition of intellectual property). In Italy damages may only be awarded in ordinary proceedings. In Luxembourg, while injunctions are granted by the President of the Commercial Court, damage claims shall be brought before the District Courts.

*(ii) Injunctions (cease and desist orders)*

In general, injunctions (cease and desist orders) are available in all EU Member States. In all Member States, injunctions (i.e. cease and desist orders) are usually available also as interim

relief remedy (i.e. during preliminary and summary proceedings where the claimant's requests are summarily examined by the Court and measures are granted within a very short time limit).

Therefore, there is civil law redress in order to block the commercialisation of goods (or services) which have been manufactured (or designed) using misappropriated trade secrets (so-called "resulting goods/services"). However, this redress varies from Member State to Member State and there is no guarantee that the "resulting goods/services" will be stopped everywhere in the EU. Cease and desist orders against the use of misappropriated trade secrets by third parties (i.e. beyond a contractual relationship) are not always available:

- (i) when trade secrets are protected under unfair competition rules, the trade secret owner needs to sue a competitor but cannot sue a person having the secret with a view to sell it to another third party or to exploit it for other purposes than competing with the original owner of the secret;
- (ii) solutions diverge regarding the possibility to obtain a cease and desist order against negligent third parties or third parties who obtained the misappropriated trade secrets in good faith but before the trade secrets had reached the public domain. In some EU Member States, remedies are potentially available regardless of the recipient's good or bad faith (Austria<sup>10</sup>, Czech Republic, Denmark, Estonia, Finland, Germany, Ireland, Latvia, Lithuania, and Portugal) and injunctions can be obtained also against a third party who obtained the secret in good faith – however, the third party is likely not to be held liable for damages, unless the use of the secret information continues even after the recipient has been informed of the confidential nature of the information. In others, this is not possible<sup>11</sup>; and
- (iii) cease and desist orders may be limited in time even if the trade secret has not yet reached the public domain. Belgium<sup>12</sup>, Cyprus, Denmark<sup>13</sup>, Greece, The Netherlands<sup>14</sup>, Poland and Slovenia, which do not allow unlimited injunctions. In Common Law countries, injunctions are equitable remedies and, as such, courts are free to determine terms and duration of the restrictions.

Concerning the situation of employees, the Baker & McKenzie study finds that though in general, whilst employed, employees have a (statutory) duty of loyalty (including non-disclosure and non-compete obligations) towards the employer, a common practice in most jurisdictions is to provide for non-use and non-disclosure, as well as non-compete clauses in contracts of employment. However, the position differs as to what can be done in relation to an ex-employee who uses or discloses secrets after leaving employment. The balance between the interests of the employer and the employee is indeed assessed differently in the relevant

<sup>10</sup> In Austria, damage claims are also available in cases of default; accordingly damage compensation could be awarded also in case of the third party's slight negligence.

<sup>11</sup> For instance, in the United Kingdom a duty of confidentiality may be implied by the circumstances (the duty of confidentiality is easy to identify in case of an employment contract or a non-disclosure agreement, but it could prove to be very difficult to demonstrate where a person has obtained the confidential information in absence of any relationship between the owner and the recipient), but a person who innocently receives a confidential information will not be under a duty of confidentiality until he is made aware the information is confidential.

<sup>12</sup> In Belgium, courts refuse to grant final injunctions against future trade secrets misappropriation because, contrary to intellectual property rights, trade secret protection can potentially last forever and thus courts are not willing to grant the owner of a trade secret a broader protection than most intellectual property right holders.

<sup>13</sup> In Denmark, although depending on a case by case analysis, final injunctions are usually granted for a period of two to three years from termination of the cooperative relationship.

<sup>14</sup> In Greece and The Netherlands, injunctions are considered temporary in nature.



countries. In general, post-employment, an employee cannot be prevented from using the skill and knowledge gained during the employment, provided that said knowledge does not consist of trade secrets or confidential information that the employee wilfully memorised or (mis)appropriated with the purpose to misuse them after termination of the employment relationship<sup>15</sup>.

*(iii) Destruction of the goods produced using the misappropriate trade secrets or the restitution of the misappropriated information*

Compared to injunctions, other measures such as the destruction of the goods produced using the misappropriate trade secrets or the restitution of the misappropriated information) are not available everywhere and are available in interim proceedings in certain countries only (see [Table A6.2](#)). Since resulting goods are not always destroyed, there is no guarantee for the trade secret owner that such goods will no reappear in the market.

*(iv) Damages*

Compensation for the prejudice suffered from the misappropriation of a trade secret is available in all jurisdictions<sup>16</sup>. Damages claims are mainly based on tort or contract and only in a few cases specific provisions on damages are included in either the unfair competition laws (see for example Spain) or in the specific provisions applying to trade secret misappropriation (Italy and Sweden).

Damages based on tort cover both accruing damages ("*damnum emergens*") and loss of profits ("*lucrum cessans*"). Loss of profits, however, is in most cases very difficult to prove, since the misappropriated information is an intangible asset<sup>17</sup>. This helps explaining the often low compensation obtained<sup>18</sup>. A claim for unjust enrichment is available in some countries

<sup>15</sup> In Denmark (and similarly in Poland), the statutory non-disclosure and non-use obligations survive termination of the employment contract for a period of three years. In Italy, as in many other European countries, non-compete agreements (or clauses) are commonly used to prevent use or disclosure after the contract of employment ceases, albeit offering more limited restrictions than those which exist during the period of employment (to be enforceable non-compete clauses must generally be limited in time and space, identify the activities which the former employee cannot engage in and provide for a monetary compensation). In Sweden, damages for breach of confidentiality obligations after termination of employment are only available where there are "extraordinary circumstances". In Ireland and the United Kingdom there is a distinction between general (low grade) confidential information that the employee is not entitled to disclose whilst employed but can use and disclose thereafter and "real trade secrets" which he cannot disclose or use without authority at any time. The distinction depends on a number of factors including whether the employer impressed the secrecy of the relevant information upon the employee; and whether the "secret" can be readily isolated from other information which the employee is free to use.

<sup>16</sup> In Bulgaria, damage compensation is the sole final remedy available to the owner of a trade secret.

<sup>17</sup> According to Baker & McKenzie, there are often evidentiary problems in proving the loss incurred by the owner of a trade secret. In some countries, damages are awarded only if the claimant is able to demonstrate that he had suffered some loss. Other countries allow courts to award damages on an equitable basis - taking into account all the circumstances of the case - if the claimant has not been able to provide sufficient evidence on the amount of damages

<sup>18</sup> According to Baker & McKenzie, damages vary on a case-by-case basis but the average figures collected during the study "seem not to be particularly encouraging". This study mentions a few cases in Italy and Sweden, where courts awarded high amounts of damages: in Italy, in two cases of trade secrets infringement the Court of Milan awarded damages for EUR 1,100,000.00 and EUR 10,000,000.00, respectively. In Sweden, courts have awarded damages for SEK 7/10,000,000.00 and 48,000,000.00. However, the study reports that these appear to be exceptional cases.

In the Force India Formula One Team Ltd. case, only €25000 were awarded by a UK court to the claimant. The plaintiff had claimed compensation in excess of £13 million (which was based on the assumption that it succeeded in the entirety of its claims for breach of confidence, which it did not). However, the judge did not accept the plaintiff argument that the relevant information was of great

only, such as among others, Belgium, Estonia, Finland, Lithuania and Spain (for further details please see Table 3 below). In some other countries (for example, Austria, Germany, Italy, Ireland, Lithuania, Poland, Sweden and the United Kingdom) the claimant has the right to claim the account of profits obtained by the infringer from its wrongdoing. In most of the cases, however, the account of profits is alternative to the loss of profits or is considered a criterion to calculate said loss. In Italy, the owner of trade secrets may claim the restitution of the infringer's profit in addition to the loss of profits to the extent that the infringer's profits exceed the claimant's loss. In Greece, account of profits and unjust enrichment are alternative ways to calculate the loss of profits. Similarly in The Netherlands loss or profits excludes account of profits.

**Table 3 – Available damages options**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Accruing damage ( <i>damnum emergens</i> )	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Loss of revenues ( <i>lucrum cessans</i> )	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Moral damages			✓						✓				✓	✓						✓	✓	✓				✓	
Punitive damages													✓														✓
Other monetary compensation					✓																✓						
Account of profits	✓			✓	✓	✓		✓	✓		✓		✓	✓	✓		✓	✓		✓	✓			✓		✓	✓
Fair royalty	✓					✓		✓	✓				✓	✓	✓		✓	✓		✓	✓			✓		✓	✓
Unjust enrichment	✓	✓		✓				✓	✓	✓	✓		✓				✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
<i>Ex aequo et bono</i> global account	✓	✓						✓	✓	✓	✓		✓				✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Cumulation of these options	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

**Comment [AŽ3]:** A claim for unjust enrichment is also available in LT.

If damages are claimed on contract, liquidated damages (if provided by the agreement) can also be claimed in addition to damages. Contractual liability, however, is often limited to the damages which were foreseeable at the time of conclusion of the contract.

The available options are in principle all cumulative (exceptions are Austria, Cyprus, Estonia, Finland, France, Germany, Hungary, Ireland, Luxembourg, Portugal, Romania and United Kingdom) provided that the total amount awarded by the court does not exceed the actual claimant's loss. Furthermore, in countries where courts are allowed to award an "*ex aequo et bono*" global amount in cases where damages cannot be alternatively calculated, such criteria are of course to be considered as alternative to all the other available damage options.

Since most of the EU Member States do not have specific criteria for the calculation of damages, they apply the general criteria of tort liability (i.e., *damnum emergens* and *lucrum cessans*). The license analogy has been indicated as a possible criterion for the calculation of damages<sup>19</sup>, among EU Member States in Austria, Denmark, Germany, Greece, Hungary, Italy, The Netherlands and United Kingdom.

## (B) CRIMINAL LAW

### (B.1) Criminal law protection in national law: summary

value and considered that the misuse of the information was limited in nature, purpose and benefit. As a result, the judge considered that €25000 was the figure the parties would have negotiated had they been in the position of a willing licensor and willing licensee acting reasonable as at the date of the breach of confidence.

<sup>19</sup>

This method of calculation is used regarding infringements of intellectual property rights, pursuant to Article 13(1)(b) of Directive 2004/48/EC. This Article provides for the rules on abstract calculation of damages (i.e. calculated on the basis of royalties which could have been due should a licence have existed) as an alternative to the general *damnum emergens* and *lucrum cessans* criteria.

Criminal protection of trade secrets against misappropriation differs from Member State to Member State on several levels, although almost all of them have provisions in this respect. Since there is a lack of a common/shared definition of the scope of trade secrets, the actual extent of the protection provided by states may vary depending on the aims pursued by the provisions implemented for this purpose.

Only a few Member states (i.e., Bulgaria, Ireland, Malta and U.K.) have not established any specific criminal framework with respect to trade secrets violations. However, even in those Member States, the conduct of the infringer may be punished under other related criminal offences (see below). In some cases, where no specific criminal provision has been implemented, penal sanctions of trade secrets misappropriation apply under unfair competition laws or commercial laws. Sweden is the only EU Member state that has implemented a specific law on trade secrets (the Swedish Act on the Protection of Trade Secrets), even though some relevant provisions are also contained in the Criminal Code<sup>20</sup>. Table 4 below summarises the criminal provisions in force:

<i>Table 4 – Criminal provisions applying to trade secrets misappropriation<sup>21</sup></i>																											
	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Criminal code	✓	✓		✓		✓	✓	✓	✓	✓		✓	✓		✓	✓	✓	✓		✓		✓	✓	✓	✓	✓	
Unfair competition / commercial law	✓			✓	✓	✓	✓	✓		✓											✓		✓				
Specific law on trade secrets																								✓			

## **(B.2) Differences in the conducts considered as crimes**

### **(i) Unauthorised disclosure/use of trade secrets**

Many of the countries seem to limit the scope of trade secrets to the information that a company has a reasonable and objective interest to keep confidential, in accordance with an objective criterion (e.g., Austria, Belgium, France, Germany, Hungary, Italy, Lithuania, Luxembourg, Netherlands, Slovakia, Spain, Sweden). Nonetheless, in some cases the relevant protection is afforded to any information having economic value that the owner deems it opportune for his benefit to keep secret according to a subjective criterion and that are subject to reasonable measures for protection of confidentiality (e.g., this broader interpretation seems to be prevailing in Czech Republic, Finland, Greece, Poland, Romania and Slovenia).

- In Austria the offender to be held criminally liable for trade secrets violations must have acted at least with conditional intent. In Belgium, Estonia, Finland, France the conduct may be punished even if the offender acted with negligence.
- Cyprus does not establish any specific requirement that the offender must meet to be charged with criminal liability for trade secret violations. Nor is there any stated obligation on the claimant to keep information confidential.
- In the Czech Republic the offender must act deliberately to commit the offence. As the relevant conduct is defined as an act of unfair competition, the offender must qualify as a competitor or someone participating in the competitive process. The concept of competition has nevertheless been construed very broadly, including even indirect or potential competitors.

<sup>20</sup> In particular, the Act on the Swedish Protection of Trade Secrets establishes two different offences: business espionage and the unauthorized dealing with trade secrets. Other complimentary or more general offences, such as, for instance, unauthorized access to computer systems or breach of faith against principal are regulated under the Criminal Code.

<sup>21</sup> Baker & McKenzie study.

- In Denmark the offences provided for under the Criminal Code require intent. Only upon certain circumstances if the employee causes a substantial risk of dissemination of confidential information by negligence he or she may be charged with criminal liability pursuant to Section 19 of the Marketing Practices Act. without having acted with intent.
- Germany requires that the infringer acts with intent and, specifically, for the purpose of competition, for personal gain, for benefit of a third party or causing damage to the owner of the secret.
- In Greece the offender must act (with intent) for purpose of competition, that means that two criteria have to be met: (i) the conduct of the offender must be suitable to serve the purpose of competition; (ii) he or she must act with the “intention of competition”, i.e. enhance his or third parties’ competitiveness.
- As to Hungary and Italy, the offender may be punished only if he or she acts with intent.
- In Latvia the employer is obliged to identify in writing the information considered to be commercial secrets. In any case, the offender requires the offender to have acted for use or disclosure by himself or another person, therefore intent is required for the offence to occur.
- Lithuania requires that the offender, in case of business espionage, acted with the intent to unlawfully obtain a trade secret, whereas, in the case of violation of trade secrets, major property damage to the victim is required with the intent to get a financial gain or to injure the owner by the disclosure to third parties or the use of the information.

As almost all EU Member states require that the offender acted with intent, it emerges that whoever commits a trade secrets infringement must have clearly the knowledge that the business information constituted trade secrets, even if there is no express obligation to keep such information confidential.

- In Luxembourg, Netherlands and Portugal the offender must act with the intent to reach a competitive advantage or to cause harm to the owner.
- Also Poland requires intent, as the offender must breach an obligation of confidentiality that must be prior established by the owner of the secret, either directly or indirectly.
- Under Romanian and Slovak law the offender must act with intent, but no specific purpose is required.
- The same applies in Slovenia, where if the conduct reaches certain outcome, the offender may be charged with the more severe correspondent penalties.
- Spain also requires intent, even if the purposes to be pursued vary depending on the type of offence considered (for instance, commercial advantage).
- The Swedish Act on the Protection of Trade Secret does not pose any requirement as to the purpose that the offender acts for. It only requires that he acted wilfully and without authorization.

#### *(ii) Related offences*

In Belgium a person who commits the offence under Section 309 of Criminal Code (unauthorized disclosure of trade secrets) may also be charged with theft or misappropriation

(provided that he qualifies as an employee with the company). Similarly, Section 491 applies when a person is entrusted as a data processor/handler manufacturing secrets that are physically stored breaches his duty of confidence.

In Bulgaria, for instance, the offence of business bribery is punishable and applicable to, any individual who discloses to third parties information that he knows in return for something.

In France there is a wide range of crimes that may arise in connection to trade secrets violations:

- First, the offence of theft may occur when the conduct at stake consists in the fraudulent appropriation of third parties' data carriers containing confidential information. Such an offence has been found by the Court of cassation to apply even in connection to disclosure of trade secrets. Theft is punished by imprisonment up to three years and a fine of Euro 45,000.00.
- Additionally, the offence of breach of trust may be committed where an individual with the company misappropriates documents containing confidential information entrusted to them for temporary use. In such a case, the offender shall be punished by imprisonment up to three years or a fine of Euro 375,000.00.
- Also, other provisions of the Criminal Code punish the act of supplying secret information to foreign powers by imprisonment up to fifteen years and a fine of Euro 225,000.00.

In Germany cases of industrial espionage may result in theft or misappropriation.

In Greece the infringement of trade secret may constitute, among other offences, a breach of trust under Section 390 of the Criminal Code. In such a case, the offender shall be punished by imprisonment up to ten years and a fine up to Euro 15,000.00.

Depending on the circumstances, violations of trade secrets may result, further to civil lawsuits, in a number of offences, including but not limited to insider trading, unauthorized access to computer systems and a breach of privacy.

As to Italy, the conduct of the offender who commits an unauthorized use or disclosure of trade secrets may also constitute theft or misappropriation.

In Latvia acts of unauthorized disclosure or acquisition of trade secrets may constitute unfair competition practices where repeated within a one-year period and, thus, result in a punishment by imprisonment of up to two years and a fine, in addition to disqualification penalties.

Violations of trade secrets may constitute fraud or bribery in Lithuania or theft in Luxembourg. In Netherlands the conducts may also result in the theft of secret documents or hacking of computer systems. In Portugal the related offences include computer and communications fraud. Slovakia, in addition to breach of trade secrets, criminalizes the misuse of participation in economic competition through unfair acts.

In Slovenia the same act may be punished under the crime of "disclosure of and unauthorized access to trade secrets" as well as, for instance, the offence of abuse of insider information. Spain provides an extensive regulation of trade secrets infringements: however, pursuant to Section 278.3 of the Criminal Code the specific provisions apply without prejudice to the penalties that may arise for appropriating or destroying the computer media, i.e. for the offences of theft or misappropriation.

In Sweden, further to the offences provided for under the act on the Protection of Trade Secrets, other criminal provisions may apply, including unauthorized access to computer

systems, unlawful dispossession, unlawful use, espionage, unlawful dealing with secret information and negligent dealing with confidential information.

Offences in any way related to trade secrets violations have significant importance in the legal systems that do not establish any specific provision in this respect:

- In Bulgaria violations of trade secrets may be punished only indirectly. The relevant offences in this respect include the disclosure of service/office secrets, the business bribe and computer crimes.
- Under Irish law, for instance, trade secrets infringements may result in: (i) disclosure of personal data obtained without authority; (ii) unauthorised accessing of data; (iii) unlawful use of a computer; (iv) theft or (v) criminal infringements of intellectual property rights.
- Under Maltese criminal law, in the absence of provisions specifically concerning trade secrets, one could be charged with misappropriation and fraudulent gains as a result of his conduct.
- In the U.K. the criminal provisions that may apply in connection to trade secrets infringement cases include theft, fraud, conspiracy to defraud as well as, upon certain circumstances, some of the offences provided for under the Computer Misuse Act (such as unauthorized access to information contained on a computer) and the Data Protection Act (although it is very unlikely that personal data qualify as trade secrets).

### (iii) Qualified offences

Certain Member States also establish qualified offences when the revelation or use of confidential information is committed by a person acting in a particular capacity (e.g., as civil servant, public official, or as person handling confidential information by reason of his job, e.g. lawyers, officers). Please note that this does not mean that for each of the offences a specific provision is established. Separate provisions may have been implemented (e.g. Italy) or, like in Estonia, the same provision may apply to professional and official secrets, also covering trade secrets. See Table 5:

Table 5 – Qualified offences <sup>22</sup>																											
	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Breach of professional secrecy	✓	✓		✓				✓	✓						✓				✓	✓		✓	✓	✓	✓		
Breach of official secret	✓		✓	✓				✓	✓		✓				✓							✓	✓				
Other breach of confidence									✓				✓														
Separate provisions	Y	Y	N	N	N/A		N/A	N	N		Y	N		Y	N				N/A	N		Y	Y			N	

### (iv) Threshold for the applicability of criminal penalties

In the Czech Republic only violations resulting in a damage of at least Euro 2,000.00 may give rise to criminal liability. The offender must cause harm to a competitor or a consumer equivalent to such an amount or provide someone else than the owner of the secret with a benefit of the same amount. The offender does not necessarily need to be a legal person or an enterprise.

<sup>22</sup> Baker & McKenzie study.

A *de minimis* threshold applies for the disclosure of a trade secret in Lithuania, where for the offender to be prosecuted it is required that the conduct caused a damage of at least EUR 5,648.00. However, the threshold does not apply to commercial espionage.

Something like a *de minimis* threshold is established in Poland, where the conduct must have caused substantial damage to the owner, although no quantification of this concept is provided for in the law.

Slovakia establishes that for the offender to be prosecuted a significant damage (more than EUR 26,600.00) must be caused by his conduct to another competitor. It also provides for a more severe penalty in cases where the conduct causes a large scale damage (over EUR 133,000.00).

Also under Estonian and Finnish criminal law a general safe harbor clause applies, preventing prosecution in case the offence is found to be of minor harm.

In Austria the offender will not be prosecuted if his conduct is justified by a compelling public or private interest.

No safe harbor seems to exist in Latvia and Sweden. In Cyprus disclosure of trade secrets is allowed, for instance, when protection of health and safety of citizens is affected, i.e. where compelling public interests are at stake or to prove the violations of statutory provisions.

Similarly, no safe harbor or *de minimis* threshold applies in Denmark, Finland, Italy, Luxembourg, Slovenia. Germany does not provide for any safe harbor; however, disclosure of trade secrets is justified when committed to avert an imminent danger to life, limb, freedom, honour, property or other prevailing legal interests. In Greece trade secrets are not protected in case a witness is examined to represent certain circumstances before the Court, excluding state secrets. In Hungary Section 300(2) of Criminal Code expressly sets forth some safe harbors that justify infringement of trade secrets. These clauses include:

- (i) fulfilment of duties prescribed in a separate act governing the publication of information and information to be disclosed in the public interest;
- (ii) fulfilment of duties subject to statutory reporting obligations, even in the case the report was filed in good faith and proved to be unfounded.

In the Netherlands a specific provision sets out an exemption for those who disclosed in good faith a trade secret assuming that the disclosure was in the public interest. Portugal and Romania consider the consent of the owner to the disclosure of a secret as a safe harbor clause. In addition to that, Romanian law permits the disclosure of trade secrets where compelling public interests are at stake. Spain does not consider information about illegal activities carried out by the owner to be a trade secret: therefore, its revelation would not determine any prosecution.

Generally speaking, the risk of dissemination of confidential information does not amount to a criminal offence (except for Slovakia, Slovenia). The conduct carried out by the infringer must result in an actual violation of the interest protected under the relevant provisions. In contrast, most legal systems (including Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Italy, Latvia, Lithuania, Slovakia, Slovenia) provide criminal protection against the intent to commit a trade secret violation. The acts carried out with the purpose of disclosing or using confidential business information which reach a certain threshold in the realisation of the offence are likely to trigger criminal liability.

### ***(B.3) Differences in the penalties***

The conducts which normally give rise to violations of trade secrets include the access to confidential information, the use or the disclosure thereof or the illicit acquisition for exploitation by the offender or third parties. These conducts are generally punished regardless of the fact that the offender qualifies as a competitor and may be committed either by (past) employees of the company or by external persons (such as consultants, contractors, agents).

It is quite frequent, however, that the violation of trade secrets committed by an employee of the company owning the confidential business information results in a more severe punishment than that provided for the same offence in other cases (i.e., in Belgium, Germany, Greece and Spain).

Table 6 below provides a summary of the main conducts concerning trade secrets violation and the related punishment provided for under the legal systems.

<i>Table 6 – Criminal penalties applying to trade secrets misappropriation<sup>23</sup></i>			
<i>Country</i>	<i>Offender</i>	<i>Conduct</i>	<i>Penalties</i>
Austria	Whoever	Disclosure or exploitation of trade or business secrets	Up to six months imprisonment; up to one year if the conduct is committed with the purpose to obtain a pecuniary advantage or to cause harm to the owner or monetary penalties
		Spying out trade or business secrets for their exploitation by somebody else or disclosure	Up to two years imprisonment OR monetary penalties
		Spying out trade or business secrets for their exploitation abroad	Up to three years imprisonment AND monetary penalties
Belgium	Whoever	Communicating in bad faith manufacturing secrets appropriated during the (past) employment with the owner	From three months up to three years imprisonment AND monetary fine from Euro 50 to 2,000.00
Bulgaria		There is no specific criminal provision concerning violation of trade secrets. However, depending on the characteristics of the conduct, the offender may be charged with more general offences, such as business bribe or computer crimes	
Cyprus	Whoever	Disclosure of trade secrets	Imprisonment up to one year OR monetary fine up to Euro 1,275.00
		Disclosure of information protected by professional secrecy involving trade secrets	Imprisonment up to six months AND/OR monetary fine up to Euro 1,700.00
Czech Republic	Whoever	Acts of unfair competition infringing trade secrets and causing damage in or in excess of Euro 2,000.00 to other competitors/consumers or providing someone with unjustified benefit in the same or greater amount	Monetary fine up to Euro 1.5 Million*
Denmark	Whoever	Unauthorized misuse or appropriation of trade secrets	Imprisonment up to 1 year and 6 months OR monetary fine
		Serious violations such as appropriation of trade secrets in a contract of service or in the performance of assignments	Imprisonment up to six years
Estonia	Whoever	Unauthorized disclosure or use of business secret learned by reason of the professional or official duties with the purpose of causing damage	Imprisonment up to one year OR monetary fine
Finland	Whoever	Disclosure or use of trade secrets known by reason of the employment, position or other lawful activities to obtain financial benefit or to injure the owner	Imprisonment up to two years OR monetary fine
		Misuse of trade secrets obtained or revealed through an unlawful act	Imprisonment up to two years OR monetary fine
		Business espionage: Unlawfully obtaining information regarding trade secrets	Imprisonment up to two years OR monetary fine
France	Whoever	Revelation of manufacturing secrets	Imprisonment up to two years AND monetary fine of Euro 30,000.00
		Theft (for instance, of carriers or materials containing trade secrets)	Imprisonment up to three years AND monetary fine of Euro 45,000.00
Germany	Employees	Unauthorized communication of trade or business secrets that the offender was granted access to for the purpose of obtaining financial advantage or injuring the owner	Imprisonment up to three years OR monetary fine



	Whoever	Unauthorized acquiring or securing trade or business secrets or using thereof	Imprisonment up to three years OR monetary fine. Imprisonment up to five years if aggravating circumstances occur
Greece	Whoever	Copying, printing, using, disclosing or in any way violating data or computer programs constituting secrets of an enterprise	Imprisonment from three months up to one year. Imprisonment from one year to five years if the offender is in the service of the owner and the secrets are of great financial significance
	Employees	Unauthorized communication to third parties of secrets that the offender has known by reason of his employment to obtain financial advantage or to cause a damage to the owner; Unauthorized use of the information so obtained	Imprisonment up to six months AND monetary fine up to Euro 8.80
Hungary	Whoever	Making available to unauthorized persons secrets for financial advantage or to cause damage to others; Using the secrets so obtained	Imprisonment up to three years
Ireland	Not applicable		
Italy	Whoever	Disclosure or use of any information concerning scientific discoveries or inventions or industrial applications that is intended to remain secret known by the offender by reason of his status, function, job or art, to obtain a profit	Imprisonment up to two years
Latvia	Whoever	Revelation of non-disclosable information other than a state secret; Unauthorized acquisition and disclosure of commercial secrets	Imprisonment up to five years OR monetary fine
Lithuania	Whoever	Unlawful acquisition of commercial secrets or communication to third persons; Disclosure of information that the offender was entrusted with by reason of his employment	Imprisonment up to two years <del>or fine (up to 18 825 euro) or restriction of liberty or community service AND/OR disqualification penalties</del>
Luxembourg	Employees	Use or disclosure, during the employment or within two years after its expiration, trade or manufacturing secrets known by reason of the job to obtain financial advantage or to cause damage to the owner	Imprisonment from three months to three years AND monetary fine from Euro 251 to 12,500.00
Malta	Not applicable		
Netherlands	Employee	Intentional disclosure of confidential information that may harm the owner	Imprisonment up to six months AND/OR monetary fine up to Euro 19,500.00
Poland	Whoever	Disclosure or exploitation of trade secret in breach of confidential duties that causes substantial damage to the owner; Use of information illegally acquired or disclosure to third persons	Imprisonment from one month to two years AND monetary fine up to Euro 260,000.00*
Portugal	Whoever	Use or disclosure to third parties of secrets that the offender knows by reason of his status, job, profession or art	Imprisonment up to one year OR monetary fine
Romania	Whoever	Disclosure, acquisition or use of trade secrets without the consent of the owner, as a result of an action of commercial or industrial espionage	Imprisonment from six months up to two years OR monetary fine from Euro 570 to 5,000.00*
		Disclosure of data or information not intended to be publicly known by a person who knows it by reason of his employment, provided that the offence is likely to cause damages	Imprisonment from two up to seven years; Imprisonment from six months to five years if the disclosure is made by another person
Slovakia	Whoever	Spying out trade secrets with the intention to disclose them to unauthorized persons	Imprisonment from six months up to three years; Imprisonment from seven to twelve years if aggravating circumstances occur
Slovenia	Whoever	Disclosure of trade secrets; Providing unauthorized third parties with access to trade secrets; Collection of trade secrets with the purpose of delivering them to unauthorized persons; Unlawful obtainment of trade secrets with the purpose of delivering them to unauthorized persons	Imprisonment up to three years; Imprisonment up to five years if the information is of particular importance
Spain	Whoever	Acquiring data, documents, media and other objects to discover trade secrets; Disclosure, revelation or communication to third parties of the discovered information	Imprisonment from two up to four years AND monetary fine; Imprisonment from three to five years AND monetary fine in case the secrets are disclosed
		Diffusion, disclosure or communication of trade secrets in breach of duties of confidentiality	Imprisonment from two up to four years AND monetary fine, in case the information is disclosed in breach of confidentiality
Sweden	Whoever	Unauthorized access of trade secrets as business espionage	Imprisonment up to two years OR monetary fine; Imprisonment up to six years in case of information of significant importance

		Acquiring trade secrets knowing that the person who made it available accessed the trade secret through acts of business espionage	Imprisonment up to two years OR monetary fine; Imprisonment up to four years in case of information of significant importance
U.K.	Not applicable		

\* Monetary penalties are expressed in local currency and converted to Euro for the reader's convenience

Generally, punishment of the offender is by imprisonment, even though he or she may also be charged, either in addition to that or alternatively, with monetary penalties: see [Table 7 with penalties that shall apply for the main offence \(for instance, unauthorized disclosure/use of trade secrets\)](#).

**Table 7 – Penalties<sup>24</sup>**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Imprisonment OR monetary penalties	✓			✓		✓	✓	✓		✓	✓							✓		✓		✓	✓	✓			
Imprisonment AND monetary penalties		✓							✓	✓		✓					✓			✓	✓						
Imprisonment ONLY													✓		✓	✓									✓	✓	
Monetary penalties ONLY					✓																						
Other penalties					✓											✓							✓				

Hungary, Italy, Lithuania, Slovakia and Slovenia only provide for the imprisonment of the offender whereas in Czech Republic only monetary penalties and, where possible, forfeiture of property shall apply. Lithuania, as well as Romania, also provide for disqualification penalties in addition to imprisonment, such as deprivation of the right to be employed in certain positions or to engage in certain activities. This is a very significant solution, as it directly impacts on the opportunity for the offender to be entrusted with certain responsibilities in his future employment.

With respect to the extent of punishment, the Czech Republic is the state where the heaviest fines apply: under Czech law, the infringer shall be punished with a fine up to 1.5 Million Euro. In contrast, Czech law does not provide for imprisonment in case of trade secrets violations.

In most of states trade secrets infringements are punished with imprisonment up to a term of two-three years. There are a few exceptions: in Denmark the offender may be charged with up to six years imprisonment, provided that serious violations have taken place; in Slovenia imprisonment may be up to five years when the acts carried out by the offender concerns information of particular importance. Under the Swedish Act on the Protection of Trade Secrets, terms of imprisonment of up to six years are foreseen for cases of business espionage and up to four years for the unlawful acquisition of trade secrets of significant importance.

### (C) THE SPECIFIC CASE OF IMPORTS OF GOODS INTO THE EU

In the specific case of goods imported from third countries which would have been manufactured using misappropriated trade secrets of EU companies, there is no specific administrative procedure before customs authorities to block them.

The EU Regulation on customs enforcement of intellectual property rights<sup>25</sup> provides for such administrative customs procedures<sup>26</sup>: the holder of an intellectual property right can ask

<sup>24</sup> Baker & McKenzie study.

<sup>25</sup> Regulation (EC) No 1383/2003 of 22 July 2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have

customs authorities to block imports of goods infringing and intellectual property right. Once the imports blocked, the holder of the intellectual property right has to file a case before a civil court which will decide on the existence (or not) of the infringement. However, this EU rules only applies as regards formal intellectual property rights and do not extent to trade secrets misappropriation claims<sup>27</sup>. Hence, national customs authorities do not process claims for misappropriation of trade secrets.

This situation differs from that in the United States. In the United States, it is possible to engage administrative proceedings before the US International Trade Commission (ITC) in order to block imported goods manufactured using misappropriated trade secrets<sup>28</sup>. Section 337 of the Tariffs Act<sup>29</sup> gives power to the US ITC to deal with claims involving infringements of intellectual property rights but also other forms of unfair competition involving imported products, such as misappropriation of trade secrets. The US ITC has investigative powers. The procedure includes trial proceedings before administrative law judges and review by the US ITC. In terms of remedies, the primary remedy available in Section 337 investigations is an exclusion order that directs US Customs to stop infringing goods from entering the US. In addition, the US ITC may issue cease and desist orders against named importers and other persons engaged in unfair acts that violate Section 337.

Therefore, in order to block goods imported from third countries which would have been manufactured using misappropriated trade secrets of EU companies, the EU owner of the trade secrets in question would need to first go to court in order to have the misappropriation of the trade secrets declared and to obtain an injunction against the third party in question which could be enforced by customs authorities. Compared to formal intellectual property rights, there is therefore an inversion of the burden of proof.

#### **(D) THE PROCEDURAL RULES BEFORE NATIONAL COURTS**

Procedural rules in national law are not always adapted to litigation in trade secrets. Secrecy of information is often at risk during civil proceedings and the absence of protection from (further) disclosure of information as a consequence of court proceedings is a considerable deterrent from starting a legal action<sup>30</sup>.

##### ***(D.1) The insufficient protection of confidential information in national proceedings***

When litigating to defend a trade secret, these procedural rules can result in disclosure of confidential information to the other party or to the public. There are three main situations.

(1) The need to describe the misappropriated trade secret in the application, so that the judge can understand it, could imply that, if the plaintiff does not know the extent of the information misappropriated by the defendant, he could disclose to the defendant (since the application is served to him) more confidential information than actually needed to defend his case<sup>31</sup>.

---

infringed such rights, OJ L 196, 2.8.2003, p.7. The Commission made a proposal in 2011 for a new Regulation concerning customs enforcement of intellectual property rights (COM(2011)285). Negotiations on this text before the European Parliament and the Council are on-going.

<sup>26</sup> Indeed, administrative customs procedures of this type would be a matter of EU law.

<sup>27</sup> Unless of course the claim encompasses both an intellectual property right infringement (e.g. a patent) as well as a trade secrets misappropriation claim.

<sup>28</sup> See generally [http://www.usitc.gov/intellectual\\_property/](http://www.usitc.gov/intellectual_property/)

<sup>29</sup> For the text of Section 337 of the Tariffs Act, see:

[http://www.usitc.gov/intellectual\\_property/documents/statute.pdf](http://www.usitc.gov/intellectual_property/documents/statute.pdf)

<sup>30</sup> Baker & McKenzie study.

<sup>31</sup> See for instance, Hogan Lovells (2012), §57 regarding Belgium, at p.12.

(2) The general rules on the production of evidence could also have the effect of having to disclose information otherwise considered confidential. In common law countries, the pre-trial duty of (full) discovery rules applies; in continental countries, the defendant may ask for certain documents/evidence to be presented by the other party when such evidence lies in the control of that party – which could imply further disclosure of trade secrets. It should be noted that this plays both ways: bad faith plaintiffs could try this way (and therefore abusing the litigation rules) to obtain confidential information from defendants<sup>32</sup>.

(3) The inherent publicity of judicial proceedings (civil proceedings in all EU Member States are public) could also result in the disclosure of trade secrets, in this case to the public:

- Firstly, hearings are often public. While national procedural laws normally include general provisions which allow Courts to exclude the public from the hearing for reasons relating to security, public order and decency, there do not necessarily apply to trade secrets litigation. In some EU Member States (notably Bulgaria<sup>33</sup>, Estonia<sup>34</sup>, Hungary<sup>35</sup>, Germany<sup>36</sup>, The Netherlands, Poland, Romania, Slovakia, Slovenia), a party has the right to request the court to order that the entire proceeding or a part thereof be heard in private to preserve the secrecy of the trade secret. However, according to Baker & McKenzie (2013), this seems to rarely happen in practice and there would be no case law on this point<sup>37</sup>. In the United Kingdom the parties may agree or apply to the Court to ensure that certain information to be revealed during the pre-trial disclosure procedure remains confidential. The parties may enter into a contractual agreement whereby the parties agree that certain information may remain confidential or only be disclosed to legal counsel or where the parties do not reach such agreement, a party may unilaterally apply to the Court requesting that confidential information is not disclosed to the other party during the proceeding. Requests for restriction of disclosure are at the discretion of the Court.
- Judicial decisions may describe the misappropriated trade secret in question when explaining the reasons for the decision<sup>38</sup>; and in some countries other judicial documents (including applications) may be accessed by third parties. According to Baker & McKenzie (2013), in most countries, pleadings and in general court

<sup>32</sup> General procedural rules will normally allow the defendant to refuse to provide a document if it includes a trade secret or a confidential information of the defendant.

<sup>33</sup> In Bulgaria private hearing is specifically provided for cases related to “protection of trade, manufacturing, invention or tax-related secrets” if public disclosure may impair a party’s legitimate interest. When publicity is precluded, only the parties, their attorneys, experts and witnesses are allowed to enter into the court room and are subject to a statutory obligation not to disclose subject matter and content of the relevant proceeding (breach of such obligation entails liability for compensation).

<sup>34</sup> In Estonia (similarly in Finland and Lithuania), in-camera examination can be ordered for the protection of trade secrets if the interest in a public hearing is not deemed to be greater than the commercial interest in protecting the secret.

<sup>35</sup> In Hungary, when the Court orders in-camera examination, the parties are also prohibited from making copies of the minutes of the hearing or of any document containing a trade secret. Examination of documents containing trade secrets is subject to a declaration of non-disclosure and special review procedures are established by the Judge.

<sup>36</sup> In Germany, besides the exclusion of the public if trade secrets are to be discussed, legal practice has developed the so called “Düsseldorf Procedure” (originally developed for patent law claims but likely applicable to trade secrets cases), which consists in a procedure where Courts order independent proceedings for the preservation of evidence as an interim injunction handed to the defendant together with the statement of claims so that there is no chance to destroy evidence. Evidence is then examined exclusively by authorized experts and attorneys bound to confidentiality. The parties do not have access to the confidential information.

<sup>37</sup> Baker & McKenzie (2013) study.

<sup>38</sup> See for instance, Hogan Lovells (2012), §57 regarding Belgium, at p.12.

documents are public and potentially accessible by anyone. Courts have a general duty to adopt adequate measures to safeguard the secret information of a party, for example, by restricting access to those documents which contain trade secrets only to the other party's attorney or to the court's expert (in certain cases the confidential information can be put under closed seals), or not disclosing certain information in the court's final decision (by blanking out the relevant information in the decision and other court's documents). However, according to that study, such measures have proved to be of limited effect to prevent the actual leak of confidential information during proceedings<sup>39</sup>.

#### ***(D.2) The example of antitrust proceedings protecting confidential information***

There are specific rules protecting secrecy of confidential information during antitrust proceedings in the Member States. All of them have measures aimed at protecting business secrets/confidential information from being disclosed during proceedings before national competition authorities, even if the procedural steps needed to obtain protection of secret information varies, to a certain extent, from jurisdiction to jurisdiction. In particular, the involved undertakings have the right to indicate the information that, in their opinion, shall not be divulged<sup>40</sup>. Similar provisions exist at EU level for the antitrust proceedings before the European Commission.

#### **(E) THE SPECIFIC CASE OF TRADE SECRETS WHICH ARE DISCLOSED TO PUBLIC AUTHORITIES PURSUANT TO REGULATORY OBLIGATIONS: EU RULES**

Several EU rules are addressing the specific case of trade secrets which are disclosed to public authorities – normally because of regulatory obligations.

##### ***(E.1) The protection of confidential information in public procurement cases***

Industry often expresses the fear that valuable confidential information (i.e. a trade secret) which is disclosed to a public authorities as part of a tender procedure for public procurement could not be sufficiently protected against misappropriation.

This concern is addressed by EU legislation. Current EU rules provide for protection in this regard: "*Without prejudice to the provisions of this Directive, in particular those concerning the obligations relating to the advertising of awarded contracts and to the information to candidates and tenderers [...] the contracting authority shall not disclose information forwarded to it by economic operators which they have designated as confidential; such information includes, in particular technical or trade secrets and the confidential aspects of tenders.*"<sup>41</sup>

This protection is also integrated in the 2011 Commission proposal for a new directive on public procurement<sup>42</sup>:

---

<sup>39</sup> Baker & McKenzie study.

<sup>40</sup> According to Baker & McKenzie (2013), however, the secrecy of information may not be sufficient to prevent disclosure when such information is relevant to prove the infringement or for the right of defence of the parties (Bulgaria, Estonia, Germany, Greece, Italy, Luxembourg, Portugal). See Baker & McKenzie study.

<sup>41</sup> Article 6 of Directive 2004/18/EC of the European Parliament and the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts.

<sup>42</sup> Commission proposal for a Directive of the European Parliament and of the Council on public procurement, COM(2011) 896 final, Brussels, 20.12.2011. Negotiations before the European Parliament and the Council are on-going.

- Article 18 of that proposal<sup>43</sup> requires the contracting authority not to disclose information forwarded to it by economic operators which they have designated as confidential, including, but not limited to, technical or trade secrets and the confidential aspects of tenders. In addition, Article 19(2) of the proposal requires the contracting authorities to ensure, in all communication, exchange and storage of information, that the integrity of data and the confidentiality of tenders are preserved.
- Other provisions in the proposal also require the contracting authorities not to reveal to the other participants in the tender solutions proposed or other confidential information communicated by a candidate participating in the "competitive procedure with negotiation"<sup>44</sup> or in the "competitive dialogue"<sup>45</sup> without its agreement. Such agreement shall not take the form of a general waiver but shall be given with reference to the intended communication of specific solutions or other specific confidential information

The underlying rationale was explained by an English Court of Appeal judge as follows: "...it is plain that there is a strong public interest in the maintenance of valuable commercial confidential information ... If the penalty for contracting with public authorities were to be the potential loss of such confidential information, then public authorities and the public interest would be the losers, and the result would be potentially anticompetitive."<sup>46</sup>

**(E.2) The protection of confidentiality of trade secrets disclosed to EU institutions and agencies**

EU institutions have a general policy of transparency and allow third parties to access to the documents they hold, under certain conditions. Given that businesses may disclose confidential business information to EU institutions in the context of specific procedures (e.g. a complaint against a Member State for failure to apply EU law etc) the risk exists that such confidential business information could be disclosed to a third party. This issue is of particular importance when businesses transfer trade secrets to EU regulatory agencies, such as the European Medicines Agency, the European Chemical Agency or the three European financial authorities.

This concern has been considered when adopting the EU general rules<sup>47</sup> dealing with access to documents held by a European institution. Regulation (EC) No 1049/2001<sup>48</sup> provides for the protection of business secrets when the information has been forwarded to a EU institution or body. Article 4(2) states in particular that "*the institutions shall refuse access to a document*

<sup>43</sup> "Article 18  
Confidentiality

1. Unless otherwise provided in this Directive or in the national law concerning access to information, and without prejudice to the obligations relating to the advertising of awarded contracts and to the information to candidates and tenderers set out in Articles 48 and 53 of this Directive, the contracting authority shall not disclose information forwarded to it by economic operators which they have designated as confidential, including, but not limited to, technical or trade secrets and the confidential aspects of tenders.

2. Contracting authorities may impose on economic operators requirements aimed at protecting the confidential nature of information which the contracting authorities make available throughout the procurement procedure."

<sup>44</sup> Cf. Article 27(4) of the proposal.

<sup>45</sup> Cf. Article 28(3) of the proposal.

<sup>46</sup> Veolia vs. Nottinghamshire CC [2010] EWCA 1214 per Rix LJ.

<sup>47</sup> There are specific rules for the access to file in competition cases, see above.

<sup>48</sup> Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. OJ L 145, 31.5.2001, p. 43

where disclosure would undermine the protection of the commercial interests of a natural or legal person, including intellectual property").

EU rules also provide for professional secrecy obligations for their staff. In the case of the EU regulatory agencies, they are under the obligation of professional secrecy and respect of confidentiality of the information when cooperating with other authorities<sup>49</sup>.

***(E.3) The protection of confidentiality of trade secrets disclosed to national supervisory/regulatory agencies***

EU rules also deal with the preservation of confidentiality of information (including business secrets) by national regulatory authorities<sup>50</sup>.

***(E.4) Rules on the non-disclosure of trade secrets to supervisory/regulatory authorities by intermediaries***

Financial intermediaries and some regulated professionals (e.g. lawyers, auditors) often know trade secrets owned by their customers. This is why (inter alia) they are subject to professional secrecy rules, which is a guarantee to their customers.

A specific issue may arise when public authorities require those intermediaries or regulated professionals to disclose to them, in the context of their supervisory functions, confidential information which is sensitive for their customers.

EU rules have addressed this issue and exceptions to the principle of respecting professional secrecy have been established in exceptional circumstances. For instance, the EU anti-money laundering rules<sup>51</sup> require financial intermediaries and regulated professions to disclose to

<sup>49</sup> See for instance Article 70 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), OJ L 331, 15.10.2010, p. 12.

"[...]

2.

*Without prejudice to cases covered by criminal law, any confidential information received by persons referred to in paragraph 1 whilst performing their duties may not be divulged to any person or authority whatsoever, except in summary or aggregate form, such that individual financial institutions cannot be identified.*

*Moreover, the obligation under paragraph 1 and the first subparagraph of this paragraph shall not prevent the Authority and the national supervisory authorities from using the information for the enforcement of the acts referred to in Article 1(2), and in particular for legal procedures for the adoption of decisions.*

3.

*Paragraphs 1 and 2 shall not prevent the Authority from exchanging information with national supervisory authorities in accordance with this Regulation and other Union legislation applicable to financial institutions.*

*That information shall be subject to the conditions of professional secrecy referred to in paragraphs 1 and 2. The Authority shall lay down in its internal rules of procedure the practical arrangements for implementing the confidentiality rules referred to in paragraphs 1 and 2."*

Recital 62 of that Regulation says:

*"It is essential that business secrets and other confidential information be protected. The confidentiality of information made available to the Authority and exchanged in the network should be subject to stringent and effective confidentiality rules."*

<sup>50</sup> See for instance Article 25 of Directive 2004/109/EC of the European Parliament and of the Council of 15 December 2004 on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC, OJ L 390, 31.12.2004, p.38.

<sup>51</sup> Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, p.15.

specific authorities (so-called financial intelligence units) data regarding situations suspected of involve money laundering.

In other cases, EU rules underlined the need to protect the business secrets of clients. A recent Commission legislative proposal indirectly addressed the protection of business secrets in the specific circumstance where an EU auditor would be required by a third country public authority, for their supervisory purposes<sup>52</sup>, to disclose to it audit working papers containing business secrets of the audited entity. In accordance with this proposal, the EU auditor could only transfer the audit working papers to the third country authority provided that "*the protection of the commercial interests of the audited entity, including its industrial and intellectual property is not undermined*"<sup>53</sup>.

<sup>52</sup>

E.g. the audited entity may be an EU subsidiary of an audited entity of that third country.

<sup>53</sup>

Cf. European Commission Proposal of 30 November 2011 for a Directive of the European Parliament and of the council amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts, COM(2011) 778 final. See Article 1(23), introducing a point (ba) in Article 47(2) of Directive 2006/43/EC.





996

## POLAND

1. Point A2 – There is a definition of a trade secret in PL national law – article 11 point 4 of the Act on combating unfair competition
2. Table 6 and 7 – penalties: according to the table there is: Imprisonment from one month to two years AND monetary fine up to Euro 260,000.00, according to my experts there should be: Fine, restriction of liberty or imprisonment up to 2 years (according to Article 23 of the above-mentioned Act).



## LEGISLATIVE FRAMEWORK IN EU MEMBER STATES ON THE PROTECTION OF TRADE SECRETS AGAINST MISAPPROPRIATION

*N.B. Unless otherwise stated, the information contained in this annex is based on: (a) the results of a study recently conducted by Hogan Lovells for the Commission on this matter (available at: [http://ec.europa.eu/internal\\_market/iprenforcement/documents/index\\_en.htm#maincontentSec2](http://ec.europa.eu/internal_market/iprenforcement/documents/index_en.htm#maincontentSec2)) and (b) the preliminary results of another study being carried out for the Commission (by Baker & McKenzie, final results expected for 1<sup>st</sup> quarter 2013).*

### INTRODUCTION

Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)<sup>1</sup> requires its signatories to protect "undisclosed information" (see Box 1).

#### **Box 1 - Article 39 of the TRIPS**

*"1. In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967)<sup>2</sup>, Members shall protect undisclosed information in accordance with paragraph 2 and the data submitted to governments or governmental agencies in accordance with paragraph 3.*

*2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices<sup>10</sup> so as long as such information:*

- (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;*
- (b) has commercial value because it is secret; and*
- (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.*

*3. Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use."*

<sup>10</sup> For the purpose of this provision, "a manner contrary to honest commercial practices" shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition.

There is no specific EU law directly dealing with the misappropriation of trade secrets by third parties (i.e. the case referred to in paragraph 2 of Article 39 of the TRIPS). Therefore, the protection of trade secrets against misappropriation by third parties is primarily addressed by national legislation.

National laws in this area provide for different types of protection. Table 1 provides an overview per country of this protection, which is explained the following sections of this Annex.

<sup>1</sup> The TRIPS is a multilateral agreement which must be joined to by all the members of the World Trade Organisation (WTO).

<sup>2</sup> Cf. The Stockholm Act of the Paris Convention for the Protection of Industrial Property, 14 July 1967.

**Table 1 – Main protection against trade secrets misappropriation by national law**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Trade secrets specific law																								✓			
Trade secret protection in intellectual property code															✓						✓						
Unfair competition law (civil and criminal provisions)	✓				✓	✓	✓											✓			✓		✓				
Unfair competition law (civil provisions only)		✓	✓					✓		✓	✓		✓			✓	✓								✓	✓	✓
Unfair competition law (criminal provisions only)				✓					✓													✓					
Common law (breach of confidence)														✓													✓
Criminal law other than unfair competition	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Tort law		✓				✓			✓			✓			✓		✓			✓							
Contract law ONLY																				✓							
Labour law																											Most Member States

Most Member States

However, there are EU rules concerning the treatment of confidential information submitted to public authorities pursuant to legal obligations (i.e. corresponding to the case described in paragraph 3 of Article 39 of the TRIPS). See below [Section \(E\)](#).

#### (A) CIVIL/COMMERCIAL LAW<sup>3</sup>

##### (A.1) Civil/commercial law protection in national law: summary

###### (i) Summary

All EU Member States offer some, more or less extensive, form of protection against the misappropriation of trade secrets, albeit this is achieved in different ways.

Some Member States have specific provisions in their civil/commercial law providing protection against the misappropriation of trade secrets

- Sweden has an Act specifically directed against the misappropriation of trade secrets.
- In Italy and Portugal, specific provisions on the protection of trade secrets are included in their respective codes of industrial property – although this does not mean that trade secrets are intellectual property rights.

Other Member States have more general legislation which can be applied.

- Most of them deal with the issue via their law of unfair competition (either civil or criminal provisions, or both): Austria, Belgium, Bulgaria, Czech Republic, Germany, Denmark, Estonia, Greece, Spain, Finland, Hungary, Latvia, Lithuania, Poland, Romania, Slovenia, Slovakia.
- Tort law (or liability for non-contractual responsibility) is used in some countries, either as the main means to address trade secrets misappropriation (Luxembourg, Netherlands) or supplementing the protection offered by unfair competition law (Belgium, Greece).

<sup>3</sup> Understood as opposed to criminal law. It therefore includes: contract law, labour law, unfair competition law, tort law, intellectual property law.

Almost all jurisdictions have general provisions included in their labour laws or civil codes to prevent employees disclosing their employers' trade secrets, at least during the employment relationship. Contract law can be used to protect trade secrets in all of them, but only Malta seems to exclusively rely on contract law to protect trade secrets.

Common law countries (Ireland, United Kingdom) have developed case law (cf. regarding breach of confidence) in the absence of legislation.

*(ii) Civil rules in Member States<sup>4</sup>*

AT (Austria): Austria's Unfair Competition Act provides civil (and criminal) sanctions against trade or business secret misuse by employees and those who exploit such information without consent for the purposes of competition. Other legislation such as the Patents Act and the Criminal Code also provides legal remedies in particular circumstances, such as disclosure of inventions by employees or in cases of industrial espionage. In addition, the Austrian courts have held that obtaining trade or business secrets by breach of confidence (in the course of contractual negotiations) falls within the Unfair Competition Act.

BE (Belgium): There is no one piece of legislation on the protection of trade secrets as such in Belgium but there are several provisions of Belgian law which can be used against the misuse or disclosure of trade secrets. Trade secret owners generally rely on the general law of tort (Article 1382 of the Belgian Civil Code), unfair competition and specific provisions in Belgian labour law.

BG (Bulgaria): There is no specific legislation on trade secrets in Bulgaria but various laws including the Law on Protection of Competition and the Law on Access to Public Information contain general provisions which may be used to protect trade secrets. In fact, there are over 60 such statutory and non-statutory provisions (including criminal liability under the Criminal Code).

CY (Cyprus): There is no specific legislation governing trade secret misuse in Cyprus but there are a number of different laws which mention trade, business and professional secrets. For example, the Commercial Descriptions Law, the General Product Safety Law and the Competition Law. However, liability is criminal; there is no civil liability for trade secret misuse.

CZ (Czech Republic): The Czech Commercial Code defines a trade secret and provides remedies for trade secret infringement. The TRIPS Agreement is directly applicable in Czech law and thus the definition of a trade secret under Article 39(2) of the TRIPS Agreement also applies in Czech law. The basis of trade secret protection in the Czech Commercial Code, however, is the civil law of unfair competition.

DE (Germany): There are a number of provisions in German legislation protecting trade secrets. The most important statutory provisions for the protection of trade secrets are found in the Act against Unfair Competition. These provisions apply to employees and to third parties. Many of the statutes protecting trade secrets under the criminal law also have civil law provisions. These provisions allow for damages and injunctive relief if one of the relevant criminal law provisions is violated. Civil law remedies are also available under the Civil Code (tort law). German contract law also provides effective protection where there is a contractual obligation to maintain the secrecy of trade secrets.

DK (Denmark): In Denmark there is no statutory definition of trade secrets; however case law has clarified the types of information that are protectable to include both technical and

---

<sup>4</sup> See generally Hogan Lovells (2012).

commercial information. Several statutes, both civil and criminal, are used to protect the rights of trade secret owners as well as legal principles derived from contract law, competition law, employment law and unfair competition law. Most notably, the Criminal Code and the Marketing Practices Act contain provisions protecting trade secrets.

EE (Estonia): Estonian legislation provides specific provisions on the protection of trade secrets, most notably in the Competition Act, the Commercial Code, the Employment Contracts Act and the Penal Code. The Competition Act includes an illustrative list of information considered to constitute trade secrets. The Supreme Court has also held that in addition to this definition, the definition of trade secrets provided in the TRIPS Agreement can also be used to interpret the term "trade secrets" under Estonian law.

EL (Greece): Greek Unfair Competition Law provides specific provisions on the protection of trade secrets. More general protection is found in the Greek Civil Code which includes general tort provisions.

ES (Spain): Trade secrets are mainly protected in Spain under the Unfair Competition Act and the Criminal Code. The Act contains provisions specifically aimed at trade secrets. There are also other laws which deal with trade secret protection indirectly, for example, the laws establishing the obligations of directors and other employees.

FI (Finland): There are a number of Acts which include provisions for the protection of trade secrets, most importantly the Unfair Business Practices Act, the Employment Contracts Act and the Criminal Code. Unlike its neighbour, Sweden, Finland does not have one piece of legislation directed specifically to the protection of trade secrets. Although trade secrets are not considered to be typical intellectual property rights, the broad definition of intellectual property rights under Finnish law encompasses their protection under the Unfair Business Practices Act.

FR (France): The only specific trade secrets legislation in French law is that protecting "manufacturing secrets" in the Intellectual Property Code. Other provisions of civil law (tort law) protect trade secrets more generally. The Labour Code also provides criminal liability for trade secret violations by employees or former employees. When parties are bound by a contractual obligation not to disclose secret information, an action lies for breach of contract.

HU (Hungary): Hungarian law provides specific provisions on the protection of trade secrets. The Civil Code and Unfair Competition Act in particular provide specific protection. Provisions also exist in the Labour Code and in various financial/banking laws.

IE (Ireland): There is no specific legislation in Ireland directed to the protection of trade secrets. However, proceedings may be brought under laws relating to breach of confidence, data protection, criminal damage and specific sectorial pieces of legislation. As in England, Irish law has the equitable principle that a person who has received information in confidence cannot take unfair advantage of it. Generally, Irish law imposes a duty of confidentiality in both non-employment cases and employment cases. In both situations, there must be an obligation of confidence and once it is established that such an obligation exists then the person to whom the information is given has a duty to act in good faith and only use the information for the intended purpose. Again, as in England, an obligation to keep information confidential may either be imposed by contract; implied because of the circumstances of the disclosure or implied because of the special relationship between the parties.

IT (Italy): Specific provisions on the protection of trade secrets are contained in the Italian Code of Industrial Property (IPC). Secret information may only be protected if the requirements set out in the IPC are met. There are also general tortious obligations and unfair

competition provisions in the Civil Code which can be employed to compensate for trade secrets misuse.

LT (Lithuania): Lithuanian legislation provides specific provisions on the protection of trade secrets, most importantly in the Civil Code, the Law on Competition, the Labour Code and the Criminal Code. Under the Civil Code, anyone unlawfully acquiring a commercial secret is liable to compensate the owner for the damage caused. There are also express provisions in the Labour Code regarding disclosure by employees who disclose a commercial secret in breach of their employment contract.

LU (Luxembourg): There are no specific legal provisions protecting trade secrets in Luxembourg. However, trade secrets can be protected by unfair competition law, criminal law, tort law and contractual law.

LV (Latvia): Latvia has a number of pieces of legislation which provide specific provisions on the protection of commercial secrets. The Commercial Law is the main Act regulating commercial activities. It defines "commercial secrets" and provides express protection for them. The Labour Law also includes provisions regarding use of commercial secrets by employees. Latvia also has an Unfair Competition Act which expressly provides that the acquisition, use or disclosure of commercial secrets of another competitor without their consent is a form of unfair competition.

MT (Malta): There is no specific legislation on the protection of trade secrets in Malta. Trade secrets may be protected contractually, by express or implied terms, and, an employee is presumed to be under an obligation not to disclose confidential information. If no contract exists there will be no civil law right to protect a trade secret.

NL (Netherlands): There are no specific provisions on the protection of trade secrets in Dutch legislation. In the Netherlands, the protection of trade secrets is based on the general principle of tort law i.e. an unlawful act. In 1919, the Dutch Supreme Court held that the provision in the Dutch Civil Code on unlawful acts could be used to secure protection against trade secret infringement. Contract law also provides some protection in contractual relationships if there are confidentiality obligations in the contract.

PL (Poland): There are specific provisions on the protection of trade secrets in Polish legislation, notably in the Unfair Competition Act. A number of other Acts mention trade secrets, for example, the Civil Code, the Labour Code, the Act on Competition and Consumer Protection, the Code of Commercial Companies and Partnerships etc. The Labour Code includes express provisions requiring employees to maintain the confidentiality of information the disclosure of which could cause damage to their employer.

PT (Portugal): The Portuguese Industrial Property Code has specific provisions relating to the protection of trade secrets. The Industrial Property Code is directed towards unlawful acts against competitors. A violation is punished, not as a crime, but as a misdemeanour. The Labour Code also contains provisions which stipulate that an employee may not disclose information, while employed, relating to his employer's organisation, production methods and company business.

**Comment [CA2]:** In Portugal, trade secrets misappropriation is considered an unfair competition act (administrative offense punished by a fine).

RO (Romania): There is specific legislation in Romania on the protection of trade secrets. Provisions regulating protection of trade secrets have been included in the Law for the Prevention of Unfair Competition ("Law on Unfair Competition") and specify that the unfair use of a competitor's trade secrets is regarded as contrary to honest commercial practices. Trade.



SE (Sweden): Sweden is the only country in the EU to have an Act specifically protecting trade secrets. The Act provides a definition of trade secrets, penalises trade secret espionage and contains provisions on civil liability.

SI (Slovenia): Trade secrets are specifically protected in Slovenia by a number of pieces of legislation, in particular, the Companies Act, the Employment Relationship Act, the Protection of Competition Act, the Penal Code and the Code of Obligations.

SK (Slovakia): Civil protection of trade secrets in the Slovak Republic is regulated by the Commercial Code. The relevant fields of protection are civil law, commercial law, intellectual property law, non-contractual liability and unfair competition law.

UK (United Kingdom): There is no legislation providing specific protection for trade secrets. Trade secrets are protected by contract and/or by the law of equity.

***(A.2) Differences in the scope of protection: the trade secret and the misappropriation***

The absence of homogenous pieces of legislation in this area implies that there is no uniform understanding of what a trade secret is and what misappropriation is:

- In Italy, Portugal and Sweden, there is a specific statutory definition of trade secrets in the applicable legislation.
- A statutory definition of trade secrets is also available in the unfair competition provisions of the Czech Republic, Lithuania and the Slovak Republic.
- In the Czech Republic, Greece, the Netherlands and Spain, the TRIPS definition has been expressly acknowledged and adopted<sup>5</sup>.
- In some cases, definitions of trade secrets can be found in other pieces of laws, for other purposes (e.g. Freedom of Information Act in the UK).

In principle information which meets the requirements of Article 39(2) of the TRIPS<sup>6</sup> would be protectable in all EU Member States. Also, no restrictions seem to exist regarding the type of information which could be protectable and in all EU Member States both technical (e.g. know-how etc.) and commercial secrets (e.g. business strategies etc.). However, the absence of specific definition results in risk of inconsistent interpretation as to what is protectable as trade secrets and consequently, a different protection depending on the type of action initiated by the trade secret owner<sup>7</sup>. Also, differences in courts practices are reported<sup>8</sup>.

Concerning the question of misappropriation, the main divergences relate to the situation of the third party who obtain the secret information in good faith<sup>9</sup>: see below on remedies.

***(A3) Differences in the remedies: injunctions, destruction of goods and compensation for prejudice suffered***

***(i) General***

---

<sup>5</sup> Cf. Baker & McKenzie study.

<sup>6</sup> In essence, information which is secret, has commercial value (because it is secret) and has been subject to reasonable steps to keep it secret.

<sup>7</sup> Baker & McKenzie study.

<sup>8</sup> Baker & McKenzie study.

<sup>9</sup> To be sure, no Member State grants any action against a third party who autonomously developed the same information.

The remedies available in civil/commercial law proceedings for the misappropriation of trade secrets do vary and appear to depend on the origin of the action (e.g. based on tort, contract law, unfair competition law etc.): see Table 2 for a summary view.

**Table 2 – Available civil remedies**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Injunctions (cease and desist orders: ordinary action	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Injunctions (cease and desist orders: interim relief	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Return/destruction of trade secrets / goods produced using misappropriated trade secrets: ordinary action	✓	✓			✓	✓	✓		✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Return/destruction of trade secrets / goods produced using misappropriated trade secrets: interim relief	✓	✓			✓				✓			✓	✓	✓	✓		✓		✓				✓				✓
Seizure of trade secrets / goods produced using misappropriated trade secrets: ordinary action		✓			✓		✓		✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Seizure of trade secrets / goods produced using misappropriated trade secrets: interim relief		✓				✓		✓	✓	✓		✓	✓		✓		✓		✓	✓	✓	✓				✓	✓
Withdrawal from the market of goods produced using misappropriated trade secrets: ordinary action		✓			✓		✓		✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Withdrawal from the market of goods produced using misappropriated trade secrets: interim relief		✓			✓				✓	✓		✓	✓		✓		✓		✓			✓	✓	✓			
Damages	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Publication of decisions: ordinary action		✓	✓				✓			✓	✓	✓	✓		✓		✓			✓	✓	✓	✓	✓		✓	✓
Publication of decisions: interim relief		✓										✓			✓												
Restraint measures (e.g. penalty for future breach of the Court's order): ordinary action	✓	✓	✓	✓					✓		✓	✓			✓	✓	✓			✓				✓			
Restraint measures (e.g. penalty for future breach of the Court's order): interim relief		✓		✓					✓			✓			✓		✓							✓			

Comment [CA3]: Insert

The above remedies are, in general, all cumulatively available to the trade secret owner, with few exceptions. For example, in Belgium, damages are available but not for cease-and-desist claims brought under the Unfair Competition Act (in the form of expedite action). In Bulgaria, it appears that final injunctions are not available (at least cease-and-desist orders in the strict sense of the word) with damages being the usual final remedy. In Latvia, although potentially available, it is not clear which remedies can effectively be used as there is no case law as to whether remedies provided in the Civil Procedure Code for intellectual property rights apply also to trade secrets (trade secrets are not expressly included among the definition of intellectual property). In Italy damages may only be awarded in ordinary proceedings. In Luxembourg, while injunctions are granted by the President of the Commercial Court, damage claims shall be brought before the District Courts.

(ii) Injunctions (cease and desist orders)

In general, injunctions (cease and desist orders) are available in all EU Member States. In all Member States, injunctions (i.e. cease and desist orders) are usually available also as interim relief remedy (i.e. during preliminary and summary proceedings where the claimant's requests are summarily examined by the Court and measures are granted within a very short time limit).

Therefore, there is civil law redress in order to block the commercialisation of goods (or services) which have been manufactured (or designed) using misappropriated trade secrets (so-called "resulting goods/services"). However, this redress varies from Member State to Member State and there is no guarantee that the "resulting goods/services" will be stopped everywhere in the EU. Cease and desist orders against the use of misappropriated trade secrets by third parties (i.e. beyond a contractual relationship) are not always available:

- (i) when trade secrets are protected under unfair competition rules, the trade secret owner needs to sue a competitor but cannot sue a person having the secret with a view to sell it to another third party or to exploit it for other purposes than competing with the original owner of the secret;
- (ii) solutions diverge regarding the possibility to obtain a cease and desist order against negligent third parties or third parties who obtained the misappropriated trade secrets in good faith but before the trade secrets had reached the public domain. In some EU Member States, remedies are potentially available regardless of the recipient's good or bad faith (Austria<sup>10</sup>, Czech Republic, Denmark, Estonia, Finland, Germany, Ireland, Latvia, Lithuania, and Portugal) and injunctions can be obtained also against a third party who obtained the secret in good faith – however, the third party is likely not to be held liable for damages, unless the use of the secret information continues even after the recipient has been informed of the confidential nature of the information. In others, this is not possible<sup>11</sup>; and
- (iii) cease and desist orders may be limited in time even if the trade secret has not yet reached the public domain. Belgium<sup>12</sup>, Cyprus, Denmark<sup>13</sup>, Greece, The Netherlands<sup>14</sup>, Poland and Slovenia, which do not allow unlimited injunctions. In Common Law countries, injunctions are equitable remedies and, as such, courts are free to determine terms and duration of the restrictions.

Comment [CA4]: Eliminate.

Concerning the situation of employees, the Baker & McKenzie study finds that though in general, whilst employed, employees have a (statutory) duty of loyalty (including non-disclosure and non-compete obligations) towards the employer, a common practice in most jurisdictions is to provide for non-use and non-disclosure, as well as non-compete clauses in contracts of employment. However, the position differs as to what can be done in relation to

<sup>10</sup> In Austria, damage claims are also available in cases of default; accordingly damage compensation could be awarded also in case of the third party's slight negligence.

<sup>11</sup> For instance, in the United Kingdom a duty of confidentiality may be implied by the circumstances (the duty of confidentiality is easy to identify in case of an employment contract or a non-disclosure agreement, but it could prove to be very difficult to demonstrate where a person has obtained the confidential information in absence of any relationship between the owner and the recipient), but a person who innocently receives a confidential information will not be under a duty of confidentiality until he is made aware the information is confidential.

<sup>12</sup> In Belgium, courts refuse to grant final injunctions against future trade secrets misappropriation because, contrary to intellectual property rights, trade secret protection can potentially last forever and thus courts are not willing to grant the owner of a trade secret a broader protection than most intellectual property right holders.

<sup>13</sup> In Denmark, although depending on a case by case analysis, final injunctions are usually granted for a period of two to three years from termination of the cooperative relationship.

<sup>14</sup> In Greece and The Netherlands, injunctions are considered temporary in nature.

an ex-employee who uses or discloses secrets after leaving employment. The balance between the interests of the employer and the employee is indeed assessed differently in the relevant countries. In general, post-employment, an employee cannot be prevented from using the skill and knowledge gained during the employment, provided that said knowledge does not consist of trade secrets or confidential information that the employee wilfully memorised or (mis)appropriated with the purpose to misuse them after termination of the employment relationship<sup>15</sup>.

*(iii) Destruction of the goods produced using the misappropriate trade secrets or the restitution of the misappropriated information*

Compared to injunctions, other measures such as the destruction of the goods produced using the misappropriate trade secrets or the restitution of the misappropriated information) are not available everywhere and are available in interim proceedings in certain countries only (see [Table A6.2](#)). Since resulting goods are not always destroyed, there is no guarantee for the trade secret owner that such goods will no reappear in the market.

*(iv) Damages*

Compensation for the prejudice suffered from the misappropriation of a trade secret is available in all jurisdictions<sup>16</sup>. Damages claims are mainly based on tort or contract and only in a few cases specific provisions on damages are included in either the unfair competition laws (see for example Spain) or in the specific provisions applying to trade secret misappropriation (Italy and Sweden).

Damages based on tort cover both accruing damages (“*damnum emergens*”) and loss of profits (“*lucrum cessans*”). Loss of profits, however, is in most cases very difficult to prove, since the misappropriated information is an intangible asset<sup>17</sup>. This helps explaining the often low compensation obtained<sup>18</sup>. A claim for unjust enrichment is available in some countries

<sup>15</sup> In Denmark (and similarly in Poland), the statutory non-disclosure and non-use obligations survive termination of the employment contract for a period of three years. In Italy, as in many other European countries, non-compete agreements (or clauses) are commonly used to prevent use or disclosure after the contract of employment ceases, albeit offering more limited restrictions than those which exist during the period of employment (to be enforceable non-compete clauses must generally be limited in time and space, identify the activities which the former employee cannot engage in and provide for a monetary compensation). In Sweden, damages for breach of confidentiality obligations after termination of employment are only available where there are “extraordinary circumstances”. In Ireland and the United Kingdom there is a distinction between general (low grade) confidential information that the employee is not entitled to disclose whilst employed but can use and disclose thereafter and “real trade secrets” which he cannot disclose or use without authority at any time. The distinction depends on a number of factors including whether the employer impressed the secrecy of the relevant information upon the employee; and whether the “secret” can be readily isolated from other information which the employee is free to use.

<sup>16</sup> In Bulgaria, damage compensation is the sole final remedy available to the owner of a trade secret.

<sup>17</sup> According to Baker & McKenzie, there are often evidentiary problems in proving the loss incurred by the owner of a trade secret. In some countries, damages are awarded only if the claimant is able to demonstrate that he had suffered some loss. Other countries allow courts to award damages on an equitable basis - taking into account all the circumstances of the case - if the claimant has not been able to provide sufficient evidence on the amount of damages

<sup>18</sup> According to Baker & McKenzie, damages vary on a case-by-case basis but the average figures collected during the study “seem not to be particularly encouraging”. This study mentions a few cases in Italy and Sweden, where courts awarded high amounts of damages: in Italy, in two cases of trade secrets infringement the Court of Milan awarded damages for EUR 1,100,000.00 and EUR 10,000,000.00, respectively. In Sweden, courts have awarded damages for SEK 7/10,000,000.00 and 48,000,000.00. However, the study reports that these appear to be exceptional cases.

In the Force India Formula One Team Ltd. case, only €25000 were awarded by a UK court to the claimant. The plaintiff had claimed compensation in excess of £13 million (which was based on the

only, such as among others, Belgium, Estonia, Finland and Spain (for further details please see Table 3 below). In some other countries (for example, Austria, Germany, Italy, Ireland, Lithuania, Poland, Sweden and the United Kingdom) the claimant has the right to claim the account of profits obtained by the infringer from its wrongdoing. In most of the cases, however, the account of profits is alternative to the loss of profits or is considered a criterion to calculate said loss. In Italy, the owner of trade secrets may claim the restitution of the infringer's profit in addition to the loss of profits to the extent that the infringer's profits exceed the claimant's loss. In Greece, account of profits and unjust enrichment are alternative ways to calculate the loss of profits. Similarly in The Netherlands loss or profits excludes account of profits.

**Table 3 – Available damages options**

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LJ	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Accruing damage ( <i>damnum emergens</i> )	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Loss of revenues ( <i>lucrum cessans</i> )	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Moral damages									✓					✓						✓			✓			✓	
Punitive damages															✓												✓
Other monetary compensation					✓																✓						
Account of profits	✓			✓	✓	✓		✓	✓		✓		✓	✓	✓	✓		✓		✓	✓			✓			✓
Fair royalty	✓					✓	✓		✓				✓		✓					✓							✓
Unjust enrichment		✓			✓			✓	✓	✓								✓			✓	✓	✓	✓	✓	✓	✓
<i>Ex aequo et bono</i> global account		✓	✓					✓			✓		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cumulation of these options	✓	✓		✓	✓	✓		✓	✓						✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓

If damages are claimed on contract, liquidated damages (if provided by the agreement) can also be claimed in addition to damages. Contractual liability, however, is often limited to the damages which were foreseeable at the time of conclusion of the contract.

The available options are in principle all cumulative (exceptions are Austria, Cyprus, Estonia, Finland, France, Germany, Hungary, Ireland, Luxembourg, Portugal, Romania and United Kingdom) provided that the total amount awarded by the court does not exceed the actual claimant's loss. Furthermore, in countries where courts are allowed to award an "*ex aequo et bono*" global amount in cases where damages cannot be alternatively calculated, such criteria are of course to be considered as alternative to all the other available damage options.

Since most of the EU Member States do not have specific criteria for the calculation of damages, they apply the general criteria of tort liability (i.e., *damnum emergens* and *lucrum cessans*). The license analogy has been indicated as a possible criterion for the calculation of damages<sup>19</sup>, among EU Member States in Austria, Denmark, Germany, Greece, Hungary, Italy, The Netherlands and United Kingdom.

## (B) CRIMINAL LAW

assumption that it succeeded in the entirety of its claims for breach of confidence, which it did not). However, the judge did not accept the plaintiff argument that the relevant information was of great value and considered that the misuse of the information was limited in nature, purpose and benefit. As a result, the judge considered that €25000 was the figure the parties would have negotiated had they been in the position of a willing licensor and willing licensee acting reasonable as at the date of the breach of confidence.

<sup>19</sup>

This method of calculation is used regarding infringements of intellectual property rights, pursuant to Article 13(1)(b) of Directive 2004/48/EC. This Article provides for the rules on abstract calculation of damages (i.e. calculated on the basis of royalties which could have been due should a licence have existed) as an alternative to the general *damnum emergens* and *lucrum cessans* criteria.

### (B.1) Criminal law protection in national law: summary

Criminal protection of trade secrets against misappropriation differs from Member State to Member State on several levels, although almost all of them have provisions in this respect. Since there is a lack of a common/shared definition of the scope of trade secrets, the actual extent of the protection provided by states may vary depending on the aims pursued by the provisions implemented for this purpose.

Only a few Member states (i.e., Bulgaria, Ireland, Malta and U.K.) have not established any specific criminal framework with respect to trade secrets violations. However, even in those Member States, the conduct of the infringer may be punished under other related criminal offences (see below). In some cases, where no specific criminal provision has been implemented, penal sanctions of trade secrets misappropriation apply under unfair competition laws or commercial laws. Sweden is the only EU Member state that has implemented a specific law on trade secrets (the Swedish Act on the Protection of Trade Secrets), even though some relevant provisions are also contained in the Criminal Code<sup>20</sup>. Table 4 below summarises the criminal provisions in force:

Table 4 – Criminal provisions applying to trade secrets misappropriation <sup>21</sup>																											
	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Criminal code	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Unfair competition commercial law	✓			✓	✓	✓	✓	✓	✓											✓	✓						
Specific law on trade secrets																								✓			

Comment [CA5]: Eliminate.

Comment [CA6]: Insert.

### (B.2) Differences in the conducts considered as crimes

#### (i) Unauthorised disclosure/use of trade secrets

Many of the countries seem to limit the scope of trade secrets to the information that a company has a reasonable and objective interest to keep confidential, in accordance with an objective criterion (e.g., Austria, Belgium, France, Germany, Hungary, Italy, Lithuania, Luxembourg, Netherlands, Slovakia, Spain, Sweden). Nonetheless, in some cases the relevant protection is afforded to any information having economic value that the owner deems it opportune for his benefit to keep secret according to a subjective criterion and that are subject to reasonable measures for protection of confidentiality (e.g., this broader interpretation seems to be prevailing in Czech Republic, Finland, Greece, Poland, Romania and Slovenia).

- In Austria the offender to be held criminally liable for trade secrets violations must have acted at least with conditional intent. In Belgium, Estonia, Finland, France the conduct may be punished even if the offender acted with negligence.
- Cyprus does not establish any specific requirement that the offender must meet to be charged with criminal liability for trade secret violations. Nor is there any stated obligation on the claimant to keep information confidential.
- In the Czech Republic the offender must act deliberately to commit the offence. As the relevant conduct is defined as an act of unfair competition, the offender must qualify as a competitor or someone participating in the competitive process. The

<sup>20</sup> In particular, the Act on the Swedish Protection of Trade Secrets establishes two different offences: business espionage and the unauthorized dealing with trade secrets. Other complimentary or more general offences, such as, for instance, unauthorized access to computer systems or breach of faith against principal are regulated under the Criminal Code.

<sup>21</sup> Baker & McKenzie study.

concept of competition has nevertheless been construed very broadly, including even indirect or potential competitors.

- In Denmark the offences provided for under the Criminal Code require intent. Only upon certain circumstances if the employee causes a substantial risk of dissemination of confidential information by negligence he or she may be charged with criminal liability pursuant to Section 19 of the Marketing Practices Act. without having acted with intent.
- Germany requires that the infringer acts with intent and, specifically, for the purpose of competition, for personal gain, for benefit of a third party or causing damage to the owner of the secret.
- In Greece the offender must act (with intent) for purpose of competition, that means that two criteria have to be met: (i) the conduct of the offender must be suitable to serve the purpose of competition; (ii) he or she must act with the “intention of competition”, i.e. enhance his or third parties’ competitiveness.
- As to Hungary and Italy, the offender may be punished only if he or she acts with intent.
- In Latvia the employer is obliged to identify in writing the information considered to be commercial secrets. In any case, the offender requires the offender to have acted for use or disclosure by himself or another person, therefore intent is required for the offence to occur.
- Lithuania requires that the offender, in case of business espionage, acted with the intent to unlawfully obtain a trade secret, whereas, in the case of violation of trade secrets, with the intent to get a financial gain or to injure the owner by the disclosure to third parties or the use of the information.

As almost all EU Member states require that the offender acted with intent, it emerges that whoever commits a trade secrets infringement must have clearly the knowledge that the business information constituted trade secrets, even if there is no express obligation to keep such information confidential.

- In Luxembourg, Netherlands and Portugal the offender must act with the intent to reach a competitive advantage or to cause harm to the owner.
- Also Poland requires intent, as the offender must breach an obligation of confidentiality that must be prior established by the owner of the secret, either directly or indirectly.
- Under Romanian and Slovak law the offender must act with intent, but no specific purpose is required.
- The same applies in Slovenia, where if the conduct reaches certain outcome, the offender may be charged with the more severe correspondent penalties.
- Spain also requires intent, even if the purposes to be pursued vary depending on the type of offence considered (for instance, commercial advantage).
- The Swedish Act on the Protection of Trade Secret does not pose any requirement as to the purpose that the offender acts for. It only requires that he acted wilfully and without authorization.

*(ii) Related offences*



In Belgium a person who commits the offence under Section 309 of Criminal Code (unauthorized disclosure of trade secrets) may also be charged with theft or misappropriation (provided that he qualifies as an employee with the company). Similarly, Section 491 applies when a person is entrusted as a data processor/handler manufacturing secrets that are physically stored breaches his duty of confidence.

In Bulgaria, for instance, the offence of business bribery is punishable and applicable to, any individual who discloses to third parties information that he knows in return for something.

In France there is a wide range of crimes that may arise in connection to trade secrets violations:

- First, the offence of theft may occur when the conduct at stake consists in the fraudulent appropriation of third parties' data carriers containing confidential information. Such an offence has been found by the Court of cassation to apply even in connection to disclosure of trade secrets. Theft is punished by imprisonment up to three years and a fine of Euro 45,000.00.
- Additionally, the offence of breach of trust may be committed where an individual with the company misappropriates documents containing confidential information entrusted to them for temporary use. In such a case, the offender shall be punished by imprisonment up to three years or a fine of Euro 375,000.00.
- Also, other provisions of the Criminal Code punish the act of supplying secret information to foreign powers by imprisonment up to fifteen years and a fine of Euro 225,000.00.

In Germany cases of industrial espionage may result in theft or misappropriation.

In Greece the infringement of trade secret may constitute, among other offences, a breach of trust under Section 390 of the Criminal Code. In such a case, the offender shall be punished by imprisonment up to ten years and a fine up to Euro 15,000.00.

Depending on the circumstances, violations of trade secrets may result, further to civil lawsuits, in a number of offences, including but not limited to insider trading, unauthorized access to computer systems and a breach of privacy.

As to Italy, the conduct of the offender who commits an unauthorized use or disclosure of trade secrets may also constitute theft or misappropriation.

In Latvia acts of unauthorized disclosure or acquisition of trade secrets may constitute unfair competition practices where repeated within a one-year period and, thus, result in a punishment by imprisonment of up to two years and a fine, in addition to disqualification penalties.

Violations of trade secrets may constitute fraud or bribery in Lithuania or theft in Luxembourg. In Netherlands the conducts may also result in the theft of secret documents or hacking of computer systems. In Portugal the related offences include computer and communications fraud. Slovakia, in addition to breach of trade secrets, criminalizes the misuse of participation in economic competition through unfair acts.

In Slovenia the same act may be punished under the crime of "disclosure of and unauthorized access to trade secrets" as well as, for instance, the offence of abuse of insider information. Spain provides an extensive regulation of trade secrets infringements: however, pursuant to Section 278.3 of the Criminal Code the specific provisions apply without prejudice to the penalties that may arise for appropriating or destroying the computer media, i.e. for the offences of theft or misappropriation.

In Sweden, further to the offences provided for under the act on the Protection of Trade Secrets, other criminal provisions may apply, including unauthorized access to computer systems, unlawful dispossession, unlawful use, espionage, unlawful dealing with secret information and negligent dealing with confidential information.

Offences in any way related to trade secrets violations have significant importance in the legal systems that do not establish any specific provision in this respect:

- In Bulgaria violations of trade secrets may be punished only indirectly. The relevant offences in this respect include the disclosure of service/office secrets, the business bribe and computer crimes.
- Under Irish law, for instance, trade secrets infringements may result in: (i) disclosure of personal data obtained without authority; (ii) unauthorised accessing of data; (iii) unlawful use of a computer; (iv) theft or (v) criminal infringements of intellectual property rights.
- Under Maltese criminal law, in the absence of provisions specifically concerning trade secrets, one could be charged with misappropriation and fraudulent gains as a result of his conduct.
- In the U.K. the criminal provisions that may apply in connection to trade secrets infringement cases include theft, fraud, conspiracy to defraud as well as, upon certain circumstances, some of the offences provided for under the Computer Misuse Act (such as unauthorized access to information contained on a computer) and the Data Protection Act (although it is very unlikely that personal data qualify as trade secrets).

### (iii) Qualified offences

Certain Member States also establish qualified offences when the revelation or use of confidential information is committed by a person acting in a particular capacity (e.g., as civil servant, public official, or as person handling confidential information by reason of his job, e.g. lawyers, officers). Please note that this does not mean that for each of the offences a specific provision is established. Separate provisions may have been implemented (e.g. Italy) or, like in Estonia, the same provision may apply to professional and official secrets, also covering trade secrets. See Table 5:

Table 5 – Qualified offences <sup>22</sup>																											
	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Breach of professional secrecy	✓	✓		✓				✓	✓						✓				✓	✓		✓	✓	✓	✓	✓	
Breach of official secret	✓		✓	✓				✓	✓		✓				✓								✓	✓			
Other breach of confidence									✓				✓														
Separate provisions	Y	Y	N	N	N/A	N/A	N	N			Y	N		Y	N				N/A	N		Y	Y			N	

### (iv) Threshold for the applicability of criminal penalties

In the Czech Republic only violations resulting in a damage of at least Euro 2,000.00 may give rise to criminal liability. The offender must cause harm to a competitor or a consumer equivalent to such an amount or provide someone else than the owner of the secret with a benefit of the same amount. The offender does not necessarily need to be a legal person or an enterprise.

A *de minimis* threshold applies in Lithuania, where for the offender to be prosecuted it is required that the conduct caused a damage of at least EUR 5,648.00.

Something like a *de minimis* threshold is established in Poland, where the conduct must have caused substantial damage to the owner, although no quantification of this concept is provided for in the law.

Slovakia establishes that for the offender to be prosecuted a significant damage (more than EUR 26,600.00) must be caused by his conduct to another competitor. It also provides for a more severe penalty in cases where the conduct causes a large scale damage (over EUR 133,000.00).

Also under Estonian and Finnish criminal law a general safe harbor clause applies, preventing prosecution in case the offence is found to be of minor harm.

In Austria the offender will not be prosecuted if his conduct is justified by a compelling public or private interest.

No safe harbor seems to exist in Latvia and Sweden. In Cyprus disclosure of trade secrets is allowed, for instance, when protection of health and safety of citizens is affected, i.e. where compelling public interests are at stake or to prove the violations of statutory provisions.

Similarly, no safe harbor or *de minimis* threshold applies in Denmark, Finland, Italy, Luxembourg, Slovenia. Germany does not provide for any safe harbor; however, disclosure of trade secrets is justified when committed to avert an imminent danger to life, limb, freedom, honour, property or other prevailing legal interests. In Greece trade secrets are not protected in case a witness is examined to represent certain circumstances before the Court, excluding state secrets. In Hungary Section 300(2) of Criminal Code expressly sets forth some safe harbors that justify infringement of trade secrets. These clauses include:

- (i) fulfilment of duties prescribed in a separate act governing the publication of information and information to be disclosed in the public interest;
- (ii) fulfilment of duties subject to statutory reporting obligations, even in the case the report was filed in good faith and proved to be unfounded.

In the Netherlands a specific provision sets out an exemption for those who disclosed in good faith a trade secret assuming that the disclosure was in the public interest. Portugal and Romania consider the consent of the owner to the disclosure of a secret as a safe harbor clause. In addition to that, Romanian law permits the disclosure of trade secrets where compelling public interests are at stake. Spain does not consider information about illegal activities carried out by the owner to be a trade secret: therefore, its revelation would not determine any prosecution.

Generally speaking, the risk of dissemination of confidential information does not amount to a criminal offence (except for Slovakia, Slovenia). The conduct carried out by the infringer must result in an actual violation of the interest protected under the relevant provisions. In contrast, most legal systems (including Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Italy, Latvia, Lithuania, Slovakia, Slovenia) provide criminal protection against the intent to commit a trade secret violation. The acts carried out with the purpose of disclosing or using confidential business information which reach a certain threshold in the realisation of the offence are likely to trigger criminal liability.

### ***(B.3) Differences in the penalties***

The conducts which normally give rise to violations of trade secrets include the access to confidential information, the use or the disclosure thereof or the illicit acquisition for

exploitation by the offender or third parties. These conducts are generally punished regardless of the fact that the offender qualifies as a competitor and may be committed either by (past) employees of the company or by external persons (such as consultants, contractors, agents).

It is quite frequent, however, that the violation of trade secrets committed by an employee of the company owning the confidential business information results in a more severe punishment than that provided for the same offence in other cases (i.e., in Belgium, Germany, Greece and Spain).

Table 6 below provides a summary of the main conducts concerning trade secrets violation and the related punishment provided for under the legal systems.

<i>Table 6 – Criminal penalties applying to trade secrets misappropriation<sup>23</sup></i>			
<i>Country</i>	<i>Offender</i>	<i>Conduct</i>	<i>Penalties</i>
Austria	Whoever	Disclosure or exploitation of trade or business secrets	Up to six months imprisonment; up to one year if the conduct is committed with the purpose to obtain a pecuniary advantage or to cause harm to the owner or monetary penalties
		Spying out trade or business secrets for their exploitation by somebody else or disclosure	Up to two years imprisonment OR monetary penalties
		Spying out trade or business secrets for their exploitation abroad	Up to three years imprisonment AND monetary penalties
Belgium	Whoever	Communicating in bad faith manufacturing secrets appropriated during the (past) employment with the owner	From three months up to three years imprisonment AND monetary fine from Euro 50 to 2,000.00
Bulgaria		There is no specific criminal provision concerning violation of trade secrets. However, depending on the characteristics of the conduct, the offender may be charged with more general offences, such as business bribe or computer crimes	
Cyprus	Whoever	Disclosure of trade secrets	Imprisonment up to one year OR monetary fine up to Euro 1,275.00
		Disclosure of information protected by professional secrecy involving trade secrets	Imprisonment up to six months AND/OR monetary fine up to Euro 1,700.00
Czech Republic	Whoever	Acts of unfair competition infringing trade secrets and causing damage in or in excess of Euro 2,000.00 to other competitors/consumers or providing someone with unjustified benefit in the same or greater amount	Monetary fine up to Euro 1.5 Million*
Denmark	Whoever	Unauthorized misuse or appropriation of trade secrets	Imprisonment up to 1 year and 6 months OR monetary fine
		Serious violations such as appropriation of trade secrets in a contract of service or in the performance of assignments	Imprisonment up to six years
Estonia	Whoever	Unauthorized disclosure or use of business secret learned by reason of the professional or official duties with the purpose of causing damage	Imprisonment up to one year OR monetary fine
Finland	Whoever	Disclosure or use of trade secrets known by reason of the employment, position or other lawful activities to obtain financial benefit or to injure the owner	Imprisonment up to two years OR monetary fine
		Misuse of trade secrets obtained or revealed through an unlawful act	Imprisonment up to two years OR monetary fine
		Business espionage: Unlawfully obtaining information regarding trade secrets	Imprisonment up to two years OR monetary fine
France	Whoever	Revelation of manufacturing secrets	Imprisonment up to two years AND monetary fine of Euro 30,000.00
		Theft (for instance, of carriers or materials containing trade secrets)	Imprisonment up to three years AND monetary fine of Euro 45,000.00
Germany	Employees	Unauthorized communication of trade or business secrets that the offender was granted access to for the purpose of obtaining financial advantage or injuring the owner	Imprisonment up to three years OR monetary fine
	Whoever	Unauthorized acquiring or securing trade or business secrets or using thereof	Imprisonment up to three years OR monetary fine. Imprisonment up to five years if aggravating circumstances occur

Greece	Whoever	Copying, printing, using, disclosing or in any way violating data or computer programs constituting secrets of an enterprise	Imprisonment from three months up to one year. Imprisonment from one year to five years if the offender is in the service of the owner and the secrets are of great financial significance
	Employees	Unauthorized communication to third parties of secrets that the offender has known by reason of his employment to obtain financial advantage or to cause a damage to the owner; Unauthorized use of the information so obtained	Imprisonment up to six months AND monetary fine up to Euro 8.80
Hungary	Whoever	Making available to unauthorized persons secrets for financial advantage or to cause damage to others; Using the secrets so obtained	Imprisonment up to three years
Ireland	Not applicable		
Italy	Whoever	Disclosure or use of any information concerning scientific discoveries or inventions or industrial applications that is intended to remain secret known by the offender by reason of his status, function, job or art, to obtain a profit	Imprisonment up to two years
Latvia	Whoever	Revelation of non-disclosable information other than a state secret; Unauthorized acquisition and disclosure of commercial secrets	Imprisonment up to five years OR monetary fine
Lithuania	Whoever	Unlawful acquisition of commercial secrets or communication to third persons; Disclosure of information that the offender was entrusted with by reason of his employment	Imprisonment up to two years AND/OR disqualification penalties
Luxembourg	Employees	Use or disclosure, during the employment or within two years after its expiration, trade or manufacturing secrets known by reason of the job to obtain financial advantage or to cause damage to the owner	Imprisonment from three months to three years AND monetary fine from Euro 251 to 12,500.00
Malta	Not applicable		
Netherlands	Employee	Intentional disclosure of confidential information that may harm the owner	Imprisonment up to six months AND/OR monetary fine up to Euro 19,500.00
Poland	Whoever	Disclosure or exploitation of trade secret in breach of confidential duties that causes substantial damage to the owner; Use of information illegally acquired or disclosure to third persons	Imprisonment from one month to two years AND monetary fine up to Euro 260,000.00*
Portugal	Whoever	Use or disclosure to third parties of secrets that the offender knows by reason of his status, job, profession or art	Imprisonment up to one year OR monetary fine
Romania	Whoever	Disclosure, acquisition or use of trade secrets without the consent of the owner, as a result of an action of commercial or industrial espionage	Imprisonment from six months up to two years OR monetary fine from Euro 570 to 5,000.00*
		Disclosure of data or information not intended to be publicly known by a person who knows it by reason of his employment, provided that the offence is likely to cause damages	Imprisonment from two up to seven years; Imprisonment from six months to five years if the disclosure is made by another person
Slovakia	Whoever	Spying out trade secrets with the intention to disclose them to unauthorized persons	Imprisonment from six months up to three years; Imprisonment from seven to twelve years if aggravating circumstances occur
Slovenia	Whoever	Disclosure of trade secrets; Providing unauthorized third parties with access to trade secrets; Collection of trade secrets with the purpose of delivering them to unauthorized persons; Unlawful obtainment of trade secrets with the purpose of delivering them to unauthorized persons	Imprisonment up to three years; Imprisonment up to five years if the information is of particular importance
Spain	Whoever	Acquiring data, documents, media and other objects to discover trade secrets; Disclosure, revelation or communication to third parties of the discovered information	Imprisonment from two up to four years AND monetary fine; Imprisonment from three to five years AND monetary fine in case the secrets are disclosed
		Diffusion, disclosure or communication of trade secrets in breach of duties of confidentiality	Imprisonment from two up to four years AND monetary fine, in case the information is disclosed in breach of confidentiality
Sweden	Whoever	Unauthorized access of trade secrets as business espionage	Imprisonment up to two years OR monetary fine; Imprisonment up to six years in case of information of significant importance
		Acquiring trade secrets knowing that the person who made it available accessed the trade secret through acts of business espionage	Imprisonment up to two years OR monetary fine; Imprisonment up to four years in case of information of significant importance

**Comment [CA7]:** In Portugal, trade secrets misappropriation is not a crime. It is considered an unfair competition act (administrative offense punished by a fine).

			importance
U.K.	Not applicable		
* Monetary penalties are expressed in local currency and converted to Euro for the reader's convenience			

Generally, punishment of the offender is by imprisonment, even though he or she may also be charged, either in addition to that or alternatively, with monetary penalties: see Table 7 with penalties that shall apply for the main offence (for instance, unauthorized disclosure/use of trade secrets).

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Imprisonment OR monetary penalties		✓			✓	✓	✓	✓		✓	✓						✓		✓			✓	✓	✓			
Imprisonment AND monetary penalties		✓							✓	✓		✓					✓			✓	✓						
Imprisonment ONLY													✓		✓	✓									✓	✓	
Monetary penalties ONLY					✓																	✓					
Other penalties					✓											✓							✓				

**Comment [CA8]:** In Portugal, trade secrets misappropriation is not a crime. It is considered an unfair competition act (administrative offense punished by a fine).

**Comment [CA9]:** Insert.

Hungary, Italy, Lithuania, Slovakia and Slovenia only provide for the imprisonment of the offender whereas in Czech Republic only monetary penalties and, where possible, forfeiture of property shall apply. Lithuania, as well as Romania, also provide for disqualification penalties in addition to imprisonment, such as deprivation of the right to be employed in certain positions or to engage in certain activities. This is a very significant solution, as it directly impacts on the opportunity for the offender to be entrusted with certain responsibilities in his future employment.

With respect to the extent of punishment, the Czech Republic is the state where the heaviest fines apply: under Czech law, the infringer shall be punished with a fine up to 1.5 Million Euro. In contrast, Czech law does not provide for imprisonment in case of trade secrets violations.

In most of states trade secrets infringements are punished with imprisonment up to a term of two-three years. There are a few exceptions: in Denmark the offender may be charged with up to six years imprisonment, provided that serious violations have taken place; in Slovenia imprisonment may be up to five years when the acts carried out by the offender concerns information of particular importance. Under the Swedish Act on the Protection of Trade Secrets, terms of imprisonment of up to six years are foreseen for cases of business espionage and up to four years for the unlawful acquisition of trade secrets of significant importance.

### (C) THE SPECIFIC CASE OF IMPORTS OF GOODS INTO THE EU

In the specific case of goods imported from third countries which would have been manufactured using misappropriated trade secrets of EU companies, there is no specific administrative procedure before customs authorities to block them.

The EU Regulation on customs enforcement of intellectual property rights<sup>25</sup> provides for such administrative customs procedures<sup>26</sup>: the holder of an intellectual property right can ask

<sup>24</sup> Baker & McKenzie study.

<sup>25</sup> Regulation (EC) No 1383/2003 of 22 July 2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights, OJ L 196, 2.8.2003, p.7. The Commission made a proposal in 2011 for a new

customs authorities to block imports of goods infringing and intellectual property right. Once the imports blocked, the holder of the intellectual property right has to file a case before a civil court which will decide on the existence (or not) of the infringement. However, this EU rules only applies as regards formal intellectual property rights and do not extent to trade secrets misappropriation claims<sup>27</sup>. Hence, national customs authorities do not process claims for misappropriation of trade secrets.

This situation differs from that in the United States. In the United States, it is possible to engage administrative proceedings before the US International Trade Commission (ITC) in order to block imported goods manufactured using misappropriated trade secrets<sup>28</sup>. Section 337 of the Tariffs Act<sup>29</sup> gives power to the US ITC to deal with claims involving infringements of intellectual property rights but also other forms of unfair competition involving imported products, such as misappropriation of trade secrets. The US ITC has investigative powers. The procedure includes trial proceedings before administrative law judges and review by the US ITC. In terms of remedies, the primary remedy available in Section 337 investigations is an exclusion order that directs US Customs to stop infringing goods from entering the US. In addition, the US ITC may issue cease and desist orders against named importers and other persons engaged in unfair acts that violate Section 337.

Therefore, in order to block goods imported from third countries which would have been manufactured using misappropriated trade secrets of EU companies, the EU owner of the trade secrets in question would need to first go to court in order to have the misappropriation of the trade secrets declared and to obtain an injunction against the third party in question which could be enforced by customs authorities. Compared to formal intellectual property rights, there is therefore an inversion of the burden of proof.

#### **(D) THE PROCEDURAL RULES BEFORE NATIONAL COURTS**

Procedural rules in national law are not always adapted to litigation in trade secrets. Secrecy of information is often at risk during civil proceedings and the absence of protection from (further) disclosure of information as a consequence of court proceedings is a considerable deterrent from starting a legal action<sup>30</sup>.

##### ***(D.1) The insufficient protection of confidential information in national proceedings***

When litigating to defend a trade secret, these procedural rules can result in disclosure of confidential information to the other party or to the public. There are three main situations.

(1) The need to describe the misappropriated trade secret in the application, so that the judge can understand it, could imply that, if the plaintiff does not know the extent of the information misappropriated by the defendant, he could disclose to the defendant (since the application is served to him) more confidential information than actually needed to defend his case<sup>31</sup>.

---

Regulation concerning customs enforcement of intellectual property rights (COM(2011)285). Negotiations on this text before the European Parliament and the Council are on-going.

<sup>26</sup> Indeed, administrative customs procedures of this type would be a matter of EU law.

<sup>27</sup> Unless of course the claim encompasses both an intellectual property right infringement (e.g. a patent) as well as a trade secrets misappropriation claim.

<sup>28</sup> See generally [http://www.usitc.gov/intellectual\\_property/](http://www.usitc.gov/intellectual_property/)

<sup>29</sup> For the text of Section 337 of the Tariffs Act, see:

[http://www.usitc.gov/intellectual\\_property/documents/statute.pdf](http://www.usitc.gov/intellectual_property/documents/statute.pdf)

<sup>30</sup> Baker & McKenzie study.

<sup>31</sup> See for instance, Hogan Lovells (2012), §57 regarding Belgium, at p.12.

(2) The general rules on the production of evidence could also have the effect of having to disclose information otherwise considered confidential. In common law countries, the pre-trial duty of (full) discovery rules applies; in continental countries, the defendant may ask for certain documents/evidence to be presented by the other party when such evidence lies in the control of that party – which could imply further disclosure of trade secrets. It should be noted that this plays both ways: bad faith plaintiffs could try this way (and therefore abusing the litigation rules) to obtain confidential information from defendants<sup>32</sup>.

(3) The inherent publicity of judicial proceedings (civil proceedings in all EU Member States are public) could also result in the disclosure of trade secrets, in this case to the public:

- Firstly, hearings are often public. While national procedural laws normally include general provisions which allow Courts to exclude the public from the hearing for reasons relating to security, public order and decency, there do not necessarily apply to trade secrets litigation. In some EU Member States (notably Bulgaria<sup>33</sup>, Estonia<sup>34</sup>, Hungary<sup>35</sup>, Germany<sup>36</sup>, The Netherlands, Poland, Romania, Slovakia, Slovenia), a party has the right to request the court to order that the entire proceeding or a part thereof be heard in private to preserve the secrecy of the trade secret. However, according to Baker & McKenzie (2013), this seems to rarely happen in practice and there would be no case law on this point<sup>37</sup>. In the United Kingdom the parties may agree or apply to the Court to ensure that certain information to be revealed during the pre-trial disclosure procedure remains confidential. The parties may enter into a contractual agreement whereby the parties agree that certain information may remain confidential or only be disclosed to legal counsel or where the parties do not reach such agreement, a party may unilaterally apply to the Court requesting that confidential information is not disclosed to the other party during the proceeding. Requests for restriction of disclosure are at the discretion of the Court.
- Judicial decisions may describe the misappropriated trade secret in question when explaining the reasons for the decision<sup>38</sup>; and in some countries other judicial documents (including applications) may be accessed by third parties. According to Baker & McKenzie (2013), in most countries, pleadings and in general court

<sup>32</sup> General procedural rules will normally allow the defendant to refuse to provide a document if it includes a trade secret or a confidential information of the defendant.

<sup>33</sup> In Bulgaria private hearing is specifically provided for cases related to “protection of trade, manufacturing, invention or tax-related secrets” if public disclosure may impair a party’s legitimate interest. When publicity is precluded, only the parties, their attorneys, experts and witnesses are allowed to enter into the court room and are subject to a statutory obligation not to disclose subject matter and content of the relevant proceeding (breach of such obligation entails liability for compensation).

<sup>34</sup> In Estonia (similarly in Finland and Lithuania), in-camera examination can be ordered for the protection of trade secrets if the interest in a public hearing is not deemed to be greater than the commercial interest in protecting the secret.

<sup>35</sup> In Hungary, when the Court orders in-camera examination, the parties are also prohibited from making copies of the minutes of the hearing or of any document containing a trade secret. Examination of documents containing trade secrets is subject to a declaration of non-disclosure and special review procedures are established by the Judge.

<sup>36</sup> In Germany, besides the exclusion of the public if trade secrets are to be discussed, legal practice has developed the so called “Düsseldorf Procedure” (originally developed for patent law claims but likely applicable to trade secrets cases), which consists in a procedure where Courts order independent proceedings for the preservation of evidence as an interim injunction handed to the defendant together with the statement of claims so that there is no chance to destroy evidence. Evidence is then examined exclusively by authorized experts and attorneys bound to confidentiality. The parties do not have access to the confidential information.

<sup>37</sup> Baker & McKenzie (2013) study.

<sup>38</sup> See for instance, Hogan Lovells (2012), §57 regarding Belgium, at p.12.



documents are public and potentially accessible by anyone. Courts have a general duty to adopt adequate measures to safeguard the secret information of a party, for example, by restricting access to those documents which contain trade secrets only to the other party's attorney or to the court's expert (in certain cases the confidential information can be put under closed seals), or not disclosing certain information in the court's final decision (by blanking out the relevant information in the decision and other court's documents). However, according to that study, such measures have proved to be of limited effect to prevent the actual leak of confidential information during proceedings<sup>39</sup>.

***(D.2) The example of antitrust proceedings protecting confidential information***

There are specific rules protecting secrecy of confidential information during antitrust proceedings in the Member States. All of them have measures aimed at protecting business secrets/confidential information from being disclosed during proceedings before national competition authorities, even if the procedural steps needed to obtain protection of secret information varies, to a certain extent, from jurisdiction to jurisdiction. In particular, the involved undertakings have the right to indicate the information that, in their opinion, shall not be divulged<sup>40</sup>. Similar provisions exist at EU level for the antitrust proceedings before the European Commission.

**(E) THE SPECIFIC CASE OF TRADE SECRETS WHICH ARE DISCLOSED TO PUBLIC AUTHORITIES PURSUANT TO REGULATORY OBLIGATIONS: EU RULES**

Several EU rules are addressing the specific case of trade secrets which are disclosed to public authorities – normally because of regulatory obligations.

***(E.1) The protection of confidential information in public procurement cases***

Industry often expresses the fear that valuable confidential information (i.e. a trade secret) which is disclosed to a public authorities as part of a tender procedure for public procurement could not be sufficiently protected against misappropriation.

This concern is addressed by EU legislation. Current EU rules provide for protection in this regard: "*Without prejudice to the provisions of this Directive, in particular those concerning the obligations relating to the advertising of awarded contracts and to the information to candidates and tenderers [...] the contracting authority shall not disclose information forwarded to it by economic operators which they have designated as confidential; such information includes, in particular technical or trade secrets and the confidential aspects of tenders.*"<sup>41</sup>

This protection is also integrated in the 2011 Commission proposal for a new directive on public procurement<sup>42</sup>:

<sup>39</sup> Baker & McKenzie study.

<sup>40</sup> According to Baker & McKenzie (2013), however, the secrecy of information may not be sufficient to prevent disclosure when such information is relevant to prove the infringement or for the right of defence of the parties (Bulgaria, Estonia, Germany, Greece, Italy, Luxembourg, Portugal). See Baker & McKenzie study.

<sup>41</sup> Article 6 of Directive 2004/18/EC of the European Parliament and the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts.

<sup>42</sup> Commission proposal for a Directive of the European Parliament and of the Council on public procurement, COM(2011) 896 final, Brussels, 20.12.2011. Negotiations before the European Parliament and the Council are on-going.

- Article 18 of that proposal<sup>43</sup> requires the contracting authority not to disclose information forwarded to it by economic operators which they have designated as confidential, including, but not limited to, technical or trade secrets and the confidential aspects of tenders. In addition, Article 19(2) of the proposal requires the contracting authorities to ensure, in all communication, exchange and storage of information, that the integrity of data and the confidentiality of tenders are preserved.
- Other provisions in the proposal also require the contracting authorities not to reveal to the other participants in the tender solutions proposed or other confidential information communicated by a candidate participating in the "competitive procedure with negotiation"<sup>44</sup> or in the "competitive dialogue"<sup>45</sup> without its agreement. Such agreement shall not take the form of a general waiver but shall be given with reference to the intended communication of specific solutions or other specific confidential information

The underlying rationale was explained by an English Court of Appeal judge as follows: "...it is plain that there is a strong public interest in the maintenance of valuable commercial confidential information ... If the penalty for contracting with public authorities were to be the potential loss of such confidential information, then public authorities and the public interest would be the losers, and the result would be potentially anticompetitive."<sup>46</sup>

**(E.2) The protection of confidentiality of trade secrets disclosed to EU institutions and agencies**

EU institutions have a general policy of transparency and allow third parties to access to the documents they hold, under certain conditions. Given that businesses may disclose confidential business information to EU institutions in the context of specific procedures (e.g. a complaint against a Member State for failure to apply EU law etc) the risk exists that such confidential business information could be disclosed to a third party. This issue is of particular importance when businesses transfer trade secrets to EU regulatory agencies, such as the European Medicines Agency, the European Chemical Agency or the three European financial authorities.

This concern has been considered when adopting the EU general rules<sup>47</sup> dealing with access to documents held by a European institution. Regulation (EC) No 1049/2001<sup>48</sup> provides for the protection of business secrets when the information has been forwarded to a EU institution or body. Article 4(2) states in particular that "*the institutions shall refuse access to a document*

<sup>43</sup>

"Article 18

Confidentiality

1. Unless otherwise provided in this Directive or in the national law concerning access to information, and without prejudice to the obligations relating to the advertising of awarded contracts and to the information to candidates and tenderers set out in Articles 48 and 53 of this Directive, the contracting authority shall not disclose information forwarded to it by economic operators which they have designated as confidential, including, but not limited to, technical or trade secrets and the confidential aspects of tenders.

2. Contracting authorities may impose on economic operators requirements aimed at protecting the confidential nature of information which the contracting authorities make available throughout the procurement procedure."

<sup>44</sup>

Cf. Article 27(4) of the proposal.

<sup>45</sup>

Cf. Article 28(3) of the proposal.

<sup>46</sup>

*Veolia vs. Nottinghamshire CC* [2010] EWCA 1214 per Rix LJ.

<sup>47</sup>

There are specific rules for the access to file in competition cases, see above.

<sup>48</sup>

Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. OJ L 145, 31.5.2001, p. 43

where disclosure would undermine the protection of the commercial interests of a natural or legal person, including intellectual property").

EU rules also provide for professional secrecy obligations for their staff. In the case of the EU regulatory agencies, they are under the obligation of professional secrecy and respect of confidentiality of the information when cooperating with other authorities<sup>49</sup>.

***(E.3) The protection of confidentiality of trade secrets disclosed to national supervisory/regulatory agencies***

EU rules also deal with the preservation of confidentiality of information (including business secrets) by national regulatory authorities<sup>50</sup>.

***(E.4) Rules on the non-disclosure of trade secrets to supervisory/regulatory authorities by intermediaries***

Financial intermediaries and some regulated professionals (e.g. lawyers, auditors) often know trade secrets owned by their customers. This is why (inter alia) they are subject to professional secrecy rules, which is a guarantee to their customers.

A specific issue may arise when public authorities require those intermediaries or regulated professionals to disclose to them, in the context of their supervisory functions, confidential information which is sensitive for their customers.

EU rules have addressed this issue and exceptions to the principle of respecting professional secrecy have been established in exceptional circumstances. For instance, the EU anti-money laundering rules<sup>51</sup> require financial intermediaries and regulated professions to disclose to

---

<sup>49</sup> See for instance Article 70 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), OJ L 331, 15.10.2010, p. 12.

"[...]

2.

*Without prejudice to cases covered by criminal law, any confidential information received by persons referred to in paragraph 1 whilst performing their duties may not be divulged to any person or authority whatsoever, except in summary or aggregate form, such that individual financial institutions cannot be identified.*

*Moreover, the obligation under paragraph 1 and the first subparagraph of this paragraph shall not prevent the Authority and the national supervisory authorities from using the information for the enforcement of the acts referred to in Article 1(2), and in particular for legal procedures for the adoption of decisions.*

3.

*Paragraphs 1 and 2 shall not prevent the Authority from exchanging information with national supervisory authorities in accordance with this Regulation and other Union legislation applicable to financial institutions.*

*That information shall be subject to the conditions of professional secrecy referred to in paragraphs 1 and 2. The Authority shall lay down in its internal rules of procedure the practical arrangements for implementing the confidentiality rules referred to in paragraphs 1 and 2."*

Recital 62 of that Regulation says:

*"It is essential that business secrets and other confidential information be protected. The confidentiality of information made available to the Authority and exchanged in the network should be subject to stringent and effective confidentiality rules."*

<sup>50</sup> See for instance Article 25 of Directive 2004/109/EC of the European Parliament and of the Council of 15 December 2004 on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC, OJ L 390, 31.12.2004, p.38.

<sup>51</sup> Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, p.15.

specific authorities (so-called financial intelligence units) data regarding situations suspected of involve money laundering.

In other cases, EU rules underlined the need to protect the business secrets of clients. A recent Commission legislative proposal indirectly addressed the protection of business secrets in the specific circumstance where an EU auditor would be required by a third country public authority, for their supervisory purposes<sup>52</sup>, to disclose to it audit working papers containing business secrets of the audited entity. In accordance with this proposal, the EU auditor could only transfer the audit working papers to the third country authority provided that *"the protection of the commercial interests of the audited entity, including its industrial and intellectual property is not undermined"*<sup>53</sup>.

<sup>52</sup>

E.g. the audited entity may be an EU subsidiary of an audited entity of that third country.

<sup>53</sup>

Cf. European Commission Proposal of 30 November 2011 for a Directive of the European Parliament and of the council amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts, COM(2011) 778 final. See Article 1(23), introducing a point (ba) in Article 47(2) of Directive 2006/43/EC.



99j

## United Kingdom

The document presents an accurate picture of the law in the United Kingdom, except for one point on page 6 in Section A.2. It is stated here that the Freedom of Information Act contains a definition of trade secrets. This is not the case. Section 43(1) of the Act does provide that information may be exempt from disclosure if "it constitutes a trade secret". However, this term is not defined in the Act. Guidance is available and this sets out the sorts of questions that should be considered in deciding whether information can be said to constitute a trade secret ([http://www.ico.gov.uk/for\\_organisations/guidance\\_index/~media/documents/library/Freedom of Information/Detailed specialist guides/AWARENESS GUIDANCE 5 V3 07 03 08.ashx](http://www.ico.gov.uk/for_organisations/guidance_index/~media/documents/library/Freedom_of_Information/Detailed_specialist_guides/AWARENESS_GUIDANCE_5_V3_07_03_08.ashx)).



# 99bis



(GROW)

99615

**From:** (MARKT)  
**Sent:** 19 February 2013 15:54  
**To:** 'Gaudino, Francesca (Francesca.Gaudino@bakermckenzie.com)'  
**Cc:** (MARKT); (MARKT);  
**Subject:** RE: National Legal Frame Work in the member States

Comments from Malta received today



MT 2013.doc

**EUROPEAN COMMISSION**  
Internal Market and Services DG  
D3 - Fight against counterfeiting and piracy  
Rue de Spa 2, B-1049 Brussels  
Tel. (+32) 22 5  
[@ec.europa.eu](mailto:)

---

**From:** (MARKT)  
**Sent:** Tuesday, February 19, 2013 3:49 PM  
**To:** Gaudino, Francesca (Francesca.Gaudino@bakermckenzie.com)  
**Cc:** (MARKT); (MARKT); (MARKT);  
**Subject:** National Legal Frame Work in the member States

Dear Francesca,

In an informal meeting that we had with representatives of Member States in December, we have made available to them a short overview of the differences in the national law, based on the results of the Hogan Lovells study and the preliminary results of your study – see doc attached.

<< File: description of national laws\_for MS\_20121210.doc >>

As a result we have received comments from some of the Member States, which we would like you to take into account when presenting the final version of the study.

For that purpose, I attach the replies that we have received; except for Luxembourg and Sweden which have replied that the summary was accurate.

<< File: DE 2013.doc >> << File: CZ 2013.doc >>

<< File: FI 2013.doc >> << File: FR 2013.pdf >> << File: HU 2013.doc >> << File: LT 2013.doc >> << File: PL 2013.doc >> << File: PT 2013.doc >> << File: UK 2013.doc >>

Having said this we would still need to receive the final version as soon as possible.

Kind regards,

**EUROPEAN COMMISSION**

Internal Market and Services DG

D3 - Fight against counterfeiting and piracy

Rue de Spa 2, B-1049 Brussels

Tel. (+32) 22

mailto: : @ec.europa.eu

## MALTA

Malta has reviewed the Commission's document entitled 'Legislative Framework in EU member States on the protection of trade secrets against misappropriations and has the following comments to submit:

As regards to the qualified offences (page 22 of the document) it is stated that 'Member states also establish qualified offences when the revelation or use of confidential information is committed by a person acting in a particular capacity'. Under the Criminal Code (Cap. 9) such action is deemed criminal and subsequently it is catered for under Article 257 where if found guilty that criminal offender is liable to a fine not exceeding €46,587.47 or to imprisonment for a term not exceeding two years or both. It should also be stated that such article is also referred to under the Professional Secrecy Act (Cap. 377) of the Laws of Malta. In addition, with regard to Table 5 on Page 22 where reference is made to Breach of Official Secret, it should be noted that Malta has an Official Secrets Act (Cap. 50).

It is noted that Table 6 (on pages 24 and 25) lays out the criminal penalties applying to trade secrets misappropriation in the different Member States. Whilst there is no reference to the concept of the protection of trade secrets against misappropriation under the Criminal Code (Cap. 9), however, the offence of misappropriation is catered for under Article 293 under the subtitle of Fraud as well as a number of articles concerning the offence of fraud. Thus by way of example if someone makes use of trade secrets with the intent of gaining an economic benefit, then depending on the nature of the offence itself, such person would be charged with the offence of fraud under Articles 308, 309 and 310 and this since there was an economic benefit as well as with the offence of misappropriation and that of disclosing secret information. Indeed, the offences mentioned under the subtitle of Fraud and under subtitle 10 'Disclosing of secret information' of the Criminal Code will be taken into consideration.

Finally, it should also be noted that various Articles of the Malta Competition and Consumer Affairs Authority Act (Cap. 510) and paragraph 5 of the Second Schedule to the said MCCA Act (namely 11 [especially the proviso to Article 11 (2)], 27 [especially subarticle (6) thereof], 28, 29, 30, 32 [especially subarticle (13) thereof], 33 [especially subarticle (5) thereof], 46 [especially subarticle (2) paragraph (a)] as well as Article 110H of the Consumer Affairs Act (Cap. 378) provide for the protection of business secrets and confidential information.'

