



**COMMISSIONER VĚRA JOUROVÁ**

**MEETING WITH AMAZON WEB SERVICES**

**LOCATION: BERL 12/176**

**DATE AND TIME: 11/07/2018, 14H00**

**Meeting Objective:** to discuss – E-commerce product safety, New Deal for consumers, Data protection / Data flows, Illegal content on the internet

**VERSION: 13/11/2018 11:37**

**JUST/1198**

**Participants:** Ms Barbara Scarafia - VP & Associate General Counsel, International Consumer Legal, Amazon, Mr James Waterworth - Director of EU Public Policy, Amazon, Mr Stephane Ducable - Director of EU Public Policy, Amazon Web Services

## **DATA PROTECTION - GDPR**

### **CONTEXT**

HoC Nikolay met with AMAZON Europe Vice-President and Associate General Counsel on 22 November 2017, discussing data protection, consumer rights and enforcement and product safety.

This meeting offers the opportunity to inform Amazon representatives of the main elements of the Communication of 15 May 2018 on 'Completing a Trusted Digital Single Market for all' and about the next steps following the entry into application of the GDPR.

The Communication underlines that the protection of personal data is key in building confidence in the digital economy. It reminds Member States of the importance of having their national legislation in place for the effective application of the GDPR and of equipping the data protection authorities with all the resources necessary to ensure a full and efficient application of the GDPR.

Amazon Web Services (AWS) has become a member of the Association of Cloud Infrastructure Services Providers in Europe (CISPE). CISPE submitted to the Article 29 Working Party its Data Protection Code of Conduct for Cloud Infrastructure Providers. On 23 February 2018, the WP29 sent a letter with comments on the Code to CISPE. CISPE is currently amending the Code in view of the comments received, and will need to resubmit the Code for approval to a DPA in accordance with GDPR.

### **OBJECTIVE(S)**

The objectives of your meeting would be to:

- Stress the importance of GDPR in the light of recent events (such as Facebook/Cambridge Analytica) and the importance of a proper application of GDPR.
- Refer to the Commission Communication of 15 May on Completing a trusted Digital Single Market for all.

### **LINE TO TAKE**

- The New European Union data protection regulation – the General Data Protection Regulation (GDPR), is applicable as of 25 May 2018. The new legislation modifies and updates data protection rules at EU level to make Europe fit for the digital age.
- The Facebook / Cambridge Analytica case highlights if necessary the relevance of the new EU-wide data protection rules set by the General Data Protection Regulation (GDPR).
- The GDPR reinforces principles and rules, it clarifies and harmonises the notion of consent and further develops transparency obligations. It requires the implementation of data protection by design from the outset. As part of the accountability principle, controllers must implement measures appropriate to the risks. In our recent Communication on Completing a trusted Digital Single Market for all, we have underlined the importance of protecting personal data for building confidence in the digital economy.
- GDPR also reinforces the role of national data protection authorities, the enforcers of the EU data protection rules. It gives them better means of cooperation, clearly divides the

competences between the DPAs in cross-border cases and harmonises the enforcement powers, in particular the power to impose fines.

- It is important to keep in mind that the GDPR, as a Regulation, is directly applicable throughout the EU from 25 May. At the same time, we are monitoring the adoption of national laws by the Member States. So far [13] Member States have adopted their national legislation [(AT, DE, FR, HR, NL, SE, SK, DK, UK, PL, IE, MT, LT)]. The others are at different stage of the procedures (including discussion in national parliaments). On 25 May, the Commission sent letters to the Member States to remind those who are not yet ready of the need to adopt their national laws without delay.
- We are continuing to engage with the European Data Protection Board. As you are well aware, the then Article 29 Working Party already issued ten guidelines to assist with implementation and interpretation of new legislation (on data portability, data protection officers, lead supervisory authority, data protection impact assessments administrative fines, urgency procedures, data breach notifications, profiling, consent and transparency). The EDPB work is ongoing on guidelines on accreditation (public consultation closed on 30 March), on certification (public consultation closing on 12/07), and on Codes of Conduct. Following our request, all guidelines are subject to a six weeks public consultation process. We encourage you to make your views known in the context of those public consultations.

#### *Next steps*

- We now need to ensure that the new rules are properly applied on the ground. We all have our roles to play: the Commission, the Member States, the Data Protection Authorities individually and in the form of the European Data Protection Board, the companies and the civil society.
- As guardian of the Treaties, the Commission will monitor the proper application of the GDPR. We have a battery of actions to carry out from now on:
  - We will continue our work with the Member States and closely monitor the application of the Regulation in Member States. We will take appropriate actions as necessary, including the recourse to infringement actions.
  - We have allocated grants to support Data Protection Authorities by co-financing their awareness-raising activities. These activities will start in the second half of this year and will continue in 2019.
  - We will continue our work with stakeholders to explain the GDPR, including through our participation to events both in Brussels and in Member States, and through the GDPR multi-stakeholder group we have established.
  - We will assess the need to make use of our power to adopt delegated or implementing acts, if we establish that there is a clear added-value and request from stakeholders.
  - In one year's time from now, in May 2019, we will take stock of the Regulation implementation, and we will report on the application of the new rules in 2020.

- The EU has set up a strong data protection framework on which a dynamic digital Europe can be built. The EU is well equipped to deal effectively with the new data challenges, provided all actors work closely together in effectively implementing and applying the new tools to protect the rights to privacy and data protection of individuals.

## **DEFENSIVES**

### **What will the Commission do if Member States' actions are late or not in compliance with the GDPR?**

- Where Member States do not take the necessary actions required under the Regulation, are late in taking them or make use of the specification clauses provided for under the Regulation in a manner contrary to the Regulation, the Commission will make use of all the tools it has at its disposal, including recourse to the infringement procedure.

### **What is the Commission position on the guidelines recently published by the Article 29 Working Party/EDPB?**

- The guidelines of the Article 29 Working Party/EDPB are very important to provide increased legal certainty to stakeholders since they will guide the data protection authorities when implementing the GDPR.
- The Commission supports the work of the Article 29 Working Party/EDPB and share with its members its views and expertise on the provisions of the GDPR. It also strongly encouraged the Working party to conduct public consultation on the draft guidelines.
- However, the Article 29 Working Party/EDPB is an independent body and therefore the content of the guidelines are their responsibility.

### **What is the procedure for the approval of Codes of Conduct under the GDPR? What happens to Codes approved under the Directive?**

- According to Article 40 GDPR, a Code of Conduct must be submitted to the competent supervisory authority at national level for its approval. Where it relates to processing activities in several Member States, the EDPB must be consulted and provide an Opinion on the compliance of the Code with the GDPR. The competent supervisory authority must approve the Code following this opinion. The Commission may then give a particular Code general validity within the Union.
- The EDPB is currently working on Guidelines to describe the procedure for submitting Codes of Conduct to supervisory authorities under Article 40 GDPR.
- Codes approved under the Directive will need to be updated by industry to conform them to the GDPR. The GDPR does not as such provide for a transition regime of currently approved Codes. Updates and amendments of current Codes to bring them in line with the GDPR will need to be submitted to the competent supervisory authority for its approval.

### **One-stop-shop mechanism**

- The new rules provide for a "one-stop-shop" mechanism. This means that companies conducting cross-border processing activities only have to deal with one national data protection supervisory authority. Previously, companies had to deal with different decisions from different national data protection authorities.
- A co-operation and consistency mechanism allows for a coordinated approach between all the data protection authorities involved.
- Both controllers and individuals benefit from the "one-stop-shop". Controllers only have to deal with one single supervisory authority, making it simpler and cheaper for companies to do business in the European Union. At the same time, it is easier for citizens to get their personal data protected since they only have to deal with the data protection authority in their Member State, in their own language.

### **What about the European Data Protection Board? What does it do?**

- Similarly to the current "Article 29 Working Party", the European Data Protection Board includes the data protection authority of each Member State, and the European Data Protection Supervisor (EDPS).
- The tasks of the European Data Protection Board are listed in the Regulation (Article 66). It shall, for example, monitor the correct application of the Regulation, advise the Commission on any relevant issue, issue opinions, guidelines or best practices on a variety of topics.
- The main difference is that the European Data Protection Board will not only issue opinions, but also binding decisions regarding some cross-border cases (e.g. if there are conflicting views between several concerned supervisory authorities). The objective is to ensure a consistent application of the Regulation.

### **What are the upcoming plans of the new Chair of the European Data Protection Board?**

- We very much congratulate Ms Jelinek on her recent confirmation on 25 May 2018 as the Chair of the European Data Protection Board.
- Ms Jelinek has stressed that the EDPB shall continue its already ongoing work streams to ensure the successful application of the new legislation.
- The new Chair is currently reflecting on further activities (including guidance) of the EDPB.

## **Background**

The General Data Protection Regulation together with the Data Protection Directive for Police and Criminal Justice Authorities ("Police Directive") form the "**data protection reform**" package. The GDPR entered into force on 24 May 2016 and shall apply from 25 May 2018. The Police Directive entered into force on 5 May 2016 and EU Member States had to transpose it into their national law by 6 May 2018.

The Commission has established an **Expert Group with Member States** to prepare the implementation of the GDPR and the transposition of the Police and Criminal Justice Authorities Directive. The Expert Group meets each month alternatively on the two pieces of legislation. The last meeting of the Expert Group took place on 20 February.

The Commission has launched a study on **certification mechanisms** in order to assess whether it would make sense to make use of Commission empowerments for delegated and implementing acts. Moreover, at the request of the Parliament, we also conduct a pilot project aimed at providing a Fundamental rights review of EU data collection instruments and Programmes.

The Article 29 Working Party (now **European Data Protection Board**) has adopted a **number of guidelines** on key aspects of the GDPR and will pursue this task in the coming months.

Guidelines/working documents by the European Data Protection Board in view of the entry into application of the Regulation <sup>1</sup>	
Right to data portability	Adopted on 4-5 April 2017
Data protection officers	
Designation of the lead Supervisory Authority	
Data protection impact assessment	Adopted on 3-4 October 2017
Administrative fines	
Profiling	Adopted on 6-7 February 2018
Data breach	
Adequacy referential	
Binding corporate rules for controllers	
Binding corporate rules for processors	
Consent	Adopted on 10-11 April 2018
Transparency	

<sup>1</sup> All adopted guidelines are available at: [http://ec.europa.eu/newsroom/just/item-detail.cfm?item\\_id=50083](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083)

Certification	Preliminary draft adopted on 25 May and public consultation ongoing until 12 July 2018
Accreditation	Work ongoing (following public consultation)
Derogations for international transfers	Work ongoing (following public consultation)

The group will work on the update of other existing opinions, as well as on the European Data Protection Board rules of procedure. The work will continue under the **new Chair** who was elected on 7 February 2018 (Ms Jelinek from the Austrian data protection authority), and confirmed as Chair of the European Data Protection Board on 25 May 2018.

In line with the Letter of Intent accompanying President Juncker's State of the Union speech, we have developed **practical guidance for individuals and citizens**. It is a practical tool launched on 24 January aimed at business (especially SMEs), public authorities and citizens, which are available on the web and in all EU languages. It also entails a chapeau communication presenting the Commission's action to ensure a proper application of the new data protection rules. It was supplemented since then by additional communication materials aimed in particular to SMEs and individuals. The Communication of 15 May on Completing a trusted Digital Single Market for all urges Member States to adopt the necessary national legislation and equip their national data protection authorities to properly enforce the GDPR.

[REDACTED]

[REDACTED]

## **PROTECTION OF PERSONAL DATA AND DATA FLOWS (INPUT OF C4)**

### **CONTEXT**

Amazon and certain of its affiliates participate in the EU-US Privacy Shield Framework. This concerns also Amazon Web Services, which are included in the Amazon Privacy Shield certification since 20 October 2017. Amazon has thus an economic interest in the sustainability of the EU-US Privacy Shield Framework.

### **LINE TO TAKE**

- The participation of companies like Amazon, but also that of many small and medium sized enterprises, confirms the (commercial) interest in the program, which facilitates transfers and reduces costs.
- At the same time, the Privacy Shield strengthens the level of protection of the personal data transferred to companies in the U.S. that are certified under the framework, which is important for maintaining the trust of consumers in Europe.
- Last autumn, the Commission conducted the first annual review of the Privacy Shield, an important milestone and key element of the framework.
- The outcome of this first annual review was positive; the Commission was able to conclude that the U.S. continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield.
- At the same time, the Commission has formulated a number of recommendations on how to improve the practical implementation of the safeguards provided in the Privacy Shield.
- In autumn this year, we will have the second annual review. As one of the major U.S. companies certified under the framework, I count on you to support the sustainability of the Privacy Shield.

### **BACKGROUND**

Amazon has certified with the Department of Commerce and thus adheres to the Privacy Shield Principles. If Amazon does not resolve a complaint relating to the Privacy Shield, a customer in the EU can submit a complaint to a US dispute resolution company (TRUSTe), which provides a third-party dispute resolution service based in the US. If neither Amazon nor TRUSTe resolves the complaint, a customer in Europe may pursue binding arbitration through the Privacy Shield Panel. Amazon is of course also subject to the investigatory and enforcement powers of the Federal Trade Commission.

[REDACTED]

## **SAFETY OF PRODUCTS SOLD ONLINE**

### **CONTEXT**

On 25 June 2018 Amazon, together with three other online marketplaces (Alibaba, Ebay and Rakuten France), signed a Product Safety Pledge with the objective of increasing the safety of products sold online by third party sellers. This initiative sets out specific voluntary actions that go beyond what is already established in the EU legislation.

The commitments include among others: response to notifications on dangerous products by Member State authorities within 2 working days and to other notices within 5 working days; to consult RAPEX and take action when the products can be identified on their websites; and to take measures to prevent the reappearance of dangerous product listings.

This initiative, which is the first one of its kind in the product safety area, is part of the general dialogue with platforms on illegal content online (similarly to the Code of Conduct on Hate Speech or the MoU on Counterfeit Goods).

### **OBJECTIVE(S)**

- To inform that the Commission welcomes the signature of the Product Safety Pledge by Amazon, whose goal is to increase the safety of products sold online.
- To inform them that the Commission will monitor the progress of the Pledge to assess if further actions are needed.

### **LINE TO TAKE**

- To inform that the Commission welcomes the signature of the Product Safety Pledge by Amazon. Ensuring that consumers are protected when they buy online or offline is of paramount importance. Proactive measures from online intermediaries such as the ones included in the Pledge go in the right direction to achieve our common goal of protecting consumers. Setting good practices can also encourage the rest of market players to follow their example.
- To inform that the Commission will closely monitor the progress made on the commitments publishing a report every six months.

### **BACKGROUND**

More and more consumers shop online. Online sales in the EU represented 20% of the total sales in 2016, and this percentage is expected to increase in the coming years. Online shopping is convenient for consumers but it poses certain challenges from the point of view of product safety.

Controlling the safety of products sold online can be also problematic for public authorities. For this reason, last year (1 August 2017) the Commission issued a **Notice on the market surveillance of product sold online** to help authorities with their work. The Notice clarifies the responsibilities of online actors, including platforms and their notice and action obligations to remove illegal content, i.e. dangerous products.

The **e-Commerce Directive** (Article 14) states that online intermediaries are not liable for the illegal content they host (including dangerous product listings), provided that they do not have knowledge of the illegal activity or information or, upon obtaining such knowledge or awareness, they act expeditiously to remove it. The directive does not specify the timing.

## **DEFENSIVES**

### ***Goods Package***

LTT:

- In 2013 the Commission tabled proposals to group under one single legal framework the regulatory provisions on product safety and on market surveillance for both harmonized and non-harmonized products.

[REDACTED]

[REDACTED]

[REDACTED]

### ***Role and responsibilities of fulfilment service providers***

LTT:

- We believe that the interpretation is a balanced one taking into consideration the role fulfilment houses have in the supply chain. In the business model where fulfilment houses are used, the product reaches the consumer with the active participation of these service providers. These economic operators profit from e-commerce and their responsibilities need to be assessed accordingly.
- All actors in the online supply chain have to take part, in a balanced way, in ensuring that products sold to European consumers are safe.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## ANNEX

**Subject: Meeting with Ms Barbara Scarafia, Amazon Vice President & Associate General Counsel (EH)**

**Participants: Amazon: Barbara Scarafia, Einiri Zafeiratou, Sthephane Ducable, CAB: Renate Nikolay (RN), Eduard Hulicius (EH), DG JUST: [REDACTED]**

**Date: 22.11.2017**

**Objective:** The meeting was requested by Amazon for an introduction of Ms. Barbara Scarafia, Amazon Vice President & Associate General Counsel. Main topics discussed: data protection, consumers rights and enforcement, product safety.

### **Key points:**

- Ms. Scarafia from Amazon thanked for receiving them. She expressed that Amazon is a big fan of the Digital Single Market and other EU initiatives, such as geo-blocking, digital contracts and data flows. Amazon is currently working with DG JUST on product safety as well as with DG GROW on counterfeit goods.
- Data Protection:
  - Amazon is working on the implementation of the GDPR and they are interested on e-privacy (because of their advertisement business). Amazon faces challenges to explain to sellers the new EU legal framework on data protection. Amazon does not disagree in principle with the GDPR or e-privacy, but they call the Commission to not force platforms to make things twice: if the e-privacy initiative is going to add extra obligations to platforms than the ones established in the GDPR, then it would be better to go directly to the final solution.
  - Mr. Ducable from Amazon presented a "Code of Conduct for Cloud Infrastructure Service Providers". This Code of Conduct has been prepared between Amazon and other competitors and it is the first Code "GDPR native". The Code has been submitted to the Article 29 Working Party last March and it has been recently considered admissible for review.
  - RN welcomed the initiative of Amazon of the Code of Conduct, foreseen under the GDPR. It comes in a good timing, as Commissioner Jourova is meeting the plenary of the Article 29 Working Party next week. The Commission is now in a crucial phase for the implementation of the GDPR, which has been an excellent example of how proactive implementation should work. This process has been done in three branches. First, through the active involvement on Member States, such as Germany. Second, with the work carried out by the Article 29 Working Party. And third, by additional guidance, mentioned in the speech of President Juncker of the State of the Union. Additional work can be done, such as campaigns for citizens and

working with platforms such as Amazon in cross-linking efforts. Regarding e-privacy, RN supports Amazon's call of need for coherence with existent legislation.

- Consumer Rights and enforcement

- Ms. Scarafia stated that Amazon is a consumer friendly company, which complies with consumers' rights legislation. Amazon calls the Commission to help them to keep promoting innovation that can help consumers, such as their devices Alexa or dash buttons.
- RN expressed that the position of Commissioner Jourova is not being over-protective on consumers policy, but consumers should have the same rights online and offline. The Commission is working in a New Deal for Consumers, coming as a result of a REFIT of consumers legislation. The main conclusion of the REFIT is that the level of protection of consumers is high in the EU, but enforcement is still behind. The Commission wants to strengthen the CPCs, to act in a faster way. The Commission is also reviewing legislation on injunctions.
- MPB explained that CPCs up to now have worked in a corrective manner, but what it would be ideal if they also have a preventive role. MPB asked Amazon to participate in a dialogue with other platforms, CPCs and the Commission to review the state of play and to assess if things put on place are acceptable. For instance, regarding innovation and the new apps designed for Amazon, there could be a dialogue to discuss about these innovations. Amazon reacted positively, although they expressed that they would need to better understand Commission's plans on this.

- Product Safety

- Ms. Scarafia expressed willingness to keep working on product safety issues with the Commission. They defend a risk based approach. Ms. Scarafia highlighted the positive aspects that innovation could bring to product safety, such as machine learning, artificial intelligence, databases and big data.
- RN thanked Amazon for their work on product safety. RN informed about the new key initiative on Artificial Intelligence to be launched during first half of 2018. RN also informed about the Trilateral Summit in June next year and its possible focus on platforms.
- Ms. Zafeiratou explained that Amazon is also following the Goods Package and expressed their concerns if the new package regulates the role of fulfilment houses. If new legislation comes that forces providers of fulfilment houses (such as Amazon) to change their business model, then it would be difficult to keep working on voluntary code of conducts such as the one on product safety.

- Transparency of platforms and Online Dispute Resolution

- EH asked if Amazon considers that there is enough transparency of online platforms. Ms. Scarafia said that every marketplace is different. MPB explained that the challenge is to find the right balance between a flexible legislation and proper enforcement.
- EH commented on the withdrawal of one of Amazon's companies of the Online Dispute Resolution system. Ms. Scarafia did not have knowledge of that withdrawal and asked to have the official letter (action for JUST E.3).





[REDACTED]

· Finally, Amazon invited the Commissioner to participate as a speaker in an event to be organized in 26th September in Brussels; Commissioner Jourova promised to check her availability.



**COMMISSIOBNER VĚRA JOUROVÁ**

**MEETING WITH AIM, FOODDRINK EUROPE AND EUROCOMMERCE**

**LOCATION: BERL 12/176**

**DATE AND TIME: [25/01/2018, 10H00]**

**MEETING OBJECTIVE: TO DISCUSS WITH INDUSTRY REPRESENTATIVES THEIR VIEW  
AND CONTRIBUTIONS REGARDING THE HARMONISED  
TESTING APPROACH ON DUAL QUALITY FOOD**

**MEMBER RESPONSIBLE:**

**CONTACT NUMBER OF ORGANISER:  
[ONLY FOR CONFERENCES ETC.]**

**DG CONTACT & TEL No:  
DIRECTOR:**



**VERSION: 09/11/2018 11:23**

**JUST/123**

**PARTICIPANTS:**

**TABLE OF CONTENTS**

STEERING BRIEF .....3

LINE TO TAKE .....4

BACKGROUND .....5

DEFENSIVES .....6

ANNEX .....9

## STEERING BRIEF

### CONTEXT/SCENE SETTER

9 Member States (BG, CZ, HU, HR, LT, LV, RO, SI, SK) have carried out comparative tests which revealed significant differences in various food and non-food products. This confirms the existence of widespread and sometime very fine market differentiation practices in food but also other basic commodities.

The Commission has clearly stated that the persistence of dual quality is not acceptable and has proposed an articulated action plan to address the issue:

- High level political intervention by President Juncker
- Dialogue with the industry concerned to convince them to have similar products across the EU.
- Development of a harmonised testing protocol for EU-wide tests by DG Joint Research Centre (JRC) to collect comparable evidence and measure the scope and dimension of the matter – AIM, FoodDrinkEurope and EuroCommerce are part of the stakeholder group supporting the project.
- Focus on enforcement of existing EU law by empowering authorities:
  - specific guidance was adopted on 26 September 2017
  - co-funding of tests and capacity building is underway ■

### OBJECTIVE OF THE MEETING

to continue to put pressure on the industry so that more companies align their formulation in their various markets.

### **LINE TO TAKE**

- The Joint Research Centre (JRC) is proceeding fast on the development of the harmonised testing approach for dual quality products.
- Express that you are happy that the associations together with the members they represent have followed the Commission's call to take ownership and to get involved in the JRC's project.
- Express your confidence in the stakeholder involvement strategy pursued by JRC.
- Encourage the associations and their members to keep up the good work with the JRC with a view to have an agreed methodology ready in April but also to participate in the testing-phase by providing list of products to be tested.
- Stress that some important brands have already announced to give up their differentiation practices and to use the same recipe everywhere in the EU.
- Express your conviction that the consumers will value this and invite the associations to advice their members to continue rethinking their differentiation practices.
- Ask whether they have information in this respect.

## BACKGROUND

### *Guidance on applicable food and consumer legislation*

- Food businesses can legally differentiate their products for objective reasons: [REDACTED]
- BUT consumers must not be misled to believe that products sold in different countries are similar when it is not true
  - Confusion can happen when products are marketed under the same brand and with a very similar package
  - Case by case assessments are therefore absolutely needed
  - At the end of the assessment, competent authorities may request more transparency by concerned traders on the differences between the various country versions including changing the packaging strategies.

MS and stakeholders generally support our action plan (High level Consumer Summit on 13 October, Agriculture and Fisheries Council on 6 November and last meeting of the High Level Forum on a Better Functioning Food Supply Chain on 6 December). [REDACTED]

[REDACTED]

[REDACTED]

### *Position of the industry regarding our guidance:*

The industry is generally supportive of our guidance and explicitly welcomed the opportunity to participate in the development of the harmonised testing approach in their letters sent to you (26 July) and President Juncker (19 September). They regularly call on the Commission to take a mediating and neutral role in the debate.

The industry did not provide us with written comment on the guidance yet as they are working on a "best practices" document. [REDACTED]

[REDACTED]

Several food manufacturers, including Ferrero (Nutella), Bahlsen (butter cookies/waffles) and Hipp (baby food) have aligned their recipes across the Single Market.

### *EU funds for capacity building*

These funds are made available under the Consumer Programme. A maximum of 1 million was available for a co-funding rate of 50% or under certain conditions of 70%. The deadline to apply was 19 December [REDACTED]. The grants are managed by the executive agency CHAFEA (in Luxembourg). Attribution decisions are expected by the end of February 2018. It is not possible to disclose any information for the moment.

## **DEFENSIVES**

### ***EP Pilot Project***

- it has been decided that the EP's pilot project will start and support the Commission's Joint Research Centre's project indicatively from end of 2018.

### ***Your advice for the concerned businesses***

- Ideal solution: provide similar high quality to all consumers.
- Second best: rename products and change packages so that consumers can understand that they are not buying products similar to those offered in neighbouring countries.
- In any case: Repair the wrong perceptions (understand better the perception/expectation issues raised by consumers when they compare products of brands across countries).
- Businesses should also be more transparent on the actual measures taken to investigate consumer preferences when they adapt to local taste.

### ***Applicable EU law for this issue***

- The 'General Food Law Regulation' (No 178/2002), which aims at ensuring that only safe food products are placed on the EU market and that consumers are accurately informed and not misled as to the composition and characteristics of the food products offered for sale;
- The 'Food Information to Consumers Regulation' (No 1169/2011), which lays down general labelling rules and requirements, including mandatory provision of a complete list of ingredients enabling consumers to be fully informed of the composition of the food products;
- The 'Unfair Commercial Practices Directive' (2005/29/EC), which ensures that consumers are not misled or exposed to aggressive marketing and that any claim made by traders in the EU is clear, accurate and substantiated. It seeks to enable consumers to make informed and meaningful choices. This horizontal Directive applies to many commercial practices which are also regulated by other general or sector-specific EU legislation, such as food, toys, cosmetics, detergents and others, but only for those aspects which are not covered by sector legislation.

### ***National authorities' powers to enforce the relevant legislation***

- Member States are free to choose the enforcement mechanisms and powers which best suit their legal tradition, as long as they ensure that adequate and effective means exist to prevent unfair commercial practices.
- According to the Consumer Protection Cooperation (CPC) Regulation 2006/2004, cross-border cases of unfair commercial practices, enforcement authorities must be equipped with a set of minimum powers.
- The recent revision of the CPC Regulation will grant enforcement authorities more powers to protect consumers (e.g. to purchase goods as test purchases, inspect, disassemble or test them in order to gather evidence and detect breaches of EU consumer law). It will be applicable by the beginning of 2020.
- Follow-up actions of the Fitness Check of EU consumer law: possible harmonisation of rules on how Member States should calculate penalties for breaches of EU consumer law. This would apply to the Unfair Commercial Practices Directive along with other directives in the consumer protection area.

### ***Specific national food quality standards***

- Under Article 36 of the Treaty (TFEU), and European Court jurisprudence national restrictions to the free circulation of goods (such as binding quality standards) can only be

justified on the basis of overriding grounds, such as health or consumer protection, and they need to be notified to the Commission and the Member States.

- The existing quality standards often result from antiquated national requirements: for example, the German or Austrian 'Food Code' set out certain composition features "which consumers can generally expect from certain food products" (e.g. in Germany fish-sticks are expected to contain at least 65% of fish-meat).
- Remaining national quality standards are questionable in today's Single market. We could ask ourselves if their persistence do not result from mere intra-EU protectionist objectives.
- If the concerned Member States pretend that such quality standards are justified on their home market because of the high expectations from their consumers, I do not see why consumers in other countries would not have the same expectations?
- The dual quality issue has shown us that we need to completely rethink food quality standardisation. Our position was that such a standardisation was not necessary at EU-level.
- But as policy-makers, can we trust that market forces alone will ensure that identical quality is delivered all across the EU? Or should we generalise the example of some of the most liberal Member States and propose specific food quality standards for a number of commonly used products?.

#### ***Price issues***

- Prices are generally set out by retailers. They vary according to local competition. Across countries, variations may also occur due to differentiation in taxation. This is why the Commission is not investigating price related issues.
- However, some of the studies carried out at national level (e.g. HU and HR) show that prices of the compared products are similar or even higher in HU or HR than in AT.

#### ***Alleged vertical restrictions by suppliers***

- We have learnt that part of the problem comes from territorial suppliers' restrictions which prevent retailers from buying where and what they want.
- We have repeatedly called the industry to revisit their market segmentation policies which are no longer adequate as they reflect a state of the Single Market which does not correspond to the reality of today's active cross border trade.
- Furthermore, with the economies of scale permitted by the Single Market of half a billion consumers, it becomes clear that it is neither economically sound to continue fine market segmentation.

#### ***Possible update of the Commission guidance including to non-food products***

- Our guidance clearly states that it may be updated in the light of new evidence based on the common testing methodology.
- This includes also an update regarding products other than food and in so far, the UCPD is a horizontal consumer protection law which can apply as a "safety net" to tackle issues not regulated by sector-specific legislation. It applies to all products and most services marketed in the EU's Single Market. The principles in the guidance which concern the UCPD can therefore mutatis mutandis also be helpful for authorities seeking to examine unfair marketing practices in the area of non-food products.
- To what regards the harmonised testing approach, some of its general principles could certainly be relevant to other types of products.

- The funding offered to Member States to carry out further studies and build enforcement capacities (1 million) stems from the Consumer Programme and is therefore not limited to activities relating to dual quality food.

***Contested validity of test results:***

- Quality is not defined in EU legislation and the industry contested the results of national tests due to different scientific testing methods and diverging interpretation standards.
- Likewise the industry, the Commission is keen to develop and implement a harmonised testing approach which allows for the gathering of robust evidence and for comparable results that are valid across the EU.
- Common testing needs to be widely endorsed and participation from the industry will be key.
- Following the conclusions of the European Council of 9 March, the High Level Forum for a Better Functioning Food Supply Chain has mandated the Commission's Joint Research Centre to work on a harmonised testing protocol in close collaboration with the industry.
- The Commission funds this work with at least EUR 1 million and first results are expected to be available by the end of 2018

## ANNEX

### Outlook on the JRC's harmonised testing approach:

**Problem:** Comparative tests at national level (9 CEEs) have been repeatedly challenged by the industry on the basis of lack of comparability resulting from the use of different methods for testing and data interpretation.

**Solution:** Together with the industry (extended stakeholder network), JRC is developing a harmonised approach (protocol) which can be used by accredited laboratories at national level.

**Outcome:** We will obtain scientific robust and comparable data on the scope and dimension of the problem which can no longer be challenged on the methodological side. For this purpose the JRC has launched an extended stakeholder network including MS as well as industry and consumer umbrella organisations at European level. The idea behind this is to obtain their expertise and to achieve a greater level of acceptance for the testing methodology and future tests.

### Details:

Date	Deliverable/Achievement
<b>Phase I: Development of a harmonised testing methodology</b>	
September 2017	Commission met with representatives of the authorities carrying out comparative tests at national level and the industry and agreement was reached on certain key elements to be discussed in details by the corresponding expert groups (see next row)
January / February 2018	<p><b><u>product selection (30 January)</u></b></p> <ul style="list-style-type: none"> <li>• Pan-European market basket of products to be included: <ul style="list-style-type: none"> <li>○ Based on Eurostat/Nielsen company data and could be supplemented by consumer complaints</li> <li>○ Food business operators would be involved to verify that selected products are in fact comparable</li> </ul> </li> <li>• Minimum number of MS (ideally at least three)</li> </ul> <p><b><u>sampling and testing (31 January)</u></b></p> <ul style="list-style-type: none"> <li>• Preference for sampling at retail-level</li> <li>• Contacting responsible food business operator for explanation if differences are found</li> <li>• Further control-testing upstream the supply chain if food business operator argues that products are the same</li> <li>• Testing should be repeated at different points in time (control)</li> </ul> <p><b><u>sensory analysis (1 February)</u></b></p> <ul style="list-style-type: none"> <li>• <u>First tier:</u></li> </ul>

	<ul style="list-style-type: none"> <li>○ Label comparison</li> <li>○ Sensory discrimination test (ISO standards could be used)</li> <li>• <u>Second tier (if differences are found)</u> <ul style="list-style-type: none"> <li>○ More targeted sensory (profile) testing to explore reason for sensory differentiation</li> </ul> </li> </ul> <p>The expert sub-groups will report back to the extended stakeholder network to make a decision and further considerations regarding the interpretation of data in the network will follow:</p> <p><b><u>data interpretation</u></b></p> <ul style="list-style-type: none"> <li>• Food business operators should have the opportunity to respond to the testing results</li> <li>• Confidentiality of the information provided by food business operators must be guaranteed</li> </ul>
April 2018	Availability of a harmonised testing approach regarding product selection, sampling, testing and data interpretation (conclusion of Phase I)
<b>Phase II: EU-wide testing using the harmonised methodology</b>	
May 2018	Entering into Phase II by selecting accredited laboratories and launch of the testing campaign under the JRC's coordination and logistics
December 2018	Interim report on the progress of testing
September 2019	Report on the outcome of the testing campaign using the harmonised testing methodology

**Previous contacts/meetings with the industry:**

6 December: HLF for a Better Functioning Food Supply Chain where you intervened together with your colleague Commissioner Bienkowska and reaffirmed the stakeholder that the Commission is firmly determined to address the issue and has taken decisive action which DDG Fonseca explained in more detail.

19 October: You opened a dinner in the context of the Annual board meeting of the 30+ CEOs brand businesses of the AIM Association to clarify the Commission's action and to explain to them what the industry needs to do to address the issue of dual quality food

13 October: You presented our guidance and the Commission's action plan during a high-level consumer Summit in Bratislava together with your colleague Commissioner Andriukaitis. Participants, including industry representatives acknowledged that the Commission's action, and in particular the testing approach and the guidance, can contribute to addressing the issue of dual quality.

11 October: You met with AIM, FoodDrinkEurope and EuroCommerce to explain to them the Commission's action and what the Commission expects from the industry ahead of the high-level consumer Summit in Bratislava.

3 October Sherpa meeting of the High Level Forum for a Better Functioning of the Food Supply Chain:

[REDACTED]

Industry representatives further called for the Commission to take the position of an 'honest broker' in a truly multi-stakeholder exchange.

DG GROW and EuroCommerce stressed that part of the problem stems from territorial suppliers' restrictions. GROW's DG, Evans, called the industry to revisit their market segmentation policies which were not adequate anymore and reflected the state of the Internal Market 20 years ago. DG Evans announced that further work will be done on this during the next meeting in December.

19 September industry letter: Following President Juncker's State of Union address, the industry representatives wrote to the President regretting that some brands have been unfairly accused of dual quality. These accusations were, in the opinion of the industry, made on the basis of tests which were not robust enough, or on a flawed interpretation of the results delivered by these tests, without giving the companies concerned any opportunity to provide for possible explanations. The industry stresses the importance of the moderating role of the Commission in this debate and in the upcoming consumer summit in Bratislava on 13 October. The industry expressed its will to cooperate with the Commission on a harmonized testing approach to improve food product comparative tests.

[REDACTED]


3 August technical meeting, your service and cab met with Mars, FoodDrinkEurope and AIM. These organisations indicated that the work on the Code of Conduct was still at a preliminary stage and that possible content could consist in: (i) a clarification that associations are

contrary to dual quality practices; and (ii) possible commitments to ensure more transparency on product composition. Subject to expeditious consultations amongst members which were about to start, a first version of the Code could be ready at the beginning of September. Industry associations were also reflecting on other initiatives such as a meeting with all relevant stakeholders in Slovakia this Autumn or invitations to policy makers (e.g. Commissioner or national authorities) to visit factories.

26 July letter of intent: FoodDrinkEurope, AIM and EuroCommerce sent you a letter, just after your meeting, restating the importance of gathering solid evidence and concluding that they were "also exploring the need for additional measures or commitments to further foster consumer trust".

25 July – your meeting with the industry: you met the representatives of Mars, FoodDrinkEurope, AIM and EuroCommerce to discuss what actions the industry could take to address the issue. The representatives welcomed the opportunity to solve this problem in a spirit of constructive cooperation with the Commission and Member States. Among others, you asked the industry to prepare a code of conduct or commitment to take the necessary measures to prevent dual quality of products across the EU. The associations are looking forward to collaborating with the Commissioner on the details of her plans as they develop.

19 September industry letter: Following President Juncker's State of Union address, the industry representatives wrote to the President regretting that some brands have been unfairly accused of dual quality. These accusations were, in the opinion of the industry, made on the basis of tests which were not robust enough, or on a flawed interpretation of the results delivered by these tests, without giving the companies concerned any opportunity to provide for possible explanations. The industry stresses the importance of the moderating role of the Commission in this debate and in the upcoming consumer summit in Bratislava on 13 October. The industry expressed its will to cooperate with the Commission on a harmonized testing approach to improve food product comparative tests.



26<sup>th</sup> July 2017

## **Manufacturers and retailers' statement after meeting Commissioner Jourová on transparency in product composition**

The undersigned organisations, representing food manufacturers and retailers, welcomed the constructive meeting with Commissioner Jourová (responsible for consumer protection) on 25 July 2017 in Brussels.

During this meeting, the associations reiterated their members' commitment to continue treating consumers across the EU equally and fairly.

Consumer trust and confidence are paramount. The priority of manufacturers and retailers is always to ensure that products sold across Europe comply with European and national regulations that foster one of the highest levels of consumer safety in the world.

Retailers and manufacturers agree on the need to address citizens' concerns in some Central and Eastern European countries about the perceived 'dual quality' in products sold under the same name.

Common, rigorous methodologies, and a transparent and peer-reviewed approach should lead to better and more uniform evidence of the alleged problem, its magnitude and significance. Therefore, the undersigned associations support in principle the initiative and plans of the European Commission to validate consistent testing methodologies using its Joint Research Centre, and commit, both as manufacturers and retailers, to share their expertise to develop a repeatable EU-wide testing methodology to ensure consistent and coherent interpretation of the results.

This should provide reassurance to consumers, create more legal certainty for businesses, and help national authorities enforce current rules on consumer protection.

The undersigned associations strongly advise against national legislation or other measures that would contravene or hamper the workings of the EU Single Market, or put unnecessary burdens on manufacturers in their efforts to offer consumers the best choice of the best products.

Finally, the associations call on national authorities to establish or strengthen dialogue with key operators in the food chain locally.

The associations look forward to collaborating with the Commissioner on the details of her plans as they develop. They are currently also exploring the need for additional measures or commitments to further foster consumer trust.

**AIM - EuroCommerce - FoodDrinkEurope**

\*\*\*

## **19th September 2017- Letter to President Juncker**

Subject: Treating all EU consumers equally and fairly

Dear Mr President,

As representatives of some of Europe's leading consumer goods industries, we are keen to ensure that any allegations of dual quality of products are addressed promptly by the companies concerned. Our whole industry is treating such allegations with the utmost seriousness.

In this context, we welcome Commissioner Jourová's proposal to launch a dialogue with other parties concerned, including consumer associations, to create the conditions for lasting results. We will be writing separately to Ms Jourová to offer our best efforts in getting this dialogue started promptly and on the right footing.

We received an invitation to participate in the Bratislava conference organized at the initiative of Prime Ministers Fico and Sobotka on 13th October. We are encouraged by the call for constructive engagement of the industry. As is good practice in any multi-stakeholder dialogue, such engagement should be the outcome of the dialogue rather than a unilateral undertaking and we would like to emphasise the importance of an active convening and moderating role of the Commission. This will give all of us a better understanding of facts and of all parties' expectations in order to achieve a mutuality of benefits. We believe this cooperative approach will be the surest way to achieve a satisfactory outcome for all, and first and foremost consumers themselves. We will be cooperating with the Commission on a harmonized testing approach to improve food product comparative tests and look forward to deepen this cooperative approach.

Some brands have recently been unfairly accused of dual quality, based on tests that were not robust enough or on a flawed interpretation of results, without giving the companies concerned an opportunity to explain. Subsequent apologies from the authorities cannot undo the damage to those brands' reputation. Gaining and maintaining consumer trust is fundamental to our industry's success. Such success would never be achieved while condoning the notion of second-class consumers. It goes against everything our industry believes in.

**AIM - EuroCommerce - FoodDrinkEurope**

[Redacted signature block]



**COMMISSIOBNER VĚRA JOUROVÁ**

**MEETING WITH MEETING SHERYL SANDBERG, COO, FACEBOOK**

**LOCATION: BERL 12/176 [OR IF EXTERNAL, ADD ADDRESS]**

**DATE AND TIME: 23/01/2018 15:00**

**MEETING OBJECTIVE: TO DISCUSS 1.HATE SPEECH, 2A) DATA PROTECTION –  
GDPR, 2B) PRIVACY SHIELD, 3.E-EVIDENCE**

**MEMBER RESPONSIBLE: BRAUN DANIEL**

**DG CONTACT & TEL NO:**

**DIRECTOR:**



**VERSION: 08/11/2018 13:06**

**JUST/123**

## TABLE OF CONTENTS

STEERING BRIEF .....	3
TOPICS .....	4
TOPIC 2 A) GDPR.....	8
TOPIC 2B) PRIVACY SHIELD .....	13
TOPIC 3 E-EVIDENCE.....	19
TOPIC 4 CYBER VIOLENCE AGAINST WOMEN AND GIRLS .....	23
ANNEXE.....	24

## STEERING BRIEF

### CONTEXT/SCENE SETTER

This visit from Sheryl Sandberg is a follow up to a previous discussion in California. She will be accompanied by:

- Richard Allan, Vice President EMEA Public Policy, Facebook
- Thomas Myrup Kristensen, Managing Director EU Affairs, Facebook
- Joel Kaplan, Vice President Global Public Policy, Facebook

She is also meeting VP Ansip and Commissioner Moedas on the same day to discuss the future of the digital single market, Platforms, illegal content online, E-Privacy and Fake news. She has attended the Macro 'do business in France' initiative at Versailles and will move to DavoS;

### OVERALL OBJECTIVES

- Secure the continued commitment by Facebook on tackling illegal hate speech through the **Code of Conduct on illegal Hate speech**
- Inquire about **addressing cyber-violence against women** in a similar way as illegal hate speech targeting minorities.
- Promote the benefits of the **GDPR** and inform about and promote the functioning of the **Privacy Shield**
- On **e-evidence**, encourage support for ongoing Commission initiatives to support practical measures on e-evidence and the forthcoming legislative proposal.

## **TOPICS**

### **HATE SPEECH**

#### **CONTEXT**

On 31 May 2016 the European Commission together with Facebook, Microsoft, Twitter and YouTube announced the Code of Conduct on Countering Illegal Online Hate Speech, which includes a series of voluntary commitments to combat the spread of such content in Europe. The four platforms agreed to assess the majority of users' notifications in 24h for illegal hate speech as defined in relevant national legislation implementing EU law and committed to remove, if necessary, those messages when considered illegal. The four companies also committed to improving the support to civil society as well as the coordination with national authorities.

On 28 September, the Commission adopted a Communication which provides for guidance to platforms on notice-and-action procedures to tackle illegal content online. The importance of sectorial dialogues including the one countering illegal hate speech online and the need to continue working with the implementation of the Code of Conduct are featuring prominently in this guidance document.

The Communication announced that the Commission will monitor the progress of the IT Companies and assess, by May 2018, impacts of actions to see if additional (including legislative) measures would be needed.

As a follow up to the Communication, several Commissioners met with representatives of online platforms on 9 January 2018 to discuss progress made in tackling the spread of illegal content online

On 19 January, the Commission published the results of the third round of monitoring of the implementation of the code of conduct. The results showed a significant improvement of the level of implementation in comparison to the first and second monitoring published in December 2016 and June 2017, will feed into to the impact assessment actions to see if additional (including legislative) measures would be needed.

#### **OBJECTIVE(S)**

- Commend Facebook for showing leadership on this file while underlining the need for continued engagement and progress.
- Discuss follow up to the September Communication on Illegal Content

## LINE TO TAKE

- Through the Code of Conduct on Countering Illegal Hate speech Facebook along with Microsoft, YouTube and Facebook agreed to assess the majority of users' notifications of in 24h also respecting national legislation implementing EU law on hate speech.
- The work in the code of conduct was important in terms of feeding into the Commissions Communication of 28 September which provides for guidance to platforms on notice-and-action procedures.
- One of the strongest features of the Code of Conduct is the monitoring process, which allows us to continuously assess progress and the difference we make on the ground.
- As you know, we have just finalised the third monitoring of the implementation of the code of conduct and the results are very good.
- On average, the IT Companies responded by removing more than 70% of the deemed manifestly illegal content notified compared to 59% six months ago and only 28% one year ago.
- The amount of notifications reviewed within 24 hours has also significantly improved and all the IT Companies now fully meet the target of reviewing the majority of the notifications within the day.
- In terms of rate of removal and time to removal, Facebook was in the lead, removing 80,8% of the notified content and assessing notifications within one day in 89,2% of the cases.
- Together with the other IT Companies, Civil Society and Member States, Facebook has shown that the collaborative approach of the Code of Conduct works. By creating an alliance between all the relevant actors, It Companies, civil society Member States and law

enforcement, you have managed create a process of converging interests where we are all working together to achieve the dual objective of ensuring effective removal of illegal racists and xenophobic hate speech while respecting freedom of expression online.

- The results will be very important to the Commission when we assess see if additional measures would be needed to tackle illegal content and, if so, which ones.
- While it is too early to give an indication on the outcome of the assessment, I want to fully preserve the Code of Conduct and its progress.
- Still, work remains to be done, in particular in relation to reporting (public transparency) and user transparency, which is an important guarantee for freedom of expression online. However, I also note that Facebook was the best performing company in terms of feedback to users.
- Another area which needs to be developed further is how to address the cyber violence against women. It is a phenomenon which I want to focus during my dialogue with IT companies.
- We have shown that the code is an efficient way to obtain results and we should now focus attention on ensuring its status as an industry standard that allow for the "onboarding" of as many relevant social media platforms as possible.
- I count on Facebook to continue showing leadership on the efforts to prevent racism and xenophobia and apply rules that apply offline also online.
- Your communication to other companies about the experience of working with the code from an industry perspective is of course very important and appreciated. Our next challenge is to demonstrate that this form of collaboration is a sustainable model not only for large platforms but also for small SME's and

start ups.

## **Background**

After three rounds of monitoring, regularly carried out since its adoption, the Code of Conduct on countering illegal hate speech online has contributed to achieve important results through a path of continuous progress. According to the latest data:

- On average, the IT Companies responded by removing more than 70% of the deemed manifestly illegal content notified. Facebook removed 80,8% of the content YouTube 75,2% and Twitter 45,6%. This corresponds to a steady improvement to the removal rate of 59% recorded in the second monitoring exercise ended in May 2017, which in turn doubled the removal rate of the first monitoring exercise of December 2016, where only 28% of the notifications led to the removal of the notified content.
- The amount of notifications reviewed within 24 hours has largely improved, reaching an average of more than 81%, considerably higher than the 40% and 51% registered one year and six months ago respectively. The third monitoring round shows that all IT Companies now fully meet the target of reviewing the majority of the notifications within the day, Facebook reviewed within the day 89,2% of notifications, YouTube 62,8%. The improvement in time of assessment of Twitter was particularly striking moving from 39% in May 2017 to 79,9% in this third exercise

[REDACTED]

## TOPIC 2 A) GDPR

### CONTEXT

You are meeting with Sheryl Sandberg, COO at Facebook.

In 2017, you had a meeting with MR. Elliot SCHRAGE, Facebook's Global VP for Policy and Communications.

The reaction of Facebook to the GDPR was not entirely positive. European Digital Media (EDiMA), where Facebook is a member, expressed some concerns after the adoption of the GDPR. According to those, GDPR failed to strike the balance between protecting the citizens' fundamental right to protection of personal data and allowing the business in Europe to grow. On the contrary, it "undermines the ability of businesses in Europe to innovate, operate efficiently and grow". However, the company is pragmatic and ready to make the new legislative framework workable. That is why it called for an open and transparent implementation process and wide consultations with all relevant stakeholders, including the industry.

Note also that Facebook 'Custom Audiences' tool has been the subject of investigation in Germany by the Bavarian DPA. With this tool Facebook promises advertisers to target both existing and potential customers directly. In a press release of 4/10/2017, the Bavarian DPA considers that the permissibility of using Custom Audiences from customer lists must depend on consent having been granted within the meaning of Section 4a of the Federal Data Protection Act (BDSG). Despite the use of the hashing process, it argues that the data transmitted are at least personal for Facebook, which is why the procedure requires justification from a data protection perspective. It found no evidence of any legal basis for such activities.<sup>1</sup> [Comment: with the GDPR in place, Facebook must also find a legal basis under Article 6 GDPR for the processing of personal data, and any further processing must meet the compatibility test in Article 6(4) GDPR.]

### OBJECTIVE(S)

The objectives of your meeting would be to:

- Promote the benefits of the GDPR;
- Explain the Commission's priorities during the transition period;
- Reassure that businesses have an opportunity to be actively involved in actions conducted during the transition period.
- To find out how they will communicate about new GDPR Rules.

---

<sup>1</sup> <https://www.spiritlegal.com/en/news/details/facebook-custom-audiences-and-data-protection-law.html>

#### LINE TO TAKE

- The New European Union data protection regulation – the General Data Protection Regulation (GDPR), will be applicable from 25 May 2018. The new legislation modifies and updates data protection rules at EU level to make Europe fit for the digital age.
- The GDPR is a competitive advantage a trust-enabler and a key instrument to ensure level-playing field for all companies operating in the EU market. Increased trust from consumers will provide further business opportunities and chances for innovation. Companies will also have easier access to the whole EU market, with the current 28 national legislations being replaced by one, simple and clear legal framework. The GDPR is not a revolution; it simplifies the legal landscape for businesses and brings enhanced legal certainty for their operations.
- Commission is working closely with Member States to accompany them in the process of adapting or repealing their existing laws as necessary. We are fully aware that one of the main concerns of business is that measures taken at national level must not lead to any new fragmentation.
- We are also supporting the work of the Data Protection Authorities who have a key role in ensuring coherent interpretation and enforcement of the new rules. The Article 29 Working Party is playing an active role in preparing guidelines for companies and other stakeholders.
- Article 29 Working Party has already issued six guidelines to assist with implementation and interpretation of new legislation (on data portability, data protection officers, lead supervisory authority, data protection impact assessments administrative fines, and on urgency procedures). It has adopted guidelines on data breach

notifications and profiling which were subject to public consultation until 28 November and are currently being finalised. At its last plenary meeting on 28-29 November, the Article 29 Working Party adopted guidelines on consent and transparency which are now subject to public consultation (until 23 January 2018). Businesses are strongly encouraged to take advantage from the current consultation and provide their views.

- We also want to maintain an open dialogue with other stakeholders, notably businesses, to ensure they are aware of their obligations and also dispel doubts about the application of the new rules. For instance, we held our first multi-stakeholder expert group on 19 October to support the application of the GDPR in view of opinions of its members, including academia, legal practitioners, civil society and business representatives.
- As announced in the letter of intent following President Juncker's State of the Union speech, the Commission will provide guidance to businesses, especially SMEs, and individuals so as to raise their understanding of the new rules in view of their application as of May 2018. This guidance will take the form of a practical online toolkit. We will have it ready by the data protection day on 28 January. We are also supporting financially awareness-raising activities carried out at national level, including by Data Protection Authorities.

## **DEFENSIVES**

### **How is the Commission planning to ensure that citizens and business are aware of new legislation?**

- We consider it essential to foster a uniform interpretation of the GDPR across Member States, hence our active work with national authorities either bilaterally or in the GDPR expert group, and our support to the work of Article 29 Working Party to produce a comprehensive set of guidelines. Existing national guidelines should be brought into compliance with those EU level WP29 guidelines since we are well aware of industry's concerns regarding the risk of inconsistent application.
- As already mentioned, EU grants are being allocated for training of DPAs and national authorities (including the production of materials), others in the coming months will more specifically target awareness-raising among SMEs and the general public. Building on this and to accompany these various actions, we have developed guidance, in the form of a toolkit, in order to prepare business and citizens about the new rights and obligations under the GDPR. This will be launched on our website by Data Protection Day on 28 January.
- We continue our open dialogue with all stakeholders, including civil society and businesses, to ensure that they are aware of their obligations and to dispel any doubts they may have about the application of the new rules.
  - We held our first multi-stakeholder expert group on 19 October to support the application of the GDPR in view of opinions of its members, including academia / legal practitioners / civil society and business representatives.
  - We also have regular exchanges to discuss about the GDPR and the sector specific issues. On 23 October, the Commission services held a workshop with more than 150 stakeholders active in the health sector.
  - On 27 November we held a workshop with the EU umbrella federation of SMEs and their national members to better understand the specific needs of SMEs.
  - On 1<sup>st</sup> February we will hold a workshop with the consumer organisations (BEUC and member organisations).

### **What is the Commission position on the guidelines recently published by the Article 29 Working Party?**

- The guidelines of the Article 29 Working Party are very important to provide increased legal certainty to stakeholders since they will guide the

data protection authorities when implementing the GDPR.

- The Commission supports the work of the Article 29 Working Party and share with its members its views and expertise on the provisions of the GDPR. It also strongly encouraged the Working party to conduct public consultation on the draft guidelines.
- However, the Article 29 Working Party (and after May 2018 the European Data Protection Board) is an independent body and therefore the content of the guidelines are their responsibility.

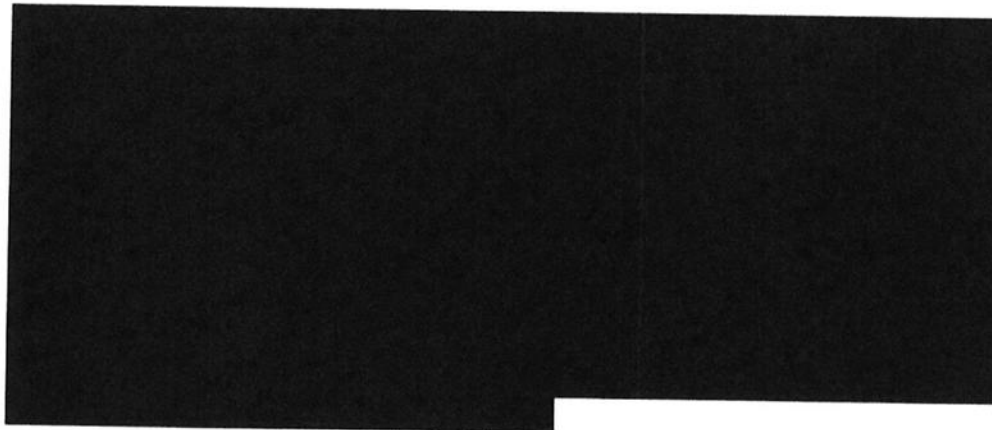


## TOPIC 2B) PRIVACY SHIELD

### CONTEXT

Facebook is certified under the Privacy Shield. Transfers of personal data from Facebook Ireland Ltd to Facebook servers located in the U.S. were the subject of the proceedings between privacy activist Max Schrems and the Irish Data Protection Commissioner which led to the invalidation of the Privacy Shield's predecessor, the Safe Harbor framework, by the Court of Justice in its *Schrems* ruling. The so-called Schrems II case (see defensives) is equally based on a complaint by Mr Schrems against data transfers by Facebook, this time on the basis of so-called "Standard Contractual Clauses".

The Commission conducted the first annual review of the Privacy Shield mid-September 2017 and published its report on 18 October 2017. At the end of November 2017, the EU data protection authorities adopted their own report on the first annual review, which in many aspects is aligned with the Commission's views but also contains more critical language, in particular as regards surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA) and the powers and independence of the Ombudsperson. The data protection authorities call for improvements to be made by the next annual review, but want to see the appointment of a permanent Ombudsperson and a clarification of the Ombudsperson's rules of procedure before the end of May 2018. If their concerns are not addressed within the indicated timeframes, the data protection authorities threaten to take action, including possibly by challenging the Privacy Shield decision before national courts.



### OBJECTIVES

- Inform about the outcome of the first annual review of the functioning of the Privacy Shield and the follow-up to the Commission's report.
- Invite Facebook to support the sustainability of the Privacy Shield framework, in particular by arguing in favour of a swift implementation of the Commission's recommendations.

#### LINE TO TAKE

- Since the launch of the Privacy Shield (on 1 August 2016), more than 2,600 companies have joined.
- The participation of companies like Facebook, Google, IBM and Microsoft, but also that of many small and medium sized enterprises, confirms the (commercial) interest in the program, which facilitates transfers and reduces costs.
- At the same time the Privacy Shield strengthens the level of protection of the personal data transferred to U.S. companies certified under the Shield, which is important for maintaining the trust of consumers in Europe.
- Last autumn, the Commission conducted the first annual review of the Privacy Shield, an important milestone and key element of the framework.
- The outcome of this first annual review was positive; the Commission was able to conclude that the U.S. continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield.
- We have seen a number of improvements compared to the old Safe Harbour framework. In particular, the Department of Commerce now manages more tightly the certification process and carries out closer checks the applications for certification.
- But the Commission also formulated a number of recommendations on how to improve the practical implementation of the safeguards provided in the Privacy Shield.
- Some of these recommendations are of an operational nature (e.g. compliance monitoring by the Department of Commerce) and we are confident that these issues can be addressed rather easily.
- My staff is in contact with the Department of Commerce (which is in charge of the administration of the Shield) on

this but it would be important that you also pass the message that this is important to show some movement and some progress following our recommendations.

- This is all the more important as also the data protection authorities in the EU who participated in the annual review want to see certain improvements without delay. They have threatened to take action – including bringing the Privacy Shield before national courts – if their concerns are not addressed in time.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- As one of the major U.S. tech companies, I count on you to support the sustainability of the Privacy Shield by arguing in favour of a swift implementation of our recommendations in your contacts with the U.S. administration and with Congress.

## BACKGROUND

The Privacy Shield provides for a review to be conducted on an annual basis. The purpose of the review is to carefully assess the proper functioning, implementation, supervision and enforcement of the Privacy Shield framework. This concerns all aspects of the framework: both compliance by companies and by U.S. authorities, including in the field of national security access to personal data.

The first annual review took place on 18-19 September in Washington, DC. On 18 October, the Commission adopted and published its Report to the European Parliament and Council on the first annual review of the functioning of the EU-U.S. Privacy Shield, which was presented to the EP's LIBE Committee on 6 November and presented to Member States in the Council on 21 November.

While the Report concludes that the U.S. does continue to ensure an adequate level of protection for personal data transferred under the Privacy Shield, it also identifies a number of areas where the implementation of the framework should be improved. To this end, it makes a number of recommendations:

In the **commercial area**, the Commission recommends

- that companies should not be allowed to publicly announce that they are Privacy Shield-certified until the Department of Commerce has finalised the certification;
- that the Department of Commerce conducts regular searches for companies falsely claiming participation in the Privacy Shield;
- that the Department of Commerce conducts compliance checks on a regular basis;
- that the Department of Commerce and the Data Protection Authorities work together to develop guidance on the legal interpretation of certain concepts in the Privacy Shield (e.g. with regard to the principle of accountability for onward transfers and the definition of human resources data);
- that the Department of Commerce and the EU Data Protection Authorities strengthen their awareness raising efforts (e.g. to inform individuals about how to exercise their rights under the Privacy Shield).

In the area of **national security**,

- the Commission would welcome if the U.S. Congress would consider favourably enshrining in the Foreign Intelligence Surveillance Act the protections for non-Americans offered by Presidential Policy Directive 28 (PPD-28);
- the Commission calls on the U.S. administration to swiftly appoint a permanent Privacy Shield Ombudsperson, as well as the missing members of the Privacy and Civil Liberties Oversight Board (PCLOB);
- the Commission calls for the public release of the PCLOB's report on the implementation of PPD-28.

In both the commercial and national security areas, the Commission also calls on

the U.S. authorities to proactively fulfil their commitment to provide timely and comprehensive information about any development that could raise questions about the functioning of the Privacy Shield.

## DEFENSIVES

### **Two actions for annulment have been brought against the Privacy Shield.**

- Two actions for annulment of the Privacy Shield decision (one brought by Digital Rights Ireland and one by La Quadrature du Net) have been lodged with the General Court. The case of Digital Rights Ireland has recently been declared inadmissible by the Court.
- While we cannot of course predict the outcome of the other case – like in any other proceedings before the Court – we are confident that the adequacy decision will withstand judicial scrutiny. We strongly believe that the decision is lawful and in particular fulfils the requirements stipulated by the Court in the *Schrems* ruling. Otherwise, the Commission would not have adopted the decision in the first place. Neither would we have received overwhelming support from the Member States.
- This being said, the commitments made under the Privacy Shield are not the only thing that matters. It will also be important that the U.S. honours its commitments in practice and fully implements the framework. This is yet another reason why the Annual Review was so important, but this now has to be followed-up by action on the recommendations that the Commission and the data protection authorities have issued.
- *[NB: In the case lodged by La Quadrature du Net, the Commission has submitted its defence in September. The applicant had until late December to file its reply (second round of written pleadings). Several Member States as well as a number of private entities have requested and received permission to intervene in the case in support of the Commission. They filed their submission in mid-December. We expect an oral hearing at the earliest in late 2018 and the judgment not before mid-2019.]*


[REDACTED]

[REDACTED]

[REDACTED]



**The EU DPA's represented in the Article 29 Working Party may decide to suspend transfers based on the Privacy Shield if their concerns are not addressed on time.**

- It is the purpose of the annual review mechanism to address issues before they become problems. This is why we are working with our U.S. partners on the implementation of our recommendations and we are confident that such a scenario can be avoided.
- 

### TOPIC 3 E-EVIDENCE

#### CONTEXT

Facebook is a key company with regard to access to electronic evidence. It has set up an online platform to receive (non-content data) law enforcement requests which has been positively received by Member States law enforcement end users and could even possibly serve as a model for others. Facebook is ready to cooperate with EU law enforcement on legitimate requests, but does not want to hand over data to some non-EU third countries in order to protect the rights and freedoms of customers.

In recent stakeholder consultations, Facebook has emphasised the need to avoid **conflicts of law** between EU and US legislation. Facebook is also aligned with Google and Microsoft in emphasising that if the service provider is providing solutions for corporate customers, the primary target of a Law Enforcement production order should be the corporate user of the service and not the service provider.

Facebook was critical regarding a common legal framework for direct access, which is no longer in the scope of the draft initiative.

In your meeting with Facebook Vice-Presidents (Schrage, Allen, Beringer) and Privacy lead Deadman last September, Facebook expressed support for practical measures on e-evidence (single points of contact, training on mutual legal assistance), but raised concerns about legislative measures that could create conflicts of laws for companies.

Facebook has been proactively involved in consultation for the forthcoming legislative proposal on e-evidence, including a recent meeting with Kevin O'Connell and DG Justice (meeting report in background).

#### OBJECTIVE

- Encourage support for ongoing Commission initiatives to support practical measures on e-evidence and the forthcoming legislative proposal.

#### LINE TO TAKE

- I am grateful for Facebook's proactive engagement in the stakeholder consultation for our forthcoming proposal on e-evidence, as well as on the ongoing practical measures to improve cross-border access to e-evidence, which we discussed when I visited Silicon Valley in September.
- Work is ongoing on our envisaged proposal, due to be adopted in February. It would introduce a cross-border European Production Order, for the disclosure by service providers such as Facebook of information stored in

electronic form that could serve as evidence in the framework of criminal investigations or proceedings.

- This proposal will be drafted in full accordance with EU data protection rules and respect of fundamental rights. It will also address conflict of law situations.
- The feedback we received from service providers has been extremely useful for us. It has helped us to shape our proposal in order to find a good balance between all interests at stake.
- I am grateful for your ongoing support in this initiative that will deliver a standardised EU approach and more legal certainty for all concerned.

## DEFENSIVES

### *Costs for service providers will be huge and the administrative burden disproportionate*

The Impact Assessment has assessed the burden for service providers linked to the proposal. It concludes that the introduction of a European Production Order, even if combined with the obligation to designate a legal representative within the EU, will even generate savings for them, notably because it will establish a clear legal framework compared to the current practice of voluntary cooperation, with clear rights and obligations on both sides. This is also why several service providers, including Facebook, support the introduction of a mandatory framework.

### *Conflicts of laws – you will force us into something illegal under U.S. law*

A clause on ensuring international comity will be included in the proposal. Its aim is also to prevent that service providers are faced with situations of conflicts of law, as is more and more the case today. This is also a very important issue for the Commission, in particular in view of reciprocal responses by third countries which could affect fundamental rights of persons protected by EU law, such as the data protection acquis. A procedure will be set up, whereby the service provider can raise such conflicts of law with the issuing authority, and which can also involve the third country.

### *There is a lack of standard of what legitimate access looks like*

The proposal contains a set of conditions and safeguards which aim to ensure respect for proportionality and fundamental rights while at the same time making sure the instrument remains an effective tool for law enforcement and judicial authorities. This includes thresholds delimiting the scope, notification requirements and judicial remedies for persons affected and even rights for service providers that exceed by far what exists in domestic legislation in the Member States.

## BACKGROUND

### Meeting on 10 January 2018 between CAB JOUROVA and Facebook

- Facebook (FB) highlighted its work on the non-legislative side of law enforcement access to data requests, notably trying to clarify what authorities may or may not access.
- FB welcomed the constructive and open working relationship with HOME and JUST services as part of the public consultation.
- This proposal is an opportunity for the EU to show leadership, since access to data by law enforcement is a global issue and the harmonisation in the EU space is necessary, given the different procedures in place in the MS for accessing data.
- On the US side, Congress is constantly pushing EU's law enforcement authorities back, because there's a lack of standards on "what good

(legitimate) access looks like".

- FB's biggest concern is the conflicts of law issue, notably between EU and US laws. They noted that US ISPs have different modus operandi when dealing with requests. For FB, the place where data is stored should not matter. What is essential is the safeguarding of data protection standards, the place where the receiving company is incorporated and, most importantly, the jurisdiction where the user is.
- US Congress has traditionally seen this as an internal affair, linked to the Stored Communications Act. FB has actively engaged with Congress to show the matter has an external dimension, since foreign law enforcement authorities have a need to access US providers' databases. FB is pushing the DoJ to enter into agreements with 3rd countries, but there are no criteria yet for what said countries have to comply with to get such an agreement.
- FB expressed concern that the forthcoming proposal isn't based on the assumption that an agreement between EU-US for companies to provide data to foreign law enforcement authorities is in place.
- FB receives 75.000 requests a year from law enforcement, EU authorities being among the most active (Latest Transparency Report published 22 December 2017)
- FB wants to encourage other ISPs (like instant messaging services) to be cooperative with law enforcement. Maybe a collaborative/knowledge transfer platform between ISPs would help. They noted the possibility that companies who don't want to be cooperative will ultimately withdraw their establishment from the EU.



## **TOPIC 4 CYBER VIOLENCE AGAINST WOMEN AND GIRLS**

### **Background on cyber violence against women and girls**

The Commission recognises cyber violence as a form of gender-based violence, which it is committed to eliminating as part of its work to promote gender equality in the EU. In 2017, the Commission launched focused actions to combat violence against women, providing support for projects tackling the problem. A number of these initiatives aim to increase reporting of online sexual harassment, as well as awareness of sexism online.

The Commission co-funds the European Safer Internet Centres, in order to raise awareness, among minors and their carers, of risks online and protection methods. This includes sexual violence, harassment and child sexual abuse images online, which affects mostly girls.

The European Institute for Gender Equality has issued a recent report on cyber VAWG showing national initiatives, such as provisions criminalising revenge porn in the U.K., France, Germany or Malta.

EU Member States that have ratified the Istanbul Convention must establish, in their national law, offences on stalking and sexual harassment. The Convention encourages cooperation with the private sector and the media to tackle this problem. The EU is in the process of acceding the Istanbul Convention which will help to streamline national approaches to combat VAWG, including cyber violence. The Commission continues to encourage Member States to consider ratification of this Convention.

Legal protection for victims of cyber violence is included in the Victims' Rights Directive and the Directive on trafficking in human beings. The Victims' Rights Directive ensures that victims get access to general and specialised support services, responding to their individual needs and providing for emotional assistance and counselling. Cybercrime is also a priority for Europol, through the European Cybercrime Centre (EC3) to improve law enforcement cooperation on online sexual coercion and extortion against minors.

The Commission is also addressing cyber violence and hate speech under initiatives creating the Digital Single Market. The Electronic Commerce Directive provides basis for notice and takedown in response to court orders or allegations of illegal content. Moreover, the proposed revision of the Audiovisual Media Services Directive contains strong provisions for internet platforms to set a flagging system. The Commission is also working with platforms through the Code of Conduct against online hate speech to increase reporting and takedown of harmful content. The Commission's work on platforms and data economy will further clarify the issue of liability of intermediaries.

## ANNEXE

### **Curriculum Vitae - Sheryl Sandberg** (source Bloomberg<sup>2</sup>)

Ms. Sheryl K. Sandberg has been the Chief Operating Officer of Facebook, Inc. since March 24, 2008.

Ms. Sandberg is responsible for helping Facebook scale its operations and expand its presence globally and also managed sales, marketing, business development, legal, human resources, public policy, privacy and communications.

Ms. Sandberg served as a Vice President of Global Online Sales & Operations at Google Inc. from November 2001 to March 2008. She joined Google Inc. in 2001.

Ms. Sandberg served as the Chief of Staff for the United States Treasury Department under President Bill Clinton, where she helped lead its work on forgiving debt in the developing world. She served as a Management Consultant with McKinsey & Company, Inc. and as an Economist with The World Bank, where she worked on eradicating leprosy in India.

She has been an Independent Director of The Walt Disney Company since March 2010.

She has been an Independent Director of Facebook, Inc. since June 25, 2012 and SurveyMonkey Inc. since July 2015. She serves on the board of the Center for Global Development. She served as a Director of The Advertising Council, Inc. She served as a Director at Starbucks Corporation from March 2009 to March 21, 2012 and eHealth, Inc. from May 2006 to December 17, 2008. She serves as a Director at One Campaign and Leadership Public Schools.

She is Director of Google.org/the Google Foundation and directs the Google Grants program. She serves as a Director of The Brookings Institution, The AdCouncil, Women for Women International and V-Day.

In 2008, she was named as one of the "50 Most Powerful Women in Business" by Fortune and one of the "50 Women to Watch" by The Wall Street Journal.

Ms. Sandberg holds a.B. in Economics from Harvard University and was awarded the John H. Williams Prize as the top graduating student in Economics. She was a Baker and Ford Scholar at Harvard Business School, where she earned an MBA with highest distinction.

---

2

<https://www.bloomberg.com/research/stocks/people/person.asp?personId=27544173&privcapId=29096>



**COMMISSIONER VĚRA JOUROVÁ**

**MEETING WITH MR J. FRANK (MICROSOFT) AND MR E. HOLDER (FORMER AG OF THE U.S.)**

**LOCATION: BERL CAB ROOM**

**DATE AND TIME: 29/11/2017, 15:00**

**MEETING OBJECTIVE: TO DISCUSS TRANSATLANTIC REGIMES FOR CROSS-BORDER ACCESS TO DIGITAL EVIDENCE**

**MEMBER RESPONSIBLE: KEVIN O'CONNELL**

**DG CONTACT & TEL No:**



**DIRECTOR:**

**ALEXANDRA JOUR SCHROEDER**

**VERSION: 09/11/2018 11:16**

**JUST/123**

**PARTICIPANTS:**

## CONTEXT

Microsoft has consistently been in favour of the Mutual Legal Assistance (and European Investigation Order) channel rather than of direct cooperation solutions for cross-border access to electronic evidence that they hold. Microsoft has called for more legal certainty and transparency on the side of law enforcement authorities and, like other providers, complains about conflicts of law (e.g. having to comply with data protection and users' privacy on the one hand and to execute mandatory production orders, on the other hand). However, Microsoft is part of agreements concluded with some MS (FR, UK, BE) on direct cooperation with law enforcement authorities on a voluntary basis.

Microsoft representatives met the Commission services several times in relation to the e-evidence file, both at service level and at Cabinet level, in particular:

- Lobbying the Commission to file an '*amicus curiae*' brief in the review of the pending Microsoft Ireland Supreme Court case.
- Underlining the need for the Commission to take into account the above-mentioned case as well as other legislative developments in Washington, such as the International Communications Privacy Act (ICPA) of 2017, when presenting a proposal on e-evidence.
- Expressing concern about the possibly wide geographic scope of the Commission's proposal and resulting conflicts of laws.

## OBJECTIVE

- Present the state of play on the implementation of the practical measures, as well as on the upcoming Commission legislative proposal.

## **Intro, Practical Measures**

- I welcome the active participation of Microsoft in our work on access to electronic evidence. The practical experience shared by your colleagues during bilateral meetings with my services and roundtables with other providers, industry and civil society are crucial for us to better understand this complex issue and to assess the impact of our future legislative proposal.
- At EU level, we are monitoring the transposition of the Directive regarding the European Investigation Order, and on that basis working on some practical measures, to improve judicial cooperation, such as the online portal for electronic requests and responses.
- We are engaged in a regular dialogue at technical level with your Department of Justice (DoJ) and we are pursuing the implementation of different practical measures including funding for training and exchange of best practices to improve the knowledge of EU law enforcement and judicial authorities about both US MLA procedures and cooperation with US-based providers.
- Beyond debates on the practical measures that could facilitate and simplify your daily work with our Member States' law enforcement and judicial authorities, we want

to provide EU citizens, practitioners and companies a high level of legal certainty and protection of fundamental rights.

### **Planned Legislation**

- As announced in the Commission's 2018 Work Programme, a proposal to improve cross-border access of law enforcement authorities to electronic evidence is due to be adopted in Q1 2018 (January 24).
- An extensive expert consultation process has taken place since June 2016 to collect the views of relevant stakeholders, including public authorities, judges and prosecutors and service providers. Microsoft has been well represented during this consultation.
- In cooperation with DG HOME, my services are working on a legislative proposal to make cross-border access to electronic evidence more efficient and to improve legal certainty, transparency and accountability in cross-border cooperation between authorities and service providers.
- We need to ensure the right balance between efficient law enforcement and respect for other States' territorial sovereignty and the protection of fundamental rights.

- We are also aware of the need to ensure that companies are not made subject to conflicting legal requirements that could put them in difficult situations and weaken criminal investigations.
- This being said, the MLA route continues to be essential. We also continue working on practical improvements to the implementation of the MLA, as agreed in the review of the agreement in 2016.

### **Microsoft Ireland Case**

- I would also like to inform you that we are currently considering whether to submit an 'amicus curiae' brief in the Microsoft case. The Council is being consulted on this possibility before the College takes a formal decision.

## DEFENSIVES

### MLA effectiveness

- Law enforcement and judicial authorities often consider the procedures for judicial cooperation for requesting electronic evidence as too slow, disproportionately cumbersome also in view of the limited interest of the receiving country, and thus inadequate. While a national request to service providers takes in general a few days at most, MLA requests to the U.S. as the main recipient take around 10 months on average and require a significant resources. In such cases, the evidence transmitted is often outdated or comes too late. For requests between Member States, the European Investigation Order provides for deadlines which in total amount to 120 days, which is faster than MLA, but still quite slow compared to direct cooperation.
- The practical measures to enhance cooperation between public authorities in the EU and in the US, in particular the training of EU practitioners and the sharing of guidelines and best practices, would to some extent improve the quality of MLA requests submitted by EU authorities and would therefore both accelerate the treatment of these requests. That being said, even if there is room to improve the expediency of judicial cooperation through a set of non-legislative initiatives, these will not be sufficient to solve the problems our authorities are facing with electronic evidence.

**Article 48 GDPR prohibits direct data transfers (to the extent they are not based on international agreements) from EU service providers to judicial/law enforcement authorities from third countries.**

- This reasoning is based on erroneous interpretation of Article 48 GDPR. Article 48 is not a "blocking status" and does not subject transfer to the existence of an international agreement as a MLA.

- Art. 48 addresses the question of the recognition or enforceability of foreign decisions in the EU. It does not as such prohibit transfers.
- Rather it simply clarifies that data transfers in response to a request from a foreign court/law enforcement authority remain "transfers" within the meaning of the GDPR. As any transfers, such transfers must thus comply with the GDPR requirements (e.g. the data must be relevant for the purpose of the request, not excessive etc.) and be based on one of the grounds for transfer in Chapter V (see Articles 44-47 and 49 of GDPR). This is what "without prejudice" means in Art. 48 GDPR. Even in the absence of an international agreement, transfers are thus permissible, for instance, if they can be based on the "public interest", the "legal claims" or the "legitimate interests" derogations.

**Is the new EU data protection legal framework (GDPR and Police Directive) an obstacle for the normal functioning of the Internet Domain Name Service, in particular WHOIS databases?**

- As the European Commission, we have a clear interest in maintaining (and possibly improving) the functioning of the DNS and WHOIS database system. We recognise that it is currently used by a variety of stakeholders for different purposes, including for important public policy objectives (law enforcement, consumer protection, copyright protection, etc), and that it is a key tool for law enforcement in particular.
- We would like to stress that the GDPR does not change the main principles of the current data protection rules which exist for more than 20 years. Many of the most relevant principles and obligations (e.g. data retention regime, purpose limitation, proportionality principle, data accuracy and responsibility of the controller for the overall processing) are already applicable under the current legal framework. This is the message we have

consistently conveyed to all ICANN representatives (with whom we already had discussions several times).

- These principles are also not unique to the EU but are broadly recognised at international level (e.g. Council of Europe Convention 108, which is open to all countries and by now has some 50 Parties from almost all parts of the world, not including the US) and followed by a large (and increasing) number of countries around the world.
- We believe that it is time to calm the debate and are working to address misperceptions on the possible impact of the GDPR on the activities of ICANN, registries and registrars. I welcome the constructive and successful cooperation between the US and the EU on this at the ICANN 60 meeting.
- Let me emphasise that in the COMs view the GDPR (like its predecessor, the Data Protection Directive and its implementation in national law) provides for the necessary tools in terms of legal basis (e.g. performance of a contract and legitimate interest), rules on further processing etc., for operating a system such as WHOIS and allowing legitimate uses.
- The Commission maintains regular and cooperative contacts with ICANN and other relevant stakeholders on these issues. Several encounters at different level have taken place, including the participation of COM representatives at the ICANN 59 and 60 meetings with the main objective of helping to find workable solutions for all parties involved.
- We are fully convinced that the way forward involves a process that requires preparation of a proper legal and technical analysis and then thinking about solutions to possible challenges (including by looking for existing best practices). These should then be discussed with the Data Protection Authorities (DPAs) (which have since 2003 provided regular advice on a number of occasions and consistently expressed their readiness to engage).
- The Commission welcomes that ICANN has finally taken the step to commission such legal advice. When

completed, it will become clearer whether there is any need for adapting WHOIS, and if so how a workable solution could look like

- Let me stress that all of this should be "normal" procedure and is not different from dealing with any other regulatory framework that ICANN, the registrars and registries need to work in.

## BACKGROUND

### EU-US Dialogue on e-evidence

e-Evidence was included in the agenda of the EU-US HA ministerial meeting in November 2017. In summary, the EU presented the state of play of the future legislative proposal, including the good cooperation with the US on this matter, outlining the key ideas of the upcoming proposal, as well as the need to implement MLA review recommendations. The EU informed of the consideration that the College of Commissioners will give to a possible amicus curiae intervention in the Microsoft case in front of the Supreme Court. The US also confirmed the good cooperation with EU and asked the EU for a public statement on the interpretation of art. 48 GDPR. The DoJ was "cautiously optimistic" with regard to the Supreme Court decision. The resources allocated to MLA work have shown results, with the backlog being reduced. The DHS informed that they doubled the resources on cybercrime and are monitoring the Dark net 24/7. AG Sessions expressed its deep concern with regard to the impact of GDPR on the ICANN WHOIS database of owners of domain names and with regard to encryption. Commissioner King considered that GDPR would not constitute an obstacle to law enforcement access to such information, while DG Astola reiterated the Commission position on art. 48 GDPR (i.e. it does prohibit as such transfers on the basis of a court warrant) and explained that work was ongoing with ICANN to identify possible problems and solve them. The US outlined their strategy on combatting cyber threats from state and non-state actors.

### US developments

#### Microsoft case

The U.S. Supreme Court announced on 16 October that it will hear arguments in United States v. Microsoft.

The case originated in December 2013 when the Justice Department obtained a warrant in the Southern District of New York for emails of an as-yet-unnamed person based on probable cause that the account was being used in narcotics trafficking. Microsoft agreed to provide non-content information about the account. The company however refused to turn over the actual content of the emails, (stored in a data centre in Ireland) citing "impermissible extraterritorial application" of the Stored Communications Act and thereby advising the DoJ to use the MLAT process to get the content of the emails.

A magistrate judge rejected Microsoft's "motion to vacate" (refusal to provide the content) in April 2014. Microsoft appealed to the District Court for the Southern District of New York, which also disagreed with Microsoft, who then lodged an appeal with the U.S. Court of Appeals. The **U.S. Court of Appeals for the Second Circuit eventually agreed with Microsoft on 14 July 2016**, triggering a petition by the DoJ for an *en banc rehearing* that was turned down by a 4-4 Second Circuit vote on 24 January 2017.

The US Government then turned to the Supreme Court, possibly encouraged by the fact that in similar cases, Courts outside the 2<sup>nd</sup> Circuit's jurisdiction have ordered companies to comply with warrants if they can access the data from within the United States, regardless of where the data is stored.

In petitioning for a Supreme Court review of the case, the U.S. Government asserted that the Second Circuit decision was causing “immediate, grave, and ongoing harm to public safety, national security, and the enforcement of (our) laws.” In opposing the Supreme Court review, Microsoft said that in addition to the extraterritoriality issue, that a ruling in favour of the Justice Department would “adversely affect U.S. technology companies” by putting them in “the untenable position of being forced to violate foreign privacy laws to comply with U.S. warrants.” Microsoft also believed that the dispute should be settled by Congress, which could indeed be encouraged to take a closer look at legislation (such as the International Communications Privacy Act <https://www.congress.gov/bill/115th-congress/house-bill/3718/text> or the legislation allowing for the signature of the "US/UK agreement").

The Supreme Court decision will be issued before the end of its annual term in June/July 2018.

Various European stakeholders will likely file amicus briefs to the Court to express their interests in the outcome of the case. Amicus briefs are due on 7 December (for briefs supporting neither party), or 9 January (for briefs supporting Microsoft’s position).

Microsoft has underlined that this has a lot of bearing on our mutual objectives to clarify the rules regarding cross-border access to digital evidence. If the US government wins the case, the chance of an EU-US agreement on e-evidence would decrease. COM is therefore encouraged to intervene.

### **Google case**

On 3 February 2017, a federal magistrate judge ordered Google to comply with a search warrant to produce foreign-stored e-mails. The judge disagrees with the Second Circuit’s Microsoft judgement, arguing that “the conduct relevant to the Stored Communications Act’s focus will occur in the United States” even for the data that is retrieved from outside the United States.

### **Consequences of these cases**

Most US ISPs base themselves on the Microsoft judgement when refusing to deliver content data located abroad. The recent Google judgement (by a district court, therefore likely to be appealed) took place in a different "circuit" (namely, the third circuit, while the Microsoft case was judged in the second circuit). It is possible, under the US system, that different "circuits" (13 of them) have different case-law and apply different rules (until the Supreme Court possibly delivers a judgement ensuring consistent interpretation on the whole US territory).

To solve the conflicting Microsoft and Google case law on access to data held by US providers of wire or electronic communications service or remote computing service, the DoJ is pursuing two parallel channels:

a) On 24 May 2017, the DoJ presented a legislative proposal modifying several US Acts including ECPA<sup>1</sup> and stated that the proposal aims to:

---

<sup>1</sup> The draft proposal, sent to the Congress by the former administration one year ago, was resubmitted in a slightly modified version on 24 May 2017 by the Department of Justice to the Committee on the Judiciary of the Congress. The current proposal also amends the Omnibus Crime Control and Safe Streets Act (Wiretap Act) and the Stored Communications Act

(1) clarify that US law enforcement authorities can obtain electronic data under a provider's custody or control, even if stored abroad;

(2) provide authority to enter into international agreements with third states to access, on a reciprocal basis, electronic data held by providers in the other state.

It seems that this proposal has not yet been formally submitted to Congress.

b) On 23 June 2017, the DoJ filed a petition asking the Supreme Court to review the lower court's opinion in the Microsoft case. The DoJ referred the following question to the Supreme Court: "Whether a United States provider of email services must comply with a probable-cause-based warrant issued under 18 U.S.C. 2703 by making disclosure in the United States of electronic communications within that provider's control, even if the provider has decided to store that material abroad". The Supreme Court will decide whether they will take up the *Microsoft* case early October. If they do, a judgment can be expected by May 2018.

On 1 August 2017 Senators Orrin Hatch, Chris Coons and Dean Heller reintroduced the International Communications Privacy Act (ICPA), which would create a legal framework for U.S. law enforcement to obtain electronic communications data of U.S. citizens, even when this information is stored overseas. The bill would require the use of a warrant for such inquiries. It would establish a standard for officials to access the data of foreign nationals in certain cases, - that is the foreign government of qualifying third countries would have to be notified of a request by US authorities to obtain data of that foreign state's national, who is located outside the US, and could raise objections. The objection could be overruled by the US judge if he/she determines that the interests of the US in obtaining information outweigh the interests of the qualifying foreign government in preventing the disclosure (so-called "comity analysis").

#### **UK-US agreement on direct access to service providers**

Negotiations are still ongoing between UK and US on an agreement on direct cooperation of law enforcement authorities with service providers in the other country to obtain electronic evidence (NB: UK is not a party to the EU-US MLAT). At least as long as the Microsoft judgement remains, the US-UK agreement cannot advance, because the US cannot ask ISPs to deliver data located in the UK (because of the Microsoft case). The Commission should ensure that this agreement and any other future bilateral agreements are fully compatible with the existing EU acquis, in particular the Data Protection Police Directive, applicable from 2018 onwards and the so called "Umbrella Agreement" signed by EU and US in 2016, which put in place a comprehensive high-level data protection framework for criminal law enforcement cooperation between EU and US. It is expected that Senator Graham will introduce the legislation allowing for the conclusion of such US-UK Agreement, possibly with an alternative proposal to address the Microsoft case, which may be inspired by the DoJ proposal.

The possibility of an EU-US agreement instead of bilateral agreements with

---

("SCA").

Member States has been flagged to the US, e.g. at the last EU-US Ministerial, but at a recent videoconference with the Commission services, they stated that they found it premature to discuss this issue, preferring to await how the US-UK Agreement would work in practice.

## ARTICLE 48 GDPR

Text of the article (emphasis added):

"Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter."

Text of the corresponding recital 115 (emphasis added):

"Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject."

Following a proposal from the U.S. Administration, the U.S. Congress is currently debating an amendment of the Stored Communications Act. The intention of the Department of Justice is to clarify in the text of the law that this Act allows U.S. law enforcement authorities to obtain a warrant against U.S. service providers to hand over ("produce") data, even where such data are not stored in the U.S. but the U.S. service provider has access to these data abroad (e.g. because it is held by a subsidiary in a third country). This is a reaction to the judgement of the U.S. Court of Appeals for the Second Circuit that rejected the interpretation of the Stored Communications Act defended by the DOJ (which would have given an "extraterritorial effect" to that Act). In parallel, the U.S. government has further appealed that judgment to the U.S. Supreme Court (which has decided to take the case).

In the legislative debate, Microsoft (which was called to testify in Congress) has called attention to the fact that the change in law would expose service providers to conflicts of law. In this context, it has referred to Article 48 GDPR to demonstrate the possibility of such a conflict by claiming that the GDPR does not allow service providers to hand over personal data in response to a

U.S. warrant in the absence of an international agreement. In its contacts with Microsoft (John Franck), the Commission (DG Justice) has rejected that claim by pointing out that Article 48 GDPR merely refers back to the existing tools for international data transfers. In reaction to Microsoft's claims, the DoJ has asked the Commission to clarify – through a public statement – that Microsoft's interpretation is incorrect. Both Microsoft and the DoJ have asked the Commission to intervene in their support in the Supreme Court case

## **ICANN & Whois**

As the "guardian" of the Domain Name System, ICANN is a very important player, even though its work focusses on very specific and technical aspects, regarding the Domain Name System. It is a private not-for-profit organisation located in the US. It coordinates different policies concerning Domain Names System. Among others, it coordinates policy on WHOIS database. Different companies involved in the sale of Domain Names define more in details their privacy policies based on general policy defined by ICANN.

WHOIS data relates to those who have registered a domain name and it contains in particular information as to the name of the contact-point for the domain name, including phone number, e-mail address and other personal data. These data were originally made publicly available to give people who operate networks a way of contacting the person technically responsible for another network, another domain, when there was a problem.

The Article 29 Working Party has been already explaining its position in different opinions and letters on WHOIS data processing since 2003. However, no concrete actions have been taken by ICANN in reaction to this.

With the upcoming date of the application of the GDPR, different companies involved in the sale of domain names (registries and registrars) have increasingly raised concerns that they may risk being fined in case their WHOIS policies do not comply with the GDPR. Therefore, ICANN was asked by such companies to find a solution. ICANN approached the Commission to seek informal advice. We have had several meetings at different level in which we have tried to convey the idea that the GDPR does not imply substantial changes in data protection principles that have been already present in EU law for more than twenty years. ICANN and the rest of the stakeholders that are part of the DNS ecosystem (registrars, registries, etc.) need to carry out an analysis of the implications of their personal data processing activities and to put in place any relevant changes, if needed. While the Commission can play a facilitator role, it is ultimately for the national data protection authorities and the Article 29 Working Party to issue guidance on these issues.

The discussion on ICANN and GDPR is further complicated as different actors, such as the Council of Europe and US administrations are trying to engage in the discussion on WHOIS. This creates a lot of misunderstanding and misinterpretations.

ICANN organises 3 meetings a year to discuss different ongoing issues with all its stakeholders. During the meeting which took place in Johannesburg in June 2017, a representative of DG HOME (in cooperation with DG JUST, participating remotely)

explained to the basic principles of the GDPR, stressing that this new legislation is an evolution, and not a revolution. Moreover, a DG JUST representative participated remotely in the ICANN meeting that recently took place in Abu Dhabi

ANNEX

CVS





**COMMISSIONER VĚRA JOUROVÁ**

**MEETING WITH MR. KENT WALKER  
SENIOR VICE PRESIDENT AND GENERAL COUNSEL GOOGLE**

**LOCATION: BERL 12/176**

**DATE AND TIME: 17/11/2017, 9:00**

**MEETING OBJECTIVE: EXCHANGE VIEWS ON PRIVACY, HATE SPEECH AND E-EVIDENCE**

**MEMBER RESPONSIBLE: KEVIN O'CONNELL / DANIEL BRAUN**

**DG CONTACT & TEL NO:**



**ACTING DIRECTOR:**



VERSION: 07/11/2018 12:05,

JUST/123

PARTICIPANTS:

Deleted: 11/09/2018 18:43

## TABLE OF CONTENTS

STEERING BRIEF .....	3
TOPICS .....	4
PRIVACY SHIELD AND SURVEILLANCE REFORM .....	4
GDPR PREPARATIONS FOR 25 MAY 2018 .....	8
ONLINE PLATFORMS AND ILLEGAL CONTENT .....	11
LAW ENFORCEMENT ACCESS TO DATA .....	17
ANNEXES .....	24

## STEERING BRIEF

### SCENE SETTER/OBJECTIVES

Google's VP and General Counsel Kent Walker is responsible for managing Google's global legal and policy teams. He has requested a meeting with you, to follow-up your visit to Google's Headquarters in Silicon Valley in September.

He will raise the Commission's recent communication on **online platforms**, as well as **law enforcement access to data (e- evidence)**.

You should also use the meeting to urge Google to support the **Privacy Shield** by advocating reform of section 702 FISA and the appointment of the Ombudsperson, as well as to reiterate your suggestion that Google should help raise awareness of citizens about their **GDPR** rights.

You met Google representatives during your visit to the Silicon Valley in September. The discussion concerned in particular the Privacy Shield and the electronic evidence topics. Extract of the report:

"Meeting with Google (Privacy, law enforcement and EU affairs teams)

Google referred to its Privacy Shield certification process, which is linked to internal audits of its products and services. In parallel, work on GDPR compliance is ongoing, including Privacy training for all staff. VJ asked Google to help inform citizens about their new data protection rights and they agreed to explore such cooperation. She further proposed an event in May 2019 to take stock of the first year of application. [...]

On electronic evidence, Google explained its cooperation with law enforcement and its transparency reporting in this regard. Google supported the work on e-evidence in the EU and reform of the Stored Communications Act in the U.S. Google supports jurisdiction based on nationality/residence of the individual rather than location of the data and calls for an international arrangement to avoid a conflict of laws. Google supports the UK-U.S. agreement on cross-border warrants. As regards the Microsoft and Google cases on 'extraterritorial warrants' (which may go to the Supreme Court) Google considered that a legislative solution is necessary."

## TOPICS

### PRIVACY SHIELD AND SURVEILLANCE REFORM

#### CONTEXT

Google is a supporter of the Privacy Shield. Google and six of its "covered entities" are certified under the Privacy Shield program.

As to the **surveillance reform in the U.S.**, a debate is currently ongoing in Congress on the re-authorisation of Section 702 of the Foreign Intelligence Surveillance Act (FISA). Various Bills have been proposed so far. None of them would enlarge U.S. national security agencies' surveillance powers. The House version of the Bill would include some additional safeguards for foreigners.

In its Privacy Shield review Report, the Commission recommends that the U.S. Congress take the opportunity of the re-authorisation of Section 702 FISA to enshrine in FISA the protections offered by PPD-28 to non-U.S. persons, to ensure the stability and continuity of these protections.

#### OBJECTIVE(S)

Inform about the Commission Report on the first annual review of the functioning of the Privacy Shield, adopted on 18 October.

Stress the EU's interest in further reforms of U.S. surveillance laws with a view to strengthening the privacy protections for non-U.S. persons, and in particular in the ongoing debate in Congress on the re-authorisation of Section 702 of the Foreign Intelligence Surveillance Act (FISA).

Invite Google to support the sustainability of the framework, in particular, by arguing in favour of:

- a reform of section 702 FISA (currently discussed in Congress) which would incorporate the protections of PPD 28 for non-U.S. persons, and
- functioning oversight institutions, starting with the swift appointment of a permanent Ombudsperson in the State Department and the missing members of the Privacy and Civil Liberties Oversight Board (PCLOB).

#### LINE TO TAKE

- Since the program's inception (on 1 August 2016), more than 2,500 companies have joined the Privacy Shield.
- The participation of companies like Google, IBM, Microsoft, Facebook, but also that of many small and medium sized enterprises, confirms the (commercial) interest in the program, which facilitates transfers and reduces costs. At the same time the Privacy Shield ensures that the level of protection of the personal data transferred to U.S. companies certified with the Privacy Shield remains essentially equivalent to the one guaranteed within the EU.

- I note that Google took two important actions to increase trust with their European customers:
  - I welcome the fact that Google files transparency reports on the amount of requests by intelligence agencies to access user data. This helps to confirm that requests are kept within the limits of what is necessary and proportionate;
  - I also welcome the fact that Google chose to elect EU data protection authorities as their dispute resolution mechanism to deal with individual complaints with regard to non-human resources data processing. Submitting to such oversight can be a competitive advantage because European customers will feel more comfortable in handing over their data when they know they can turn to their "regular" authorities in case of complaints.
- The Commission adopted on 18 October its "Report on the first annual review of the functioning of the Privacy Shield".
- In its Report, the Commission concludes that the United States continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield, but also formulates a number of recommendations on how to improve the practical implementation of the data protection safeguards in the Privacy Shield.
- Swift appointment of the Ombudsperson, of the missing members of the PCLOB, as well as incorporation of the PPD-28 protections in FISA in the context of the re-authorisation of Section 702 FISA, are among the recommendations made by the Commission in its Report. The Commission is currently monitoring the follow up that the U.S. is giving to these and the other recommendations in the Report.
- As a major U.S. IT company, I invite you to support the sustainability of the framework by arguing in favour of a swift implementation of the recommendations in the Commission Report with the US authorities.
- 

## BACKGROUND

The Privacy Shield is up and running since 1 August 2016.

The Privacy Shield provides for a review to be conducted on an annual basis. The purpose of the review is to carefully assess the proper functioning, implementation, supervision and enforcement of the Privacy Shield framework. This concerns all aspects of the framework: both compliance by companies and by U.S. authorities, including in the field of national security access to data.

The first annual review took place on 18-19 September, in Washington, DC.

On 18 October, the Commission adopted and made public a Report to the European Parliament and Council on the first annual review of the functioning of the EU-U.S. Privacy Shield.

On 6 November, the Commission presented the Report to the EP LIBE

Committee. It will be presented to Member States in the near future.

On 28-29 November the Article 29 Working Party will discuss and adopt their own report on the annual review. They are expected to broadly concur with the Commission's recommendations, though using more critical language on surveillance and the Ombudsperson (and its degree of independence).

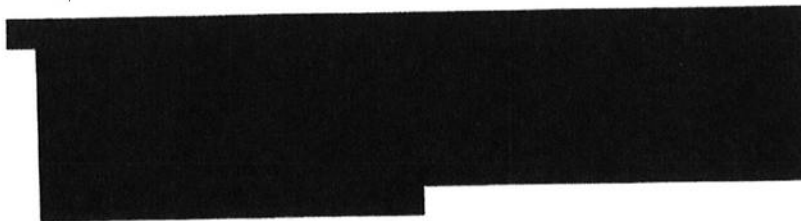
#### DEFENSIVES



##### *What about the two actions for annulment brought against the Privacy Shield?*

- Two actions for annulment of the Privacy Shield decision (one brought by Digital Rights Ireland and one by La Quadrature du Net) have been lodged with the General Court. While we cannot of course predict the outcome – like in any other case before the Court – we are confident that the decision will withstand judicial scrutiny. We strongly believe that the decision is lawful and in particular fulfils the requirements stipulated by the Court in the *Schrems* ruling. Would that be otherwise, the Commission would not have adopted the decision in the first place. Neither would we have received overwhelming support from the Member States.
- This being said, the commitments made under the Privacy Shield are not the only thing that matters. It will also be important that the U.S. honours its commitments in practice and fully implements the framework. This is yet another reason why the Annual Review was so important: it allowed us to check this and have a dialogue with our U.S. counterparts on all aspects of the Privacy Shield.

##### *How do you see the so-called Schrems II case? (i.e. the referral that the Irish High Court (on 3 October) decided to make to the CJEU to determine the legal status of data transfers to the U.S. under the Commission-approved "Standard Contractual Clauses", Commission decision 2010/87/EU)*

- To be clear, the Irish case concerns a different data transfer tool, namely so-called Standard Contractual Clauses laid down in Commission decision 2010/87/EU.
- The Irish High Court decided, on 3 October, to refer questions to the CJEU to ascertain whether the alleged absence of effective remedies in the U.S. in case of access by U.S. state agencies to personal data sent there on the basis of the Commission-approved standard contractual clauses violates European fundamental rights (namely the rights to privacy, to the protection of personal data, and the right to an effective remedy and to a fair trial under, respectively, Articles 7, 8 and 47 of the Charter of Fundamental Rights of the EU).



- 
- As the case is very much focused on the question of individual redress for Europeans when their data is transferred to the U.S., it is worth noting that the Ombudsperson mechanism provides an important avenue in this respect (but we must be able to demonstrate that the Ombudsperson has the necessary independence and powers to address complaints).
- 

## **GDPR PREPARATIONS FOR 25 MAY 2018**

### **CONTEXT**

The meeting is an opportunity to inform Google Senior Vice-President about the work that the Commission is undertaking vis-à-vis the Member States, the Article 29 Working Party and the stakeholders in the transition period towards implementation of the GDPR on 25 May 2018.

There are currently two preliminary rulings (C-136/17; C-507/17) before the Court of Justice of the EU involving processing of personal data by Google: the first pertaining to requests for erasure (right to be forgotten) for sensitive data (e.g. political views; religious beliefs) and the legal basis for Google to process such data and the second one regarding the "coverage" – global or limited to the EU – of the right to be forgotten. These two cases should not be discussed at the meeting as the examination of the cases is on-going.

### **OBJECTIVE**

Explain the work done during the transition period to prepare for GDPR application on 25 May 2018. Urge Google to join this effort by informing its users about the rights they benefit from under the GDPR.

### **LINE TO TAKE**

- The New European Union data protection regulation – the General Data Protection Regulation (GDPR), will be applicable from 25 May 2018. The new legislation modifies and updates data protection rules at EU level to make Europe fit for the digital age.
- The Commission is working closely with Member States to accompany them in the process of adapting or repealing their existing laws as necessary. Measures taken at national level must not lead to any new fragmentation.
- The Commission is also supporting the work of the Data Protection Authorities who have a key role in ensuring coherent interpretation and enforcement of the new rules.
- The Article 29 Working Party has already issued four guidelines to assist with implementation and interpretation of new legislation: on data portability, data protection officers, lead supervisory authority, and data protection impact assessments. The Article 29 Working Party plans to adopt further guidelines this year and at the beginning of 2018. For instance, guidelines on data breach notifications and profiling are subject to public consultation until 28 November 2017. Businesses are strongly encouraged to take advantage from the current consultation and provide their views.
- The Commission is reaching out to stakeholders, for instance through the organisation of targeted GDPR events (e.g. on health on 23 October and on SMEs in November). We have also set up a multi-stakeholder group on GDPR to get the views of businesses and civil society (first meeting on 19 October).
- As announced in the letter of intent following President Juncker's State of the

Union speech, the Commission will provide guidance to businesses, especially SMEs, and individuals so as to raise their understanding of the new rules in view of their application as of May 2018. This guidance would take the form of a practical online toolkit. We plan to have it ready by the data protection day on 28 January. It will likely also entail a chapeau communication presenting the Commission's action to ensure a proper application of the new data protection rules.

- As discussed with your colleagues when I came to Silicon Valley I also count on companies like Google to inform users about the rights they will benefit from thanks to the GDPR. I see you as a partner in raising awareness of the GDPR.

#### **DEFENSIVES**

*What is the Commission position on the guidelines recently published by the Article 29 Working Party?*

- The guidelines of the Article 29 Working Party are very important to provide increased legal certainty to stakeholders since they will guide the data protection authorities when implementing the GDPR.
- The Commission supports the work of the Article 29 Working Party and share with its members its views and expertise on the provisions of the GDPR. It also strongly encouraged the Working party to conduct public consultation on the draft guidelines.
- However, the Article 29 Working Party (and after May 2018 the European Data Protection Board) is an independent body and therefore the content of the guidelines is their responsibility.

*Aren't the sanctions foreseen in the GDPR too high? 4% of annual turnover of a company is disproportionate.*

- The GDPR establishes a range of enforcement tools, including penalties and fines. All these tools must be effective, proportionate and dissuasive. The agreement on fines ensures that they are a deterrent. Each case must be determined by taking into account the relevant circumstances of the infringement:
  - gravity/ duration of the violation;
  - number of data subjects affected and level of damage suffered by them;
  - intentional character of the infringement;
  - any actions taken to mitigate the damage;
  - degree of co-operation with the supervisory authority.
- The GDPR sets out two main categories of ceilings of fines for infringements of the Regulation, depending on the gravity of the infringements.
- The first ceiling of fines is up to a maximum of EUR 10 million or in case of

an undertaking up to 2% of worldwide turnover. An example would be an infringement of the obligations of the controllers to conduct impact assessments.

- The higher ceiling of fines is up to a maximum of EUR 20 million or 4% of worldwide turnover. An example would be an infringement of the data subjects' rights under the Regulation. This depends on the circumstances of each individual case.



## ONLINE PLATFORMS AND ILLEGAL CONTENT

### CONTEXT

On 28 September, the Commission unveiled guidance on how to tackle the spreading of material such as incitement to terrorism, illegal hate speech or child sexual abuse material online. Such material is already illegal under EU law, both online and offline, and the new guidance calls on online platforms to further step up their efforts to prevent the spread of this type of illegal content. This guidance will complement and reinforce the ongoing sector-specific dialogues including the Code of Countering Illegal Hate Speech.

With these policies, the Commission expects that illegal content will be removed faster while duly respecting and promoting freedom of expression and public insight in how online platforms assesses notifications of alleged illegal content.

On the basis of progress in implementing these guidelines, the Commission will prepare an Impact Assessment, and determine if further legislative measures are needed in the first half of 2018

The dialogue on countering illegal online hate speech and the Code of Conduct is the only forum where the Commission is presently monitoring in detail the take down rate/time in respect of notices as well as the feedback provided to trusted flaggers and normal users respectively. It follows that it should be expected to provide a major contribution to the Commission's assessment of the progress of implementation of the guidance.

### OBJECTIVE(S)

Ensure the continued support for the work under the Code of Conduct by Google (YouTube),

#### LINE TO TAKE

- Our aim is to ensure that the internet remains a place of free and democratic expression, where European laws are respected. We have to fight against the proliferation of incitement to violence and hatred online, as this fuels fears, and reduces the space for open democratic exchanges.
- A recent (November 2016) European survey showed that 75% of those that follow or participate to debates online has come across episodes of abuse, threat or hate speech against journalists, bloggers or people active on the web. For almost half of them, the consequence was to inhibit engagement in online discussions.
- This reinforces the need to ensure that manifestly illegal content, such as illegal hate speech, is removed from social media, while fully upholding the principle of freedom of expression.
- We are happy that YouTube, Twitter, Facebook and Microsoft share this view.
- By agreeing to the Code of conduct on countering illegal hate speech your companies committed to review and assess most of the notifications of illegal hate speech in less than 24 hours, not only against your own terms and conditions, but also, when necessary, against national laws implementing EU law.
- As you know, one year after its adoption, our monitoring exercise showed that the Code of Conduct has delivered some important progress
- This shows that that self-regulatory measures have proven their effectiveness. What we have managed to achieve in the short period since the adoption of the Code of conduct goes beyond the commitments in the text. Our Dialogue with stakeholders has created a sustainable collaborative process, between all the actors concerned. We are now all firmly grounding our work around the principle that content that is considered as illegal hate speech in the real world, it is also to be recognised and treated as such in the online world. The determination of the IT Platforms including YouTube has been key to the success and I hope that I can count on your continued support in the months to come!
- The Code of Conduct has now reached a maturity and credibility with industry as a whole. The next important steps will be to stabilise and consolidate the results and ensure uptake by a wider group of IT platforms.
- I am confident that Google + will join the companies which committed to the Code. As you might know, we are discussing with several IT platforms on this matter and a meeting is planned end November in Dublin with potential new platforms that may be interested in working with us, including yours.

- As you know, the Commission unveiled guidance on how to tackle the spreading of material such as incitement to terrorism, illegal hate speech or child sexual abuse material online on 28 September this year.
- On the basis of progress in implementing these guidelines, the Commission will prepare an Impact Assessment, and determine if further legislative measures are needed in the first half of 2018.
- As concerns the need to codify a notice and action procedure and the duty of IT platforms to take action once they have knowledge of the illegal content we need to evaluate the progress made in the coming months to see if guidance's and self-regulatory measures would suffice or if we need to go for law.
- As you know, we will keep monitoring of the code of conduct. We hope to see improved results, including in terms of feedback to users and we hope to see the companies reflect on how they can improve transparency in how they apply their content management policies,
- We count on YouTube to continue to show leadership on this important file and on Google more broadly to commit on the way ahead.

**Deleted:** have set out to carry out a third

**Deleted:** so that we can deliver results to this process by January

## BACKGROUND

### Code of Conduct on tackling illegal hate speech

On the 31 May 2016, the Commission presented together with Facebook, Microsoft, Twitter and YouTube a "Code of conduct on countering illegal hate speech online". The main commitments are:

- a) The IT Companies to have in place clear and effective processes to review notifications regarding illegal hate speech on their services so they can remove or disable access to such content. The IT Companies to have in place Rules or Community Guidelines clarifying that they prohibit the promotion of incitement to violence and hateful conduct.
- b) Upon receipt of a valid removal notification, the IT Companies to review such requests against their rules and community guidelines and, where necessary, national laws transposing the Framework Decision 2008/913/JHA, with dedicated teams reviewing requests.
- c) The IT Companies to review the majority of valid notifications for removal of illegal hate speech in less than 24 hours and remove or disable access to such content, if necessary.

The IT Companies and the European Commission agreed to assess the public commitments in the Code of conduct on a regular basis, including their impact.

On 7 December 2016, in the context of the High Level Group on combatting Racism, Xenophobia, and other forms of intolerance, the Commission presented the preliminary results of a first monitoring exercise testing the response by IT Companies to notifications on alleged illegal hate speech received by 12 civil

society organisations in 9 Member States.

The assessment showed that IT companies are making an effort but continued work is needed to ensure that notifications are reviewed within the time frame set out by the Code of conduct, regardless if they come from trusted flaggers or from normal users and irrespective of the organisation or country that the notification originates from.

The 2nd exercise was carried out for a period of 7 weeks, from 20 March to 5 May 2017, using the same methodology as the 1st monitoring exercise in October-November 2016.

31 organisations and 3 public bodies (France, Romania and Spain) reported a total sample of 2575 notifications from all the Member States except for Finland, Sweden, Bulgaria and Luxembourg.

Notifications on hate speech deemed illegal led to the deletion of the content in 59,1% of the cases. All the 3 IT Companies reported improvements on the rates of removal as compared to the first monitoring, with Facebook increasing takedown rates from around 28% to 67%, YouTube from around 48% to 66% and Twitter progressing from around 19% to 37%.

Overall on the time of assessment, IT Companies assessed notifications in less than 24 hours in 51,4% of cases, in less than 48h in 20,7%, in less than a week in 14,7% and in 13,2% it took more than a week.

Concerning the coherence of treatment irrespective of the reporting channels, out of the total notifications, 71,1% of cases were submitted through the channels available to general users, while 28,9% of the cases were notified through the tools available only to trusted flaggers/reporters. Breaking down the removals by reporting channel, in 56,5% notifications made using channels available to general users lead to the removal of the notified content, while a higher removal rate of 65,6% was recorded for cases notified using the trusted flaggers/reporters channel.

Compared to the 1st monitoring exercise, the removal rates between the two reporting channels are converging, narrowing the gap in difference of treatment depending on the source of notification (trusted flaggers/general users). The removal for Facebook for normal users is 64,2% while for trusted flaggers is 72,6%. The corresponding figures for YouTube are 63,2% for normal users and 74% for trusted flaggers and Twitter 31,5% for normal users and 48,5% for trusted flaggers.

The monitoring exercise also examined the level of transparency and the feedback that the IT companies provided to users and trusted flaggers in response to notifications. Data shows a large disparity between IT Companies when giving feedback to notifications made. While Facebook sent feedback in 93,7% of the cases, Twitter did so in only 32,8% and YouTube in 20,7% of the cases.

Next steps will focus on working with the IT companies to stabilise and consolidate the results and on to encouraging the uptake of the code of conduct

also by other IT platforms

The dialogue on countering illegal online hate speech and the Code of Conduct is the only forum thus far where the Commission is presently monitoring in detail the take down rate/time in respect of notices as well as the feedback provided to trusted flaggers and normal users respectively. It follows that it should be expected to provide a major contribution to the Commission's assessment of the progress of implementation of the guidance in the Communication on online Platforms.

#### **Communication on online Platforms of 28 September 2017**

Online platforms need to exercise a greater responsibility in content governance. The Communication proposes common tools to swiftly and proactively detect, remove and prevent the reappearance of content online:

- Detection and notification: Online platforms should cooperate more closely with competent national authorities, by appointing points of contact to ensure they can be contacted rapidly to remove illegal content
- Effective removal: Illegal content should be removed as fast as possible, and can be subject to specific timeframes, where serious harm is at stake, for instance in cases of incitement to terrorist acts;
- Prevention of reappearance: Platforms should take measures to dissuade users from repeatedly uploading illegal content. The Commission strongly encourages the further use and development of automatic tools to prevent the reappearance of previously removed content.

The Commission considers that online intermediaries can put in place proactive measures without fearing to lose the liability exemption under the e-Commerce Directive

#### **Defensives**

**The Commission keeps threatening with legislation despite progress made in the context of the code of conduct. In the light of the Communication on illegal content, what is the incentives of companies to continue working on self regulatory measures and collaborate in under the Code of Conduct**

- The Platform guidance to a large extent repeats commitments from the code of conduct. For this means that you have already taken significant steps to live up to the steps that the Commission expects you to take.
- The assessment of how the effectiveness of the Code of Conduct will of course be an important factor to take into account before the Commission decides on the need to legislate.
- It is true that there is a possibility that the Commission will move for legislation on notice of action but by the same token the steps that the Platforms would have taken in order to comply with the code or with the illegal content communication will of course not be wasted. On the contrary it will put them in a position where they will have to make much smaller adjustments to comply with the law since they have already

implemented the measures voluntarily

[REDACTED]

## LAW ENFORCEMENT ACCESS TO DATA

### CONTEXT

Google has acknowledged the need for better and faster ways to collect cross-border evidence that appropriately balance the various interests at stake (privacy rights of users, and the obligations of governments to investigate crimes). <https://blog.google/topics/public-policy/international-framework-digital-evidence/>

In their opinion, sustainable solutions need to be based on two core principles: First, countries that honor baseline principles of privacy, human rights, and due process should be able to make direct requests to service providers for user data that pertains to serious crimes. Second, the United States and foreign governments should sign new agreements that could provide an alternative to the MLAT process. Accordingly, in technical meetings in which it has been involved (for example the Roundtable meeting on e-evidence on 19 June 2017) Google has sometimes expressed concerns about a binding EU production order that could put them in a conflict of law situation.

During your visit to Silicon Valley in September 2017, Google supported the work on e-evidence in the EU and reform of the Stored Communications Act in the U.S. Google supports jurisdiction based on nationality/residence of the individual rather than location of the data and called for an international arrangement to avoid a conflict of laws. As regards the Microsoft and Google cases on 'extraterritorial warrants' Google considered that a legislative solution is necessary.

### OBJECTIVE(S)

Stress COM's commitment to improving law enforcement access to electronic evidence, update on related developments and listen to the stakeholder's views.

### LINE TO TAKE

- On access to electronic evidence, let me briefly update you on developments as regards practical measures that the Commission, jointly led by DGs JUST and HOME, is pursuing, as well as on our plans for a legislative proposal.
- Measures to improve practical cooperation amongst judicial authorities in the EU are already being implemented on the basis of the Directive on the European Investigation Order.
- But more work is needed to improve practical cooperation with service providers. Meetings with stakeholders to make progress on these practical measures are foreseen in the coming weeks and throughout 2018.
- In parallel, we are developing legislative options to make cross-border access to electronic evidence more efficient and to improve legal certainty, transparency and accountability in direct cross-border cooperation between authorities and service providers. Quick access to electronic evidence is

crucial since it can be deleted at the click of a mouse.

- As announced in the Commission's 2018 Work Programme, a proposal to improve cross-border access of law enforcement authorities to electronic evidence is due to be adopted in the first quarter of 2018.
- With this in mind, we recently carried out a public consultation to collect the views of relevant stakeholders, including public authorities, judges and prosecutors. In parallel, we have also continued targeted discussions on the different scenarios with a variety of experts.
- The consultation with the Member States revealed there is no common approach to obtain cross-border access to digital evidence, each Member State maintains its own domestic practice. This diversity creates legal uncertainty for all the stakeholders involved and represents an obstacle to joint and cross border investigations.
- In parallel, voluntary cooperation between law enforcement and US service providers has developed as an alternative path to access e-evidence.
- We need to ensure the right balance between security and efficient law enforcement and prosecution of crimes, on the one hand, and the respect of other States' territorial sovereignty and the protection of fundamental rights, including the protection of individual rights in criminal proceedings and the rights to privacy and personal data protection, on the other hand.
- We are also aware of the need to ensure that companies are not made subject to conflicting legal regimes that could put them in difficult situations and weaken criminal investigations.
- Last but not least, we should ensure consistency and coherence with other ongoing instruments. We are following the progress of the Council of Europe's Cybercrime Convention Committee (T-CY)'s work on an additional protocol, and also keeping a close eye on developments in the U.S.
- As the internet is borderless, options for legislative measures within the EU could be complemented by agreements with key partner countries or through expanding multilateral treaties, in particular the Council of Europe Budapest Convention on Cybercrime.

## BACKGROUND

The 9 June 2016 JHA Council conclusions on Improving criminal justice in cyberspace call on the Commission to inter alia:

- Develop a framework for the effective cooperation of law enforcement authorities with the private sector to obtain specific categories of electronic evidence;
- Improve the functioning of Mutual Legal Assistance procedures (including the European Investigation Order) for obtaining electronic evidence;
- Explore possibilities for a common EU approach on enforcement jurisdiction in cyberspace where existing frameworks are not sufficient, i.e. to explore other connecting factors than the location of data, and to explore investigative

measures that could be used on that basis;

- Since last year, the Commission has carried out a comprehensive expert consultation process which has allowed defining problems raised and possible solutions to address them. On 8 June 2017 at the Justice and Home Affairs Council the Commission presented a non-paper setting out the conclusions of this process, including an overview of possible practical and legislative measures to address the problems identified. On 4 August 2017 the Commission published an Inception Impact Assessment and launched a public consultation to collect views of relevant stakeholders.
- Possible legislative measures at EU level that are presented in the Inception Impact Assessment include:
  1. A legal framework authorising authorities to directly request or compel a service provider in another Member State to disclose e-evidence processed in the Union, including appropriate safeguards and conditions. This framework can leave to the discretion of the service provider a decision on whether to provide a response ("production request") or can obligate service providers to respond ("production order"). This could also be considered with respect to service providers located outside of the Union and/or data stored outside of the Union. This system could be complemented by an obligation for service providers established in third countries but offering services in the EU to designate a legal representative in the EU for the purpose of the cooperation on the basis of production requests/orders.
  2. A legal framework for law enforcement to access e-evidence pursuant to a set of safeguards and measures to mitigate cross-border effects, without cooperation of a service provider or the owner of the data, through a seized device or an information system. This could also be considered with respect to data whose storage place is not known or data which is stored outside of the Union.

As announced in the CWP 2018, a proposal to improve cross-border access of law enforcement authorities to electronic evidence is due to be adopted on 24 January 2018.

### **US developments**

#### **Microsoft case**

The U.S. Supreme Court announced on 16 October that it will hear arguments in *United States v. Microsoft*.

The case originated in December 2013 when the Justice Department obtained a warrant in the Southern District of New York for emails of an as-yet-unnamed person based on probable cause that the account was being used in narcotics trafficking. Microsoft agreed to provide non-content information about the account. The company however refused to turn over the actual content of the emails, (stored in a data centre in Ireland) citing "impermissible extraterritorial application" of the Stored Communications Act and thereby advising the DoJ to use the MLAT process to get the content of the emails.

A magistrate judge rejected Microsoft's "motion to vacate" (refusal to provide

the content) in April 2014. Microsoft appealed to the District Court for the Southern District of New York, which also disagreed with Microsoft, who then lodged an appeal with the U.S. Court of Appeals. The U.S. Court of Appeals for the Second Circuit eventually agreed with Microsoft on 14 July 2016, triggering a petition by the DoJ for an en banc rehearing that was turned down by a 4-4 Second Circuit vote on 24 January 2017.

The US Government then turned to the Supreme Court, possibly encouraged by the fact that in similar cases, Courts outside the 2nd Circuit's jurisdiction have ordered companies to comply with warrants if they can access the data from within the United States, regardless of where the data is stored.

In petitioning for a Supreme Court review of the case, the U.S. Government asserted that the Second Circuit decision was causing "immediate, grave, and ongoing harm to public safety, national security, and the enforcement of (our) laws." In opposing the Supreme Court review, Microsoft said that in addition to the extraterritoriality issue, that a ruling in favour of the Justice Department would "adversely affect U.S. technology companies" by putting them in "the untenable position of being forced to violate foreign privacy laws to comply with U.S. warrants." Microsoft also believed that the dispute should be settled by Congress, which could indeed be encouraged to take a closer look at legislation (such as the International Communications Privacy Act <https://www.congress.gov/bills/115/congress/house-bill/3718/text> or the legislation allowing for the signature of the "US/UK agreement")

The Supreme Court decision will be issued before the end of its annual term in June/July 2018.

Various European stakeholders will likely file amicus briefs to the Court to express their interests in the outcome of the case. Amicus briefs are due on 7 December (for briefs supporting neither party), or 9 January (for briefs supporting Microsoft's position).

Latest development: The Commission Legal Service intends to file an amicus curiae brief (supporting neither party). The objective would be to clarify in a neutral manner the impact of Article 48 of the GDPR (which is not a blocking statute but sets certain conditions on data transfers to third countries' judicial law enforcement authorities – see below) and other relevant considerations under EU and international law. The amicus curiae brief would also have to take into account our objective to clarify the rules regarding cross-border access to digital evidence (e-evidence proposal planned for January). The College will have to decide in the coming days to meet the 7 December deadline.

Microsoft argues that if the US government wins the case, the chance of an EU-US agreement on e-evidence would decrease.

#### **Google case**

On 3 February 2017, a federal magistrate judge ordered Google to comply with a search warrant to produce foreign-stored e-mails. The judge disagrees with the

Second Circuit's Microsoft judgement, arguing that "the conduct relevant to the Stored Communications Act's focus will occur in the United States" even for the data that is retrieved from outside the United States.

#### Consequences of these cases

Most US ISPs base themselves on the Microsoft judgement when refusing to deliver content data located abroad. The recent Google judgement (by a district court, therefore likely to be appealed) took place in a different "circuit" (namely, the third circuit, while the Microsoft case was judged in the second circuit). It is possible, under the US system, that different "circuits" (13 of them) have different case-law and apply different rules (until the Supreme Court possibly delivers a judgement ensuring consistent interpretation on the whole US territory).

To solve the conflicting Microsoft and Google case law on access to data held by US providers of wire or electronic communications service or remote computing service, the DoJ is pursuing two parallel channels:

a) On 24 May 2017, the DoJ presented a legislative proposal modifying several US Acts including ECPA and stated that the proposal aims to:

(1) clarify that US law enforcement authorities can obtain electronic data under a provider's custody or control, even if stored abroad;

(2) provide authority to enter into international agreements with third states to access, on a reciprocal basis, electronic data held by providers in the other state.

It seems that this proposal has not yet been formally submitted to Congress.

b) On 23 June 2017, the DoJ filed a petition asking the Supreme Court to review the lower court's opinion in the Microsoft case. The DoJ referred the following question to the Supreme Court: "Whether a United States provider of email services must comply with a probable-cause-based warrant issued under 18 U.S.C. 2703 by making disclosure in the United States of electronic communications within that provider's control, even if the provider has decided to store that material abroad". The Supreme Court will decide whether they will take up the Microsoft case early October. If they do, a judgment can be expected by May 2018.

On 1 August 2017 Senators Orrin Hatch, Chris Coons and Dean Heller reintroduced the International Communications Privacy Act (ICPA), which would create a legal framework for U.S. law enforcement to obtain electronic communications data of U.S. citizens, even when this information is stored overseas. The bill would require the use of a warrant for such inquiries. It would establish a standard for officials to access the data of foreign nationals in certain cases, - that is the foreign government of qualifying third countries would have to be notified of a request by US authorities to obtain data of that foreign state's national, who is located outside the US, and could raise objections. The objection could be overruled by the US judge if he/she determines that the interests of the US in obtaining information outweigh the interests of the qualifying foreign government in preventing the disclosure (so-called "comity analysis").

## Background on Article 48 GDPR

Text of the article:

"Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter."

Text of the corresponding recital 115:

"Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject."

Following a proposal from the U.S. Administration, the U.S. Congress is currently debating an amendment of the Stored Communications Act. The intention of the Department of Justice is to clarify in the text of the law that this Act allows U.S. law enforcement authorities to obtain a warrant against U.S. service providers to hand over ("produce") data, even where such data are not stored in the U.S. but the U.S. service provider has access to these data abroad (e.g. because it is held by a subsidiary in a third country). This is a reaction to the judgement of the U.S. Court of Appeals for the Second Circuit that rejected the interpretation of the Stored Communications Act defended by the DOJ (which would have given an "extraterritorial effect" to that Act). In parallel, the U.S. government has further appealed that judgment to the U.S. Supreme Court (which has decided to take the case).

In the legislative debate, Microsoft (which was called to testify in Congress) has called attention to the fact that the change in law would expose service providers to conflicts of law. In this context, it has referred to Article 48 GDPR to demonstrate the possibility of such a conflict by claiming that the GDPR does not allow service providers to hand over personal data in response to a U.S. warrant in the absence of an international agreement. In its contacts with Microsoft (John Franck), the Commission (DG Justice) has rejected that claim by pointing out that Article 48 GDPR merely refers back to the existing tools for international data transfers. In reaction to Microsoft's claims, the DoJ has asked the Commission to clarify – through a public statement – that Microsoft's interpretation is incorrect. Both Microsoft and the DoJ have asked the

Commission to intervene in their support in the Supreme Court case. The Commission is likely to intervene (in support of neither party) to clarify the meaning of Article 48 (see above).

#### DEFENSIVES

##### **A proposal including binding production orders can put service providers in a conflict of law situation**

[LTT: COM is aware of this concern and exploring ways to address it in the future proposal]

- The need to avoid creating new conflicts of laws has been raised repeatedly by service providers, civil society and some Member States during the consultations. We are looking into how to best achieve this, while preserving the efficiency of a Commission proposal.

•

##### **Article 48 GDPR prohibits direct data transfers (to the extent they are not based on international agreements) from EU service providers to judicial/law enforcement authorities from third countries.**

- This reasoning is based on erroneous interpretation of Article 48 GDPR. Article 48 is not a "blocking status" and does not subject transfer to the existence of an international agreement as a MLA.
- Article 48 addresses the question of the recognition or enforceability of foreign decisions in the EU. It does not as such prohibit transfers
- Rather it simply clarifies that data transfers in response to a request from a foreign court/law enforcement authority remain "transfers" within the meaning of the GDPR. As any transfers, such transfers must thus comply with the GDPR requirements (e.g. the data must be relevant for the purpose of the request, not excessive etc.) and be based on one of the grounds for transfer in Chapter V (see Articles 44-47 and 49 of GDPR). This is what "without prejudice" means in Art. 48 GDPR. Even in the absence of an international agreement, transfers are thus permissible, for instance, if they can be based on the "public interest", the "legal claims" or the "legitimate interests" derogations.

[REDACTED]

## ANNEXES

### Curriculum Vitae



**Kent Walker**  
**Senior Vice President & General Counsel**

As General Counsel, Kent is responsible for managing Google's global legal team and advising the company's board and management on legal issues and corporate governance matters.

Before joining Google, Kent held senior legal positions at a number of leading technology companies. Most recently he was Deputy General Counsel of eBay Inc., where he managed corporate legal affairs, litigation, and legal operations. Previously, he was executive vice president of Liberate Technologies, a provider of interactive services software founded by Oracle and Netscape Communications. He also served as Associate General Counsel for Netscape and America Online and Senior Counsel for AirTouch Communications, which was later acquired by Vodafone.

Earlier in his career, Kent was an Assistant U.S. Attorney with the United States Department of Justice, where he specialized in the prosecution of technology crimes and advised the Attorney General on management and technology issues.

Kent has served on the boards of a number of technology industry trade associations. He graduated from Harvard College and Stanford Law School.



**COMMISSIONER VĚRA JOUROVÁ**

**MEETING WITH MR DLOUHY,  
PRESIDENT OF THE CZECH CHAMBER OF COMMERCE**

**LOCATION: BERL 12/176**

**DATE AND TIME: 09/11/2017, 11H00**

**MEETING OBJECTIVE: EXCHANGE ON DUAL QUALITY FOOD AND PROMOTE THE  
BENEFITS OF THE GDPR**

**MEMBER RESPONSIBLE: EDUARD HULICIUS**

**DG CONTACT & TEL No:**

**HoU:**

**VERSION: 09/11/2017**

**CAB JOUROVA/851**

**PARTICIPANTS:**

## TABLE OF CONTENTS

STEERING BRIEF .....	2
DUAL QUALITY FOOD.....	3
GENERAL DATA PROTECTION REGULATION .....	8
CURRICULUM VITAE.....	12

### STEERING BRIEF

You are meeting the President of the Czech Chamber of Commerce, Mr Vladimír Dlouhý (CV in Annex), to discuss the issue of dual quality food and the General Data Protection Regulation.

The objectives for your meeting are:

#### **on dual quality food:**

- enquire about the position of Czech businesses;
- insist that existing laws are sufficient to address the issue and that new legislation especially at national level could backfire and generate a chain of protectionist measures across the Single Market. This would not be good for Czech exporters and the current good state of the Czech economy.

#### **on the GDPR:**

- promote the benefits of the GDPR;
- explain the Commission's priorities during the transition period;
- reassure that businesses have an opportunity to be actively involved in actions conducted during the transition period.

## DUAL QUALITY FOOD

### CONTEXT

It is likely that most members of the Czech Chamber of commerce, especially those which operate on local and regional markets only, are in favour of stricter controls of alleged dual quality practices by multinational competitors. The Czech Republic is very active in carrying out comparative tests which have confirmed the existence of dual quality of both food and non-food products (see Annex).

### LINE TO TAKE

- The Commission takes this issue seriously and has already taken decisive action, starting in the area of food.
- Our action comprises two strands: 1) dialogue with the industry concerned, and 2) empowering national enforcement authorities.
- The Commission has issued a specific interpretative notice to help traders and national authorities with the application of existing EU food and consumer protection legislation. The guidance acknowledges food business operators' right to differentiate their products to better adapt to local consumer preferences or sourcing.
- Consumers cannot be misled to believe that a product which is packaged and presented in the same way in several Member States is of the same quality and composition when this is not the case.
- The Commission's Joint Research Centre is developing and implementing a common testing approach, also regarding other products than food.
- In addition to funding the development of a harmonised testing approach (at least EUR 1 million), the Commission has offered funding to Member States to build enforcement capacities and to carry out further studies (EUR 1 million).
- The Commission is continuing the dialogue with the industry concerned and the high level Consumer Summit in Bratislava has reaffirmed the necessity for an effective and constructive multi-stakeholder dialogue.
- It is key that multinational brands take concrete steps to reduce unnecessary differentiations of products. Where such differentiations continue for legitimate goals, this should be made in a transparent way to make sure that consumers understand what they are buying. For example, if a brand manufactures several grades of a certain product: say: regular and extra crusty or extra fishy, consumers should understand which one is available in their local shops.
- The best way forward for the concerned industry is to engage in a proactive and voluntary way to increase the information available to consumers and to supply the same high-quality goods across the Single Market.
- These steps should be taken now; we are speaking about common high principles which stem directly from the Single Market spirit and they should therefore not be made dependant on the existence of a harmonised testing approach.
- There may be diverging views on these matters in your organisation – have you held a debate on this issue?

## **DEFENSIVES**

### **Your advice for the businesses concerned**

- Ideal solution: stop differentiation of markets or communicate better on possible differences, including the creation of specific grades.
- Businesses should also be more transparent on the actual measures taken to adapt to consumer preferences.

### **Your advice for the local/regional businesses**

- This debate is a good opportunity for local, regional, national producers to demonstrate the value of their products and to engage with consumers on issues such as sustainable consumption, local sourcing, preservation of traditional modes of production.
- However, it should not be turned into a disguised fight to obtain protectionist measures. Protection is not a winning path, competition on higher quality and better taste is the business way forward.
- The Single Market has considerably benefited the Czech economy it is therefore important that the free circulation of goods is preserved.

### **Freedom to do business**

- Producers and retailers are free to sell different products as long as they respect all legal requirements.
- However, consumers must not be misled.
- Studies show that there are seemingly similar products on the EU market, which contain more meat or fish in some Member States than in others.
- There should be neither double standards nor second-class consumers in the EU.

### **Applicable EU law for this issue – explained in the Commission's notice of 26 September**

- The 'General Food Law Regulation' (No 178/2002), which aims at ensuring that only safe food products are placed on the EU market and that consumers are accurately informed and not misled regarding the composition and characteristics of the food products offered for sale;
- The 'Food Information to Consumers Regulation' (No 1169/2011), which lays down general labelling rules and requirements, including mandatory provision of a complete list of ingredients to fully inform consumers about the composition of the food product;
- The 'Unfair Commercial Practices Directive' (2005/29/EC), which ensures that consumers are not misled or exposed to aggressive marketing. Moreover, it ensures that any claim made by traders in the EU is clear, accurate and substantiated. It seeks to enable consumers to make informed choices. This horizontal Directive applies to many commercial practices which are also regulated by other general or sector-specific EU legislation, such as food, toys, cosmetics, detergents and others, but only for those aspects which are not covered by sector-specific legislation.

### **New legislation to address the issue of dual quality of products**

- The Commission does not exclude but is currently not considering new legislation to tackle the issue of dual quality.
- Numerous rules in the field of food safety, labelling and consumer protection already apply. Now we need to focus on more effective enforcement of these rules.

### **Amending the Unfair Commercial Practices Directive as follow up to the Fitness Check of EU consumer law**

- Misleading practices can, already today, be caught by the specific Regulation on Food Information to Consumers or by the Unfair Commercial Practices Directive, which acts as a 'safety net'.
- Last year the Commission updated the guidance on how to apply the Unfair Commercial Practices Directive in practice, including addressing practices that can mislead consumers about the quality and composition of food products.
- The Commission recently adopted a Notice which further extends this guidance to assist national enforcement authorities when applying the Unfair Commercial Practices Directive and Food law legislation to address misleading practices related to dual food quality.

### **Finding of the Fitness Check: no need for a general revision of the Unfair Commercial Practices Directive**

- We are looking into targeted changes: a possible EU-wide right for consumers to seek redress against traders; or possible harmonisation of rules on how Member States should calculate penalties for breaches of EU consumer law.

### **Commission action to enforce EU consumer rules**

- Member States have the competence and powers to make sure that consumers are not misled.
- National consumer authorities need to make appropriate controls and enforce the European legislation at national level.
- At EU level, the national consumer authorities can cooperate and launch joint enforcement actions.
- The Commission has a supporting role in such actions

### **Possibility to restrict the free movement of goods**

- Under EU law, possible limitations to the free movement of goods are very strict:
- Under Article 36 TFEU, and the jurisprudence of the European Court of Justice, restrictions can only be justified on the basis of overriding grounds, such as health or consumer protection, but they need to be necessary to protect these objectives, and

proportionate, which means that there must be no less-restrictive measures available.

- Any national legislation would need to be notified to the Commission under the so-called technical regulations procedure (Directive 1535/2015) allowing the Commission and Member States to submit observations

#### **Alleged vertical restrictions by retailers**

- We have learnt that part of the problem comes from territorial suppliers' restrictions which prevent retailers from buying centralised and we have repeatedly called the industry to revisit their market segmentation policies which are no longer adequate as they reflect the state of the Single Market 20 years ago.
- When we look at the economic balance between the economies of scale permitted by the Single Market, on the one side, and the costs for managing and maintaining several production and distribution lines for differentiated products, on the other side, it becomes clear that it is neither worth nor necessary to continue fine market segmentations in an EU of half a billion consumers.
- We will continue to discuss this issue with the industry and at the political level, for example during the next meeting of the High Level Forum for a Better Functioning Food Supply Chain in December.

#### **Applicability of the Commission actions regarding food to non-food products**

- We clearly state in the guidance that we started to look at food related issue but that the guidance may be updated in the future in the light of new evidence based on the common testing common approach, also regarding products other than food.
- The UCPD is a horizontal consumer protection law which can apply as a "safety net" to tackle issues not regulated by sector-specific legislation. It applies to all products and most services marketed in the EU's Single Market. The principles in the guidance which concern the UCPD can therefore mutatis mutandis also be helpful for authorities seeking to examine unfair marketing practices in the area of non-food products.
- To what regards the harmonised testing approach, some of its general principles could certainly be relevant to other types of products.
- The funding offered to Member States to carry out further studies and build enforcement capacities (1 million) stems from the Consumer Programme and is therefore not limited to activities relating to dual quality food.

# ANNEX

## Overview over studies on dual quality food carried out in the Czech Republic

Date	Outline	Main findings	Comments
July 2017	Products sold in CZ were compared to products sold in DE (authorities)	Out of 23 products tested... 8 were different (35%) 15 were the same (65%)	In respect of the following products differences were identified by both studies:
September 2017	Products sold in CZ were compared to products sold in neighbouring countries (authorities)	Out of 21 products tested... 13 were different (62%) 5 were slightly different (24%) 3 were the same (14%)	<ul style="list-style-type: none"> <li>• Ice Tea Lemmon (NESTEA)</li> <li>• Activia Strawberry yoghurt (DANONE)</li> <li>• IGLO fish-sticks (NOMAD FOODS)</li> <li>• Luncheon Meat (TULIP)</li> </ul>
September 2017	A legal study carried out by the Faculty of Law of Palacky University in Olomouc	Examined several solutions to tackle the issue of dual quality food by legislation. The author of the study acknowledged that the action taken by the Commission is the fastest option but also raised amendments to the UCPD as possible solutions	Regarding possible UCPD amendments: <ul style="list-style-type: none"> <li>• Adding a specific criterion to Article 6(1)(b)</li> <li>• 'blacklisting' the practice in the annex of the UCPD</li> </ul>
September 2017	dTest o.p.s. (main Czech consumer testing association)	Compared detergents sold in CZ to detergents sold in DE  washing gels and powders from Ariel and Persil  8 products tested	<p>Gels: Tests did not show any major differences. The differences found in the "washing powder" were always less than 3%.</p> <p>- ingredients on the labels slightly different</p> <p>Powders: DE powders contains 3x more of phosphorus</p>
October 2017	Products sold in CZ compared to products sold in DE, AT, SK and HU (authorities)	Out of 21 products tested... 11 were different (52.4%) 3 were slightly different (14.3%) 7 were the same (33.3%)	

## **GENERAL DATA PROTECTION REGULATION**

### **CONTEXT**

The meeting is an opportunity to inform the President of the Czech Chamber of Commerce about the work that the Commission is undertaking vis-à-vis the Member States, the Article 29 Working Party and the stakeholders in the transition period towards implementation of the GDPR on 25 May 2018.

Companies doing business in Czech Republic should be in a phase of assessment as to the compliance of their processing operations with GDPR (to the extent that they have establishments in the EU or they offer products/services to the EU market). They might be critical of the guidelines of the Article 29 Working Party or over-exaggerate the costs incurred by compliance with GDPR.

As concerns the application of GDPR, at the end of August the Ministry of Interior published a draft law, which will replace current Act No. 101/2000 Coll. on the Protection of Personal Data. The draft law was submitted to inter-ministerial consultation in August with closure date 15/09. The draft law was planned to be submitted to Cabinet in the first part of October and to Parliament later following the general election at the end of October 2017.

### **LINE TO TAKE**

- The New European Union data protection regulation – the General Data Protection Regulation (GDPR), will be applicable from 25 May 2018. The new legislation modifies and updates data protection rules at EU level to make Europe fit for the digital age.
- The GDPR is a competitive advantage a trust-enabler and a key instrument to ensure level-playing field for all companies operating in the EU market. Increased trust from consumers will provide further business opportunities and chances for innovation. Companies will also have easier access to the whole EU market, with the current 28 national legislations being replaced by one, simple and clear legal framework. The GDPR is not a revolution; it simplifies the legal landscape for businesses and brings enhanced legal certainty for their operations.
- Commission is working closely with Member States to accompany them in the process of adapting or repealing their existing laws as necessary. We are fully aware that one of the main concerns of business is that measures taken at national level must not lead to any new fragmentation.
- We are also supporting the work of the Data Protection Authorities who have a key role in ensuring coherent interpretation and enforcement of the new rules. The Article 29 Working Party is playing an active role in preparing guidelines for companies and other stakeholders.
- Article 29 Working Party has already issued four guidelines to assist with implementation and interpretation of new legislation: on data portability, data protection officers, lead supervisory authority, and data protection impact assessments. The final versions of such documents were adopted on 5 April

2017 for the first 3 guidelines, and on 3 October 2017 for the last guideline, after a public consultation. The Article 29 Working Party plans to adopt further guidelines this year and at the beginning of 2018. For instance, guidelines on data breach notifications and profiling are subject to public consultation until 28 November 2017. Businesses are strongly encouraged to take advantage from the current consultation and provide their views.

- The Commission is reaching out to stakeholders, for instance through the organisation of targeted GDPR events (e.g. on health on 23 October and on SMEs in November). We published earlier this year an infographic aimed at SMEs. As announced in the letter of intent following President Juncker's State of the Union speech, the Commission will provide guidance to businesses, especially SMEs, and individuals so as to raise their understanding of the new rules in view of their application as of May 2018. This guidance would take the form of a practical online toolkit. We plan to have it ready by the data protection day on 28 January. We are also supporting financially awareness-raising activities carried out at national level, including by Data Protection Authorities. Finally, we have set up a multi-stakeholder group on GDPR to get the views of businesses and civil society (first meeting on 19 October).

## **DEFENSIVES**

### **How is the Commission planning to ensure that citizens and business are aware of new legislation?**

- We consider it essential to foster a uniform interpretation of the GDPR across Member States, hence our active work with national authorities either bilaterally or in the GDPR expert group, and our support to the work of Article 29 Working Party to produce a comprehensive set of guidelines. Existing national guidelines should be brought into compliance with those EU level WP29 guidelines since we are well aware of industry's concerns regarding the risk of inconsistent application.
- As already mentioned, EU grants are being allocated for training of DPAs and national authorities (including the production of materials), others in the coming months will more specifically target awareness-raising among SMEs and the general public. Building on this and to accompany these various actions, we will develop guidance, in the form of a toolkit, in order to prepare business and citizens about the new rights and obligations under the GDPR.
- We continue our open dialogue with all stakeholders, including civil society and businesses, to ensure that they are aware of their obligations and to dispel any doubts they may have about the application of the new rules.
  - For instance, we recently held our first multi-stakeholder expert group on 19 October to support the application of the GDPR in view of opinions of its members, including academia / legal practitioners / civil society and business representatives.
  - We also have regular exchanges to discuss about the GDPR and the sector specific issues. On 23 October, the Commission services held a workshop with more than 150 stakeholders active

in the health sector.

- On 27 November we will hold a workshop with the EU umbrella federation of SMEs and their national members to better understand the specific needs of SMEs.

### **Is the Regulation future-proof?**

- Future proofing means ensuring that legislation can adapt to new, diverse situations: therefore, many elements have been incorporated in the draft Regulation to face these challenges.
- Data protection by design means that responsible controllers, and developers, and manufacturers) should incorporate protection of personal data into new products and services while they are being designed, not after. Data protection must be the starting point and a continuum for appropriate protective measures, not an ending.
- The risk-based-approach: the Regulation pairs flexibility with effective protection. The reform is not about "box ticking" but ensuring that obligations reflect the risks posed by specific processing. Processing that is small and low-risk should not be treated as if it were high risk and frequent. Data protection impact assessments are a key part of the risk based approach, making sure that measures are always appropriate to specific risks and situations.
- Obligations to report data security breaches will improve consumer trust in the digital economy.

### **What is the Commission position on the guidelines recently published by the Article 29 Working Party?**

- The guidelines of the Article 29 Working Party are very important to provide increased legal certainty to stakeholders since they will guide the data protection authorities when implementing the GDPR.
- The Commission supports the work of the Article 29 Working Party and share with its members its views and expertise on the provisions of the GDPR. It also strongly encouraged the Working party to conduct public consultation on the draft guidelines.
- However, the Article 29 Working Party (and after May 2018 the European Data Protection Board) is an independent body and therefore the content of the guidelines are their responsibility.

### **Aren't the sanctions foreseen in the GDPR too high? 4% of annual turnover of a company is disproportionate.**

- The GDPR establishes a range of enforcement tools, including penalties and fines. All these tools must be applied in an effective, proportionate and dissuasive way. In each case the appropriateness to use this corrective measure must be determined by taking into account all the relevant

circumstances of the case into account, like inter alia:

- ☐ gravity/ duration of the violation;
  - ☐ number of data subjects affected and level of damage suffered by them;
  - ☐ intentional/negligent character of the infringement;
  - ☐ any actions taken to mitigate the damage;
  - ☐ degree of co-operation with the supervisory authority, etc.
- The GDPR sets out two main categories of caps of fines for infringements of the Regulation, depending on the gravity of the infringements.
  - The first cap of fines is set at the level of maximum EUR 10 million or in case of an undertaking up to 2% of worldwide turnover. An example would be an infringement of the obligations of the controllers to conduct impact assessments.
  - The higher cap of fines is set at the level of maximum EUR 20 million or 4% of worldwide turnover. An example would be an infringement of the data subjects' rights under the Regulation.



## CURRICULUM VITAE



✱ **Vladimír Dlouhý** was elected president of the Czech Chamber of Commerce in 2014 after having unsuccessfully tried to run for President of the Czech Republic in the first direct presidential elections in 2013.

Previously, since 1997, Dlouhý worked as international advisor for Goldman Sachs in Prague where he was covering the region of Central and Eastern Europe.

From 1992-1997 Dlouhý served as Czech Minister for Industry and Trade, while he simultaneously was member of the Parliament and Vice-chairman of Civic Democratic Alliance, a political party forming governing coalition.

In 1989 he was invited to join the first post-communist government and served as Minister of Economy of Czechoslovakia until 1992.

Dlouhý studied mathematical economics and econometrics in the Czech Republic and pursued MBA Studies at Catholic University Leuven in Belgium before starting an academic career.

The **Czech Chamber of Commerce** is the most important representation of the business sphere in the Czech Republic. It combines about 15.000 members from all business fields except for agriculture, food and forestry, which are represented by the Agrarian Chamber of the Czech Republic.

Its mission is to create opportunities for entrepreneurship, to promote and support measures that contribute to the development of business and thus to the overall economic stability of the Czech Republic.

**From:** HULICIUS Eduard (CAB-JOUROVA)  
**Sent:** 18 October 2017 23:06  
**To:** BRAUN Daniel (CAB-JOUROVA); [REDACTED]  
[REDACTED] CONSTANTIN Simona (CAB-JOUROVA);  
[REDACTED] HULICIUS Eduard (CAB-JOUROVA);  
LADMANOVA Monika (CAB-JOUROVA); NIKOLAY Renate (CAB-JOUROVA);  
O'CONNELL Kevin (CAB-JOUROVA); [REDACTED]  
[REDACTED] TALKO Wojtek (CAB-JOUROVA)  
**Cc:** [REDACTED]  
**Subject:** Flash note - meeting NOMAD foods  
**Importance:** High

Commissioner met today with representatives of Nomad Foods (Iglo and Findus frozen foodstuff brands) on discussion about the dual quality.

Nomad was represented by

- Steven Libermann (Managing director of Nomad Western Europe)
- Felix Fröhner (General manager Iglo for CEE)
- Sandra Brand (Director of Nomad European+Corporate department)
- Chokoualé Datou Laurent (Chairman of European Public Affairs, Weber-Shandwick)

The Commissioner gave brief overview of the history of the issue, her aims and the Commission plans of the next months, accenting also the political dimension of the problem (East-West divide).

Nomad has welcomed opportunity to talk to the Commission on allegations putting it into negative light. The representatives have explained that of 50 frozen foodstuff products sold in the CEE only 2 have cross-border differences – Vegetables (due to local conditions and tastes) and the Fish fingers. While the "Euro" version available in CEE AND Western Europe contains only 58% of fish (and as such is clearly leading in all markets), the DE+AT version contains 65% of fish – due to tradition. DE+AT legislation (today at level of ministerial notice?) sets the percentage of fish in fish sticks at 65%. We have also received a table comparing 14 main Fish fingers marks sold in the CEE+AT-DE – the range of meat content varies between 48%-67%.

Nomad regretted the lack of understanding and will to communicate on this issue by the CEE governments, and welcomed Commissions efforts. It has repeatedly pointed out the Consumers appreciation of the Iglo products, explaining the crispiness factor behind the reason of 58% of fish content.

The Commissioner has thanked for the information received and asked the company to be more assertive in explaining and communicating, also inviting them to participate actively on the JRC preparation of testing methodology. She has recalled the need for the companies to approach directly the governments of MSs seeing problems of the dual quality, and asked for understanding that the procedures next year are important for re-establishing trust in the single market and equality between EU consumers.

DG will keep contact with Nomad Food.

Kind regards,

**Eduard HULICIUS**

Member of Cabinet

Consumers and European Parliament



**European Commission**

Cabinet of Commissioner Věra Jourová  
Justice, Consumers and Gender Equality

B-1049 Brussels/Belgium

**From:** Steven Libermann [REDACTED]  
**Sent:** 23 October 2017 09:47  
**To:** CAB JOUROVA CONTACT  
**Cc:** HULICIUS Eduard (CAB-JOUROVA); NIKOLAY Renate (CAB-JOUROVA)  
**Subject:** Meeting with Nomad Foods Europe  
**Attachments:** Leave Behind in English Czech FINAL - 18 October 2017  
FINALDoubleSided.pdf

**Follow Up Flag:** Follow up  
**Flag Status:** Completed

Dear Commissioner,

Thank you for giving us the opportunity to meet with you and your team to discuss the 'dual quality in food' dossier.

We hope that you found the information that we provided helpful, and in particular the fact that our *iglo* branded fish finger products sold in the Czech Republic, Slovakia and Hungary are the same as those we sell in the UK, France and Portugal. We were therefore particularly shocked to see our brand explicitly associated with the notion of an East-West divide at the recent Bratislava Consumer Summit.

The fish finger products that we sell in Central and Eastern Europe (CEE) markets is the 'hero product' that we sell in the UK, where we first launched fish fingers in the 1950's. This product has achieved market leading positions in most of the markets where it is sold. The German and Austrian variant is, in effect, an exception to our preferred recipe due to local guidelines which we follow.

All the fish fingers that are sold to consumers in the UK, Germany, Austria and CEE markets are made in our Bremerhaven factory in Germany. As mentioned, we would be delighted to invite you for a visit.

Nevertheless, we do understand the challenge that industry and political leaders are facing on this issue, which is why we are happy to confirm our commitment to collaborating with the European Commission and the governments concerned so as to arrive at a mutually satisfactory solution that will ultimately enhance consumers' trust in the fish finger category.

We look forward to participating in the European Commission's work with the Joint Research Centre to establish a common testing methodology to improve food product comparative tests and related work streams. Sandra Brand, Head of Policy and Regulatory Affairs, will be our point of contact on this matter.

Please find attached a document summarising our position on this topic which also includes a Czech translation. In the meantime, if there are any questions or comments, please do not hesitate to contact me.

Kind regards,

Steven Libermann

Steven Libermann  
Managing Director – Western Europe

## Nomad Foods Europe



Nomad Foods Europe - Findus France

Maille Nord III | 7/10 Porte de Neuilly | 12 Boulevard du Mont d'Est | 93192 Noisy-le-Grand cedex | France



Web : [www.nomadfoodseurope.com](http://www.nomadfoodseurope.com)



*THINK BEFORE YOU PRINT: Before printing e-mails, think whether it is really necessary. Thanks!*

**CONFIDENTIALITY:** This email and any attachments hereto are strictly confidential and exclusively intended for the use of the recipient(s). They may contain material protected by legal, professional or other privilege whose non-authorized disclosure, copy, distribution, retain or utilization is contrary to the Law. If you are not the intended recipient hereof or the person responsible for delivering to the intended recipient, we request that you notify us immediately, and that you delete this email and its attachments from your systems without keeping a copy. You should refrain from using or disclosing the contents thereof to anyone, whether in full or in part.

# Nomad Foods Europe

## **We offer single quality fish finger products within a highly diversified food category**

1. All of our products are of the same high quality, irrespective of their market of destination. For example, the fish fingers we sell in the Czech Republic, Slovakia and Hungary are the same in fish content as the branded product of reference that we sell in the UK (our "hero product", with a 58% fish content), where we first launched fish fingers over sixty years ago. The identical product to CEE is also sold in France and Portugal.
2. There is no technical standard for fish fingers, which is part of the reason why the recipes vary so much across brands. In any given market, many different fish finger products, manufactured by both domestic and international players, compete for the consumer's purchasing decision. In the Czech Republic alone, 14 different fish finger references are sold under 9 manufacturer or retailer brands. Their fish content, including domestic manufacturers' products, ranges from 49% to 65%.

## **We offer a great quality fish finger product across markets**

3. We are committed to delivering quality, nutritious, affordable fish fingers to all our consumers wherever they live in Europe, and this is what has made our branded products the leading consumers' choice in many markets. Indeed, we tend to acquire a leading market share over time wherever we sell our "hero product".
4. Regarding sensory aspects, recent UK consumer testing showed that consumers judge fish fingers on great taste, high quality fish, balance of fish and crumb and the fish finger keeping its shape when cooked. Recent surveys showed that consumers preferred or equally rated 58% fish content over own and competing products with higher fish content.

## **We are transparent and any occasional recipe deviation is objectively justified**

5. Nomad Foods Europe's branded products either meet or exceed all EU regulatory requirements as regards transparent labelling and consumer information, therefore reflecting the actual products content and any variation that may exist from market to market.
6. As far as Nomad Foods Europe's products are concerned, objective factors determine occasional differences in the composition of our packaged products from market to market, including the availability of raw materials, preference for local sourcing, price elasticity, distribution channels, local regulatory requirements and indeed consumer taste.
7. National markets may also impose recipe alterations. In Germany, for instance, in the "Fischleitsätze" (Fish Guidelines) require some of our products to deviate from our so-called product of reference, hence creating an exception.

## **We welcome progress regarding the definition of a single testing methodology for food in the EU**

8. Nomad Foods Europe welcomes the European Commission decision to support the definition of a single testing methodology to improve food product comparative tests. We believe this to be essential to enhancing consumer trust in the food and drink sector across Europe. We equally believe that the tests that have been conducted on some of the fish finger products sold in Central and Eastern European markets may have led to misleading results because of the lack of stable and consistent testing methodology.

# Nomad Foods

## Europe

### Nabízíme produkty rybích prstů jednotné kvality ve vysoce různorodé kategorii potravin

9. Všechny naše výrobky mají stejně vysokou kvalitu, bez ohledu na to, pro který trh jsou určeny. Například rybí prsty, které prodáváme v České republice, na Slovensku a v Maďarsku, jsou stejný obsahem ryb jako značkový referenční produkt, který prodáváme ve Velké Británii (náš tzv. "hrdinský výrobek" s obsahem 58% ryb), kde jsme před šedesáti lety poprvé spustili prodej rybích prstů. Výrobek totožný tomu, který se prodává ve střední a východní Evropě, se také prodává ve Francii a Portugalsku.
10. Pro rybí prsty neexistuje žádná technická norma, což je také důvod, proč se recepty značně liší mezi značkami. Na kterémkoli daném trhu soutěží o spotřebitele mnoho různých výrobků, které jsou vyráběny jak domácími, tak mezinárodními hráči. Pouze v České republice se pod 9 značkami výrobců nebo maloobchodníků prodává 14 různých odkazů na rybí prsty. Obsah jejich ryb, včetně produktů domácích výrobců, se pohybuje od 49% do 65%.

### Nabízíme vysoce kvalitní produkt rybích prstů na různých trzích

11. Jsme odhodláni dodávat kvalitní, výživné a cenově dostupné rybí prsty všem našim spotřebitelům, ať už žijí kdekoli v Evropě, a to činí z našich značkových produktů popřední volbu pro spotřebitele na mnoha trzích. V průběhu času vskutku zvykneme získávat vedoucí podíl na trhu, kdekoli prodáváme náš "hrdinský výrobek".
12. Pokud jde o senzorické aspekty, nedávné spotřebitelské testování ve Velké Británii ukázalo, že spotřebitelé hodnotí rybí prsty dle jejich skvělé chuti, vysoce kvalitních ryb, rovnováhy ryb a obalovací směsi a jestli si udržují tvar při vaření. Nedávné průzkumy ukázaly, že spotřebitelé dávají přednost nebo ohodnocují stejně 58% obsah ryb v porovnání s vlastními a konkurenčními produkty s vyšším obsahem ryb.

### Jsme transparentní a každá příležitostná odchylka receptů je objektivně odůvodněná

13. Výrobky značky Nomad Foods Europe splňují nebo převyšují všechny regulační požadavky EU, pokud jde o transparentní označování a informace pro spotřebitele, a odrážejí tak skutečný obsah výrobků a jakoukoli odchylku, která může mezi trhy existovat.
14. Pokud jde o produkty společnosti Nomad Foods Europe, objektivní faktory určují příležitostné rozdíly v složení našich balených výrobků mezi trhy, včetně dostupnosti surovin, preferování místních zdrojů, cenové pružnosti, distribučních kanálů, místních regulačních požadavků a taky chutě spotřebitelů.
15. Vnitrostátní trhy mohou rovněž ukládat úpravy receptů. Například v Německu, Fischleitsätze (Pokyny pro ryby) požadují, aby se některé z našich výrobků odchylovali od našeho tzv. referenčního výrobku, a tudíž vytvářejí výjimku.

### Vítáme pokrok, pokud jde o definici jednotné metodiky pro testování potravin v EU

16. Nomad Foods Europe vítá rozhodnutí Evropské komise podpořit definici jednotné metodiky testování pro zlepšení srovnávacích testů potravinových výrobků. Věříme, že to má zásadní význam pro zvýšení důvěry spotřebitelů v potravinový a nápojový sektor v celé Evropě. Stejně jsme přesvědčeni, že testy, které byly provedeny na některých produktech rybích prstů prodávaných na trzích střední a východní Evropy, mohly vést k zavádějícím výsledkům kvůli nedostatku stabilní a konzistentní metodiky testování.



**EUROPEAN COMMISSION**  
DIRECTORATE-GENERAL JUSTICE and CONSUMERS

Directorate E: Consumers  
Unit E3: Consumer enforcement and redress

Brussels  
DG JUST [redacted]

Mr Steven Libermann  
Managing Director – Western Europe  
Nomad Foods Europe – Findus France  
E-mail [redacted]

**Subject: your email of 23 October 2017, 'Meeting with Nomad Foods Europe'**

Dear Mr Libermann,

Thank you for your availability to meet Commissioner Jourová at her request and for your email of 23 October 2017 in which you summarise again your position. Commissioner Jourová asked me to reply on her behalf.

The Commissioner welcomes your commitment to collaborate with the Commission and the governments concerned to arrive at a mutually satisfactory solution to the issue of dual quality food.

The Commission furthermore welcomes your active approach and your interest in participating in the work of the Commission's Joint Research Centre towards the development and implementation of a harmonised testing approach.

For this purpose, the JRC has recently launched a multi-stakeholder network. This network will be composed of approximately 50 participants from Member States' authorities, industry umbrella organisations (e.g. FoodDrinkEurope, AIM European Brands Association and others) and consumer associations. In order to guarantee the feasibility of the project and its completion in a timely manner, it was however necessary to restrict the pool of participants to the members and observers of the Sherpa Group of the High Level Forum (HLF) for better functioning of the food supply chain. The HLF was mandated with addressing the issue of dual quality of foodstuffs by the President of the European Council in its conclusions on 9 March 2017. The participation by individual companies, groups etc. will therefore not be possible, but in case you are a member of one of the industry associations you may wish to use them for voicing your concerns or making a contribution.

Engaging in a proactive and voluntary way to increase the information available to consumers is in my view the best way forward for the industry to ensure the consumers' trust in the Single Market. I would therefore like to encourage you to continue to take all possible steps in this regard and to participate to future dialogue opportunities not only at the European but also at the national level.

Thank you for your commitment and support of our work.

Yours sincerely,

[redacted signature]





**COMMISSIONER VĚRA JOUROVÁ**

**MEETING WITH IBM CEO GINNI ROMETTY**

**11/10/2017 16:15 -17.00**

**BERL 12/147**

**MEMBER RESPONSIBLE: MONIKA LADMANOVA/ WOJTEK TALKO/ KEVIN O'CONNELL**

**DG JUST CONTACT:**



**VERSION: 09/11/2018 12:36**

## TABLE OF CONTENTS

SCENE SETTER.....	3
PRIVACY SHIELD FIRST ANNUAL REVIEW .....	6
DATA FLOWS IN TRADE AGREEMENTS .....	17
GDPR .....	22
ROBOTICS / ARTIFICIAL INTELLIGENCE .....	27
WOMEN IN IT SECTOR .....	31
ENCRYPTION .....	34
CURRICULUM VITAE .....	37
IBM CEO GINNI ROMETTY .....	37
ANNEXES.....	38

## SCENE SETTER

You are meeting the CEO of one of the major and oldest US technology company – IBM (nicknamed Big Blue, founded in 1911). IBM is one of the world's largest employers, with (as of 2016) nearly 380,000 employees. It holds the record for the number of patents in the industry.

Ginni Rometty is the first female CEO of the company (since 2012, having climbed up the ranks since 1981). Long before that, IBM advocated for equal work for equal pay nearly 30 years before the US Equal Pay Act of 1963. Ms Rometty has been, on the other hand, criticised for increasing executive bonuses while firing staff and while profits lowered.

IBM is a member of the Privacy Shield and is supportive of the framework. In the company's statement at the launch of the framework, the main focus was the importance of international data flows. A bi-partisan House bill reauthorising but reforming Section 702 FISA has just been put forward. You should ask Ms Rometty to support reforms that would benefit also EU individuals.

IBM is actively promoting its products, which ensure GDPR compliance. To note that the Chief Privacy Officer is also a women (Cristina Cabella).

IBM's strategy has been to always move to higher value products, while spinning them off when they become "commodities" (e.g. personal computers, printers, servers). Therefore Artificial Intelligence is key for the company and the Watson AI computer is strong brand for the company and it is strongly focused on healthcare.

In the eve of your meeting, Ginni will host a public event in Brussels where she'll introduce the IBM corporate principles on ethics in AI (global data policy manifesto).

## LTT

### *Privacy Shield annual review*

- We were pleased with the review process. The Commission is now finalising a report that we intend to submit to the European Parliament and the Council very soon. The report will be made public.
- The report might contain a number of recommendations on how to improve the functioning of the Privacy Shield, but it positive overall.
- However, you will be aware that there are a number of ongoing legal challenges. As a major US IT company, you can support the sustainability of the framework by arguing in favour of maintaining the US legal framework – in particular PPD 28 - and supporting reforms of section 702 FISA (which is currently discussed in Congress), as well as ensuring functioning institutions – such as the Ombudsperson in the State Department and the PCLOB.

### *International Data flows*

- The Commission understands the economic importance of international data flows. Data protection is an EU fundamental right and therefore, transfers of personal data cannot be negotiated by the EU in a trade agreement, but in a separate track, such as with US and Japan.
- Ensuring a high level of data protection can go hand in hand with a policy of facilitating such data flows. Our Communication on "*Exchanging and Protecting Personal Data in a Globalised World*" of 10 January this year describes our vision and strategy to promote "upward convergence" of data protection standards around the world.
- Countries should not implement protectionist measures that are merely labelled as data protection but in reality pursue different (e.g. economic) objectives.
- Therefore, the Commission will seek to use trade agreements to set rules for e-commerce and tackle new forms of digital protectionism (such as data localisation requirements), in full compliance with and without prejudice to the EU's data protection rules.

#### *GDPR*

- Welcome the efforts IBM is taking on privacy and ensuring compliance with GDPR.
- The GDPR is a competitive advantage, a trust-enabler and a key instrument to ensure level-playing field for all companies operating in the EU market. Increased trust from consumers will provide further business opportunities and chances for innovation.
- Companies will also have easier access to the whole EU market, with one clear legal framework. The GDPR is not a revolution; it simplifies the legal landscape for businesses and brings enhanced legal certainty for their operations.
- Commission is working closely with Member States to accompany them in the process of adapting their existing laws as necessary. We are fully aware that one of the main concerns of business is that measures taken at national level must not lead to any new fragmentation.
- We are also supporting the work of the Data Protection Authorities who have a key role in ensuring coherent interpretation and enforcement of the new rules. The Article 29 Working Party is playing an active role in preparing guidelines for companies and other stakeholders.

#### *Women entrepreneurship and digital (gender) gap*

- Congratulate IBM on the long standing record of supporting women – the tech sector has persistent and deep gender-based asymmetries and they are not improving over time so success stories are very important.
- Among women entrepreneurs, very few are IT entrepreneurs. This lack of diversity is a major concern for European policy makers and employers alike.
- The Commission is determined to tackle the digital gender gap - specifically by supporting the Coalition for Digital Skills and Jobs – a platform for industry for upskilling in tech and by leading Code Week, during which hundreds of thousands of boys and girls across

Europe participate in coding classes. Also, special EU- funded platforms for women entrepreneurs help to connect, exchange expertise and get access to finance

- Women can thrive in digital careers and clearly diversity is an asset. It would be interesting to learn what actions IBM is planning to bring more women in the sector, help them to stay on the job and progress. Also, importantly, what were the lessons learnt.

#### *Robotics*

- The EU (Commission, Parliament) are actively looking at the impact of Robotics and Artificial Intelligence. Civil liability, safety and ethical/fundamental rights aspects are particularly relevant for the portfolio
- Invite IBM CEO to share with you their experience and views on these issues.

## **PRIVACY SHIELD FIRST ANNUAL REVIEW**

### **Context**

IBM is certified under the Privacy Shield program. Mrs Rometty (who has met also Vice President Ansip) might therefore be particularly interested in hearing the Commission's first impressions on the first annual review that took place on 18 and 19 September in Washington, DC.

Its purpose was to assess the correct functioning, implementation, supervision and enforcement of all aspects of the Privacy Shield framework, *i.e.* commercial aspects, as well as aspects relating to access by U.S. authorities to personal data transferred from the EU for national security and law enforcement purposes.

The Commission was accompanied by eight representatives of the Article 29 Working Group (from data protection authorities in France, Bulgaria, Germany, the UK and Hungary and from the European Data Protection Supervisor).

Around the table were all the U.S. authorities responsible for the administration, supervision and implementation of the program (the U.S. Department of Commerce, the Federal Trade Commission, the Department of Transportation), but also the authorities that committed to apply safeguards and limitations to government access to personal data for national security and law enforcement purposes (the Ombudsperson (an Acting Under-Secretary in the Department of State), the Office of the Director of National Intelligence, the Department of Justice, the Privacy and Civil Liberties Oversight Board, and the Inspector General of the Intelligence Community). In addition, there were representatives from some companies (Microsoft, Cisco, Ernst and Young) and Alternative Dispute Resolution bodies like TrustArc or Better Business Bureau (BBB) (that act as "independent recourse mechanism" under the Privacy Shield).

### **LTT**

- Since the program's inception (on 1 August 2016), more than 2,500 companies have joined the Privacy Shield.
- The participation of companies like IBM, Google, Microsoft, Facebook, but also that of many small and medium sized enterprises, confirms the (commercial) interest in the program, which facilitates transfers and reduces costs. At the same time the Privacy Shield ensures that the level of protection of the personal data transferred to U.S. companies certified with the Privacy Shield remains essentially equivalent to the one guaranteed within the EU.
- Moreover, let me stress that companies could increase trust with their European customers, in particular, with two specific types of actions:
  - under US law, companies can file transparency reports on the amount of requests by intelligence agencies to access user data. This helps to confirm that requests are kept within the limits of what is necessary and proportionate.

- and companies can choose the EU data protection authorities as their dispute resolution mechanism to deal with individual complaints. Unless they process human resources data, this is entirely voluntary. But submitting to such oversight can be a competitive advantage because European customers will feel more comfortable in handing over their data when they know they can turn to their "regular" authorities in case of complaints. Companies need to understand that "trust sells".
- **The first annual review of the Privacy Shield took place some three weeks ago in Washington, DC.**
- We were pleased with the process and in particular that all the U.S. authorities involved in the implementation of the Privacy Shield were around the table during the two-day meeting and ready to answer the questions of the Commission and of the representatives from the data protection authorities (the so-called Article 29 Working Party).
- This allowed the Commission and the data protection authorities to receive answers to our questions and led to constructive exchanges.
- The Commission is now finalising a report that we intend to submit to the European Parliament and the Council in the second half of October. The report will be made public.
- I can anticipate that the report might contain a number of recommendations on how to improve the functioning of the Privacy Shield, but it will be positive overall.
- However, you will be aware that there are a number of ongoing legal challenges. As a major US IT company, you can support the sustainability of the framework by arguing in favour of maintaining the US legal framework – in particular PPD 28 - and supporting reforms of section 702 FISA (which is currently discussed in Congress), as well as ensuring functioning institutions – such as the Ombudsperson in the State Department and the PCLOB.

### **Background**

The Privacy Shield is up and running since 1 August 2016.

It is a framework for the transfer of personal data from the EU to companies in the U.S. for commercial purposes. It is based on a certification system by which U.S. companies commit to adhere to a set of privacy principles - the EU-U.S. Privacy Shield Framework Principles (hereinafter also referred to as: 'the Principles'). While certification is voluntary, companies that have been certified are obliged to comply with the Principles, as they become enforceable under U.S. law. The Privacy Shield framework is administered and monitored by the U.S. Department of Commerce ("DoC") and compliance with the Principles is enforced by the Federal Trade Commission ("FTC") or the Department of Transportation ("DoT"), depending on which authority has jurisdiction over the Privacy Shield-certified company.

The Privacy Shield provides for a review to be conducted on an annual basis. The purpose of the review is to carefully assess the proper functioning, implementation, supervision and enforcement of the Privacy Shield framework. This concerns all aspects of the framework:

both compliance by companies and by U.S. authorities, including in the field of national security access to data.

**Defensive points**

***What about the two actions for annulment brought against the Privacy Shield?***

- Two actions for annulment of the Privacy Shield decision (one brought by Digital Rights Ireland and one by La Quadrature du Net) have been lodged with the General Court. While we cannot of course predict the outcome – like in any other case before the Court – we are confident that the decision will withstand judicial scrutiny. We strongly believe that the decision is lawful and in particular fulfils the requirements stipulated by the Court in the *Schrems* ruling.
- This being said, the commitments made under the Privacy Shield are not the only thing that matters. It will also be important that the U.S. honours its commitments in practice and fully implements the framework. This is yet another reason why the Annual Review was so important: it allowed us to check this and have a dialogue with our U.S. counterparts on all aspects of the Privacy Shield.

***How do you see the so-called Schrems II case?***

*(i.e. the referral that the Irish High Court (on 3 October) decided to make to the CJEU to determine the legal status of data transfers to the U.S. under the Commission-approved "Standard Contractual Clauses", Commission decision 2010/87/EU)*

- To be clear, the Irish case concerns a different data transfer tool, namely so-called Standard Contractual Clauses laid down in Commission decision 2010/87/EU.

- The Irish High Court decided, on 3 October, to refer questions to the CJEU to ascertain whether the alleged absence of effective remedies in the U.S. in case of access by U.S. state agencies to personal data sent there on the basis of the Commission-approved standard contractual clauses violates European fundamental rights (namely the rights to privacy, to the protection of personal data, and the right to an effective remedy and to a fair trial under, respectively, Articles 7, 8 and 47 of the Charter of Fundamental Rights of the EU).

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

***Influence of the Tele2 judgement on the Privacy Shield?***

- The Court's judgment in Tele 2 has brought an important clarification of the conditions for legality of national legislation imposing data retention obligations on private actors (electronic communication service providers), in

the light of EU law. In essence, the judgment applies the standards that the Court developed in "Digital Rights" – the 2014 judgment that invalidated the EU data retention directive – to national regimes on data retention.

- The Court makes clear that general and indiscriminate retention of data are precluded under EU law. Targeted retention of data solely for the purpose of fighting serious crimes is admitted, provided that a number of strict conditions are observed. The Court also spells out the conditions under which access of public authorities to retained data can take place.
- This last aspect certainly influences the way in which the Parliament considers the issue of bulk collection in the Privacy Shield. This and the independence and powers of the Ombudsperson are points of major concern for the European Parliament.

### ***Outstanding implementation measures in the Privacy Shield***

- Since the Privacy Shield became operational on 1 August 2016, a lot has been done to implement the various complaint mechanisms for Europeans.
- For example: our Data Protection Authorities have set up a centralised body for dealing with complaints concerning access to personal data by U.S. intelligence agencies. This centralised body will help EU individuals by transferring complaints to the newly created Ombudsperson.
- Our Data Protection Authorities have also drawn up the rules on a data protection panel that will deal with complaints concerning the processing of personal data transferred for commercial purposes.

- A third example is the arbitration panel that will be the last resort for unresolved complaints and which is now ready to operate. The U.S. Department of Commerce, together with the Commission, has selected 16 arbitrators from various countries (not just the U.S.), all with a privacy background. We are going to select soon some more candidates to have a solid pool of at least 20 arbitrators. Moreover, we have agreed with our American counterpart the Rules of Procedure of the Arbitration Panel.

### ***EU-US data protection under the Trump administration***

- At the annual review we have reiterated that it is essential for the sustainability of the Privacy Shield that the overall privacy framework in the US does not change, in particular as regards access to personal data by public authorities, and that surveillance reforms continue. This includes for example keeping in place Presidential Policy Directive 28 (PPD- 28), which is a key foundation for the part of Privacy Shield addressing access to data for national security reasons. It also includes ensuring the effective functioning of the newly created Ombudsperson.
- We have received assurance that the new administration is committed to our common goal and again confirmation that none of the developments in the U.S. over the past year affect the commitments taken under the Obama administration.
- Since the new administration took office, certain developments seemed at first sight possible cause for concern. This includes President Trump's Executive Order on immigration matters of 25 January, or the current status of the PCLOB - the Privacy and Civil Liberties Oversight Board -, which still

lacks four of the five regular Board members (although President Trump has recently nominated a new Chairman who still needs to be confirmed by the Senate).

- We have analysed these developments when they occurred and our assessment is that, so far, they do not negatively affect the Privacy Shield.
- Moreover, the Commission has contacted the U.S. authorities on a number of occasions to request clarifications. On both accounts (the Executive Order and the PCLOB), the Department of Justice has confirmed our preliminary assessment that the Privacy Shield will not be affected.

***Does President Trump's Executive Order "Enhancing Public Safety in the Interior of the United States" of 25 January 2017 negatively impact the Privacy Shield?***

- Despite its specific objective to address issues of immigration, the Order indeed contains a general provision - Section 14 - which concerns the treatment of foreigners (including Europeans) under the 1974 U.S. Privacy Act and provides that: *"Agencies shall to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information"*.
- However, according to the Commission's analysis, the Executive Order does not affect the data protection guarantees available to Europeans under the EU-U.S. Privacy Shield, as the adequacy decision does not rely on the protections under the U.S. Privacy Act which the Executive Order seeks to

limit. This assessment has also been officially confirmed by the U.S. Department of Justice following a request for clarification from the Commission. In its letter of 22 February, the DoJ expressly states that Section 14 of the Executive Order does not affect the U.S. commitments under the Privacy Shield.

- [REDACTED]  
[REDACTED] the Commission will remain vigilant and continue to monitor any developments in U.S. law that might have an impact on the data protection rights of Europeans when their personal data are transferred across the Atlantic.

***Repeal of Obama-era broadband privacy rules. Will this cause the suspension of the Privacy Shield?***

- The decision by the U.S. Congress to repeal the privacy rules adopted by the Federal Communications Commission (FCC) in October of last year certainly sends a negative sign when it comes to privacy protections in the United States. However, we see no impact on the EU-US Privacy Shield, for three reasons:
  - the Privacy Shield only applies to companies that fall under the jurisdiction of either the Federal Trade Commission (FTC) or, for airlines companies, the U.S. Department of Transport (DOT). Companies that fall under the jurisdiction of the FCC are not covered;
  - the Commission's adequacy decision on the Privacy Shield does not

- and could not rely – on the new FCC privacy rules which were only adopted AFTER the adoption of the Privacy Shield decision and have in fact never become effective;
- in any event, the Privacy Shield framework by itself stipulates the privacy principles and obligations on which the Commission's adequacy assessment is based. U.S. companies that want to benefit from the Commission's adequacy decision have to commit to comply with these principles and obligations.

***Trump's administration has not yet appointed a new Ombudsperson. Will that cause the suspension of the Privacy Shield?***

- We have repeatedly indicated that even if, to date, the incoming US administration has not yet appointed a new Ombudsperson following the end of term of Mrs Novelli, Mrs Judith G. Garber, Acting Assistant Secretary, Bureau of Oceans and International Environmental and Scientific Affairs, currently ensures, ad interim, the functions of the Ombudsperson, as Acting Under Secretary.
- Of course, however, the lack of a swift appointment of a successor to Mrs Novelli has not been well perceived and we therefore hope that the appointment of the new Ombudsperson will take place soon.

## **DATA FLOWS IN TRADE AGREEMENTS**

### **Context**

In the EU, data protection is a fundamental right that is non-negotiable in trade agreements. That is why discussions on data protection (including adequacy talks) and trade negotiations with third countries have to follow separate tracks.

At the same time, the Commission intends to use trade agreements to tackle new forms of digital protectionism (such as data localisation requirements), as long as this is done in full compliance with and without prejudice to the EU's data protection acquis.

This includes rules on international data transfers, which under our acquis are only allowed under certain conditions, namely if it is ensured that the level of protection guaranteed in the EU is not undermined.

Consequently, with the US, the issue of commercial data flows and data protection (as regards personal data) is dealt with in the Privacy Shield arrangement, outside the context of trade agreements. Similarly, with Japan, personal data protection is being dealt with in adequacy discussions, in parallel with FTA negotiations.

### **LTT (in case IBM raises this issue)**

- Trade negotiations, including TTIP or TISA are not the right place to deal with data protection. In our constitutional system, data protection and privacy are fundamental rights that are not 'negotiable' (in trade agreements or otherwise).
- This being said, ensuring a high level of data protection does not require impeding cross-border data flows, including of personal data. In fact, the EU data protection rules prove that a high level of protection can go hand in hand with a policy of facilitating such data flows. The EU data protection rules provide business operators with a number of flexible transfer tools that can be used to facilitate data transfers.
- The EU fully respects – and in fact encourages – that other countries also implement safeguards for the protection of personal data. In fact, our Communication on *"Exchanging and Protecting Personal Data in a Globalised World"* of 10 January this year describes our vision and strategy to promote "upward convergence" of data protection standards around the world.
- At the same time, countries should not implement protectionist measures that are merely labelled as data protection but in reality pursue different (e.g. economic) objectives.
- Therefore, the Commission will seek to use trade agreements to set rules for e-commerce and tackle new forms of digital protectionism (such as data localisation requirements), in full compliance with and without prejudice to the EU's data protection rules.

**Defensives**

***Where is the Commission with the ongoing debate on including data flow provisions in trade agreements?***

- The Commission issued a concept paper on this important issue last January.
- This was followed by a broad consultation with the Parliament, Member States, the European Data Protection Supervisor (EDPS) and other stakeholders from both civil society and the business side that have provided us with multiple inputs.
- This is an important and difficult debate, and we must get the balance right between our "offensive" (trade) and "defensive" (data protection) interests. Given that we are talking about a fundamental right, we indeed have to make sure that there are "rock solid safeguards on data protection" when we include obligations to tackle data protectionism in trade agreements.
- This internal debate is still ongoing so I am afraid I cannot tell you more at this point.

***Why are you dealing with data flows through separate adequacy decisions and not addressing this issue in the Free Trade Agreement?***

- The EU considers that trade negotiations are not the right place to deal with data protection.
- This being said, the EU data protection rules prove that a high level of protection can go hand in hand with a policy of facilitating such data flows.

- The most comprehensive solution is that of an adequacy decision as it essentially treats a third country – for the purposes of data protection – like an EU Member State. This ensures the free flow of data.
- Aside from an adequacy decision, the EU's data protection rules provide business with a number of flexible transfer tools, in particular contractual arrangements such as Standard Contractual Clauses and Binding Corporate Rules.

***Is it possible to address the issue of personal data transfers when the data protection regimes in the EU and the US are so different?***

- Yes, this is what the EU and the US have succeeded to achieve with the Privacy Shield finalised in July and entered into operation in August 2016.
- This new framework protects the fundamental rights of Europeans when their data is transferred to the United States, whilst at the same time allowing the free flow of (personal) data from the EU and ensuring legal certainty for businesses.
- Compared to the old Safe Harbour, this arrangement imposes stronger obligations on companies in the U.S. to protect the personal data of Europeans and stronger monitoring and enforcement by the U.S. Department of Commerce and the Federal Trade Commission (FTC), including increased cooperation with the European Data Protection Authorities.

- The new arrangement also includes written commitments and assurances by the U.S. government that any access by public authorities to personal data transferred under the Privacy Shield on law enforcement and national security grounds will be subject to clear conditions and limitations, preventing generalised access.
- In addition, it creates a totally new oversight mechanism in the area of national security access, the Ombudsperson.

[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]

## **GDPR**

### **Context**

The meeting is an opportunity to inform the audience about the work that the Commission is undertaking vis-à-vis the Member States, the Article 29 Working Party and the stakeholders in the transition period towards implementation of the GDPR on 25 May 2018.

IT companies as other operators should be in a phase of assessment as to the compliance of their processing operations with GDPR (to the extent that they have establishments in the EU or they offer products/services to the EU market). They might be critical of the guidelines of the Article 29 Working Party or over-exaggerate the costs incurred by compliance with GDPR.

IBM belongs to the umbrella organisation Business Europe. During the negotiations of the GDPR, Business Europe was very active in presenting the views of their members. While Business Europe welcomed the adoption of harmonised law at EU law, it was nevertheless dissatisfied that such law imposes obligations which have financial implications (like the appointment of data protection officer required in certain cases). Business Europe was also dissatisfied that the GDPR leaves certain flexibility clauses for the Member States.

At the same time, it seems that IBM sees the introduction of the GDPR as a possibility for the promotion of its products. IBM stresses in its materials for their potential new clients that the GDPR may substantially affect their different business models and that the GDPR allows for the possibility to impose substantial fines. Therefore, IBM advertises its products as fully compliant with the GDPR.

### **LTT**

- The GDPR is a competitive advantage a trust-enabler and a key instrument to ensure level-playing field for all companies operating in the EU market. Increased trust from consumers will provide further business opportunities and chances for innovation. Companies will also have easier access to the whole EU market, with the current 28 national legislations being replaced by one, simple and clear legal framework. The GDPR is not a revolution; it simplifies the legal landscape for businesses and brings enhanced legal certainty for their operations.
- Commission is working closely with Member States to accompany them in the process of adapting or repealing their existing laws as necessary. We are fully aware that one of the main concerns of business is that measures taken at national level must not lead to any new fragmentation.
- We are also supporting the work of the Data Protection Authorities who have a key role in ensuring coherent interpretation and enforcement of the new rules. The Article 29 Working Party is playing an active role in preparing guidelines for companies and other stakeholders.
- The Article 29 Working Party has selected several central aspects of the GDPR on which

they have or will issue guidelines (e.g. portability, data protection officer, high risk, consent, transparency). The Commission strongly encouraged the Working Party to conduct public consultation on the draft guidelines, and shared its view and expertise on their content. However, the Article 29 Working Party (and after May 2018 the European Data Protection Board) is an independent body and therefore the content of the guidelines are their responsibility. We strongly encourage you to make your views known in the context of the public consultations.

- The Commission is reaching out to stakeholders, for instance through the organisation of targeted GDPR events (e.g. on health on 23 October and on SMEs in November). We published earlier this year an infographic aimed at SMEs. As announced in the letter of intent following President Juncker's State of the Union speech, the Commission will provide guidance to businesses, especially SMEs, and individuals so as to raise their understanding of the new rules in view of their application as of May 2018. This guidance might take the form of a practical toolkit. We plan to have it ready by the data protection day on 28 January. We are also supporting financially awareness-raising activities carried out at national level, including by Data Protection Authorities. Finally, we have set up a multi-stakeholder group on GDPR to get the views of businesses and civil society (first meeting on 19 October).

### **Background**

The General Data Protection Regulation together with the Data Protection Directive for Police and Criminal Justice Authorities ("Police Directive") form the "data protection reform" package. The GDPR entered into force on 24 May 2016 and shall apply from 25 May 2018. The Police Directive entered into force on 5 May 2016 and EU Member States have to transpose it into their national law by 6 May 2018.

At the request of the Member States, we will continue working with them in the context of the Member States Expert Group prepare the implementation of the GDPR and the transposition of the Police and Criminal Justice Authorities Directive.. The last meeting of the Expert Group was on 18 September on GDPR and on 2 October on the Police Directive.

The Commission has just launched a study in 2017 on certification mechanisms in order to assess whether it would make sense to make use of Commission empowerments for delegated and implementing acts. At the request of the Parliament, we conduct a pilot project aimed at providing a Fundamental rights review of EU data collection instruments and Programmes.

The Article 29 Working Party has adopted a first set of 3 guidelines in April: the right to data portability, data protection officers (DPO), and the designation of the lead Supervisory Authority . Guidelines on data protection impact assessment were submitted to public consultation in April. At the WP29 Plenary of 3-4 October, WP29 plan to adopt guidelines on data protection impact assessment, profiling and data breach notifications. They will also adopt guidelines on administrative fines and urgency procedure as internal documents. The WP29 will also discuss future guidelines on content, transparency and on issues related to international data transfers.

In the coming months, we will start co-financing the training of data protection supervisory

authorities and other public authorities and data protection officers via action grants. The results of the call for proposals shall be published soon. We published earlier this year an infographic aimed at SMEs and a series of factsheets published in January 2017 which explains in easy way different benefits of the new data protection legislation for citizens and industry.

We will organise targeted GDPR events, e.g. on health on 23 October and on SMEs in November.

In line with the letter of intent issued following President Juncker speech on the state of the Union, we will prepare guidance for businesses and individuals. This guidance could take the form be a practical toolkit, the exact form of which still has to be discussed with CAB. . The objective is to have it ready for the Data protection day on 29 January.

We are also launching a new multi-stakeholder expert group to support the application of the GDPR, which will include a number of civil society/business/industry representatives. The group will allow for a structured dialogue on potential challenges resulting from the application of the GDPR, on ensuring awareness-raising and providing early advice on the preparation of delegated / implementing acts. The first meeting of the group will take place on 19 October.

### **Defensive points**

#### ***What is the Commission position on the guidelines recently published by the Article 29 Working Party?***

- The guidelines of the Article 29 Working Party are very important to provide increased legal certainty to stakeholders since they will guide the data protection authorities when implementing the GDPR.
- The Commission supports the work of the Article 29 Working Party and share with its members its views and expertise on the provisions of the GDPR. It also strongly encouraged the Working party to conduct public consultation on the draft guidelines.
- However, the Article 29 Working Party (and after May 2018 the European Data Protection Board) is an independent body and therefore the content of the guidelines are their responsibility. Commissionaire Jourova addressed a letter to WP 29 concerning the guidelines on portability.

#### ***Is the Regulation not extra-territorial?***

- The Regulation has a very clear territorial scope which ensures a level-playing field for all operations active in the EU market.

- It applies to operators having establishments in the EU or to those not established in the EU but operating on the EU market by offering goods/services to data subjects in the EU or monitoring their behaviour.

***Won't the Regulation hamper innovation and 'big data' analytics?***

- High levels of data protection and innovation can go hand in hand.
- In fact, the "data protection by design" principle encourages innovative ways of strengthening data protection. It requires that data protection is built in from the start.
- 'Big data' analysis does not always require personal data, but when it does, fundamental rights have to be respected.
- The Regulation provides for ways that allows for further processing of personal data for "big data" analysis.
- "Big data" analytics can lead to useful discoveries, but it is not really necessary to use all personal data, for example the person's name.
- Pseudonymisation can be a useful tool in this context and it is recognised in the Regulation.

***Aren't the sanctions foreseen in the GDPR too high? 4% of annual turnover of a company is disproportionate.***

- The GDPR establishes a range of enforcement tools, including penalties and fines. All these tools must be effective, proportionate and dissuasive. The agreement on fines ensures that they are a deterrent. Each case must be determined by taking into account the relevant circumstances of the infringement:
  - gravity/ duration of the violation;
  - number of data subjects affected and level of damage suffered by them;
  - intentional character of the infringement;
  - any actions taken to mitigate the damage;
  - degree of co-operation with the supervisory authority.

- The agreement sets out two main categories of ceilings of fines for infringements of the Regulation, depending on the gravity of the infringements.
- The first ceiling of fines is up to a maximum of EUR 10 million or in case of an undertaking up to 2% of worldwide turnover. An example would be an infringement of the obligations of the controllers to conduct impact assessments.
- The higher ceiling of fines is up to a maximum of EUR 20 million or 4% of worldwide turnover. An example would be an infringement of the data subjects' rights under the Regulation. This depends on the circumstances of each individual case.

***What does it mean in practice: Commission guidance to prepare citizens, business and public administrations for the direct application of the General Data Protection Regulation as of 25 May 2018, to be prepared in close consultation with the Article 29 Working Party/the new European Data Protection Board?***

- As already mentioned, we consider it essential to foster a uniform interpretation of the GDPR across Member States, hence our active work with national authorities either bilaterally or in the GDPR expert group, and our support to the work of Article 29 Working Party to produce a comprehensive set of guidelines. Existing national guidelines should be brought into compliance with those EU level WP29 guidelines since we are well aware of industry's concerns regarding the risk of inconsistent application. EU grants are being allocated for training of DPAs and national authorities (including the production of materials), others in the coming months will more specifically target awareness-raising among SMEs and the general public. Building on this and to accompany these various actions, we will develop practical guidance in order to help prepare business, especially SMEs and citizens about the new rights and obligations under the GDPR, and achieve the objective set in the letter of intent published after President Juncker's speech on the state of the Union. Our objective is to have this ready by January 2018.

## **ROBOTICS / ARTIFICIAL INTELLIGENCE**

### **Context**

Robotics/AI are complex systems which distinguish from "traditional" machinery by a certain level of autonomy. The complexity of algorithms governing autonomous systems increases, resulting in systems with sophisticated self-learning capabilities and increased autonomy. They bring benefits, since they may potentially increase productivity, prevent human failures and improve safety. On the other hand, such autonomous systems may eventually cause harm to humans or damage to persons or to other objects. The different layers of components that compose autonomous systems increase the complexity of liability issues, making it difficult to assess the contribution of each component to an act or decision of the system as a whole. The level of complexity further increases, when the system is composed of hard- and software components from different providers. The traditional liability rules on these systems with regard to damages need to be assessed.

As announced in the Commission Communication on Building a European Data Economy of 10 January 2017, the Commission carried out in spring 2017 a public consultation and a structured dialogue with stakeholders. The results showed that the appetite for changing the current liability regime in Europe is limited in general among stakeholders. A few stakeholders, mainly from the consumer side, believe an overhaul would be beneficial and necessary. The state of progress of internal discussions in the Member States is very heterogeneous while the importance of liability issues is acknowledged in general. The main message sent by Member States was that any initiative at European level would need to be discussed further and carefully considered before considering improvements and modifications to the current legislative framework.

Issues related to the safety of robots, artificial intelligence and connected products are likely to present significant challenges for the future. Currently the safety of robots and connected products is covered by several pieces of legislation, mainly under the responsibility of DG GROW. However, the General Product Safety Directive has a role as a "safety net" and could cover possible gaps that are identified with regard to consumer product safety. These possible gaps are to be mapped.

The European Parliament has adopted a resolution on 16 February 2017 with recommendations on Civil Law Rules on Robotics which request the Commission to submit a proposal for a legislative instrument.

### **LTT**

- Explain that civil liability aspects for Robotics/AI in Europe need to be evaluated.
- Point out that in the EU, the current Product Liability Directive (PLD) of 1985 which attaches strict liability for defective products to the producer is an important element of the current legislative framework and will be examined in this context.
- However, Robotics/AI have specificities such as system autonomy and technical complexity, which put into question the adequacy of the existing rules at EU and national

level.

- The question of safety of such products that are made available to consumers is also a priority for the Commission. Safety is addressed by several pieces of EU legislation and it is currently being assessed whether there are any gaps that need urgent action.
- Invite IBM CEO to share with you their experience and views on civil liability and safety challenges in connection with Robotics/AI.

### **Background**

During the last years, concerns on the possible inadequacy of the current legal frameworks in relation to liability for Internet of Things (IoT) and robotics have been voiced by different Commission Communications: the DSM Strategy (2015), the Digitising the European Industry Package (2016) and the Package on Building a European Data Economy (January 2017). In its Communication on the Mid-Term Review on the DSM the Commission stated that it will further analyse whether to define principles to determine who is liable in cases of damage caused by data-intensive products.

The concerns regarding a potential inadequacy of the current legal frameworks are linked to the specificities of IoT/robotics technologies. Firstly, they show an increased level of complexity and high interdependency between their different components and layers, ranging from the data itself, the different software components and applications, the tangible parts and their components, to sensors, actuators, data services, and connectivity. Secondly, robots/autonomous systems evolve towards increased autonomous behaviour. They will have increased capabilities to understand and interpret the environment, interact with humans, learn new behaviours and execute actions autonomously without humans.

Both specificities make it difficult to minimise at the outset the risk of damages and to allocate liability in case of damages as it will be difficult to identify the liable actor and to establish what, if anything, went wrong.

Legal certainty in relation to the allocation of liability in the IoT/robotics environment is important to create investment security and ensure consumer protection. Safety issues are also crucial when reflecting on the policy recommendation for IoT and robotics. The Commission therefore considers that a discussion on the adaptation of the regulatory framework is needed. In the same vein, a Resolution of the EP calls on the Commission to look at these challenges and consider a legal regime that adequately deals with the challenges raised by emerging digital technologies.

#### *Existing Product Liability regime*

One of the main questions in relation to liability is whether it is appropriate to shape liability rules for damages arising in the context IoT and robotics around the existing rules on product liability.

The Products Liability Directive (PLD) establishes a liability of producers when defective products cause damages to consumers as they do not provide the safety which consumers are

entitled to expect. Different from usual tort law liability, this is a strict liability, i.e. the victim does not have to prove fault of the wrongdoer. Still, the injured person has to prove the defect in the product, the damage and the causal link between the defect and the damage.

Both IoT and robotics can involve/constitute tangible products which, if found defective, trigger the application of PLD. However, as acknowledged in the Data Economy Communication and its accompanying Staff Working Document, there are problems stemming from the above mentioned specificities of IoT and robotics/autonomous systems, which can make it difficult to use/adapt the PLD for this purpose.

Indeed, the increased level of complexity and the high interdependencies between the different layers of these technologies, it may be difficult for the victim (which will be most often a natural person) to discover and prove that a defect occurred. On top of that, as robots acquire autonomous capabilities, some effects may not constitute a defect, but still lead to damage. For instance we may conceive an action performed by a robot, which, based on its self-learning abilities, causes damage for which no flaws in the software layers, no defect in the tangible product as such and no problem at the level of connectivity or other data services can be shown - as the action was exclusively based on robots' autonomous behaviour.

Furthermore, these new technologies and ecosystems involve a wide range of market players each providing the different parts and layers of this ecosystem - and consequently, each playing a potential role when allocating liability. It is also assumed that such interdependencies are becoming more complex as products evolve. In many cases IoT technology depends for its proper functioning on remote third party applications/technologies. This also adds to the complexity of the design and system integration. It may therefore not be appropriate to allocate liability always to the producer.

#### *Possible solutions*

Based on preliminary discussions at services level (JUST, GROW, CNECT) and initial input from stakeholders, the Data Economy package has put forward several options for further consideration.

- **Product liability approach**

This option is based on the approach taken by the PLD. This would mean that only the manufacturer could be held liable. For the injured party it would not be necessary to prove the manufacturer's fault. However, the victim would still need to prove a defect, the damage and the causal link between the defect and the damage in order to trigger the strict liability of the producer. Injured parties would be likely to face considerable difficulties in proving the defect and its causal link with the incurred damage. Technical expertise may be costly and litigation long.

- A risk-opening approach

A risk-opening approach would allocate liability to the market actor using the technology and thereby generating a risk for others, but at the same time benefitting from the use of the relevant device, product or service. Such an actor could be for instance the hospital that uses surgical robots to perform complex surgery on patients or a company that operates a factory and is using industrial robots working together with human employees to produce and assembly products, etc. This would still be a strict liability regime, i.e. the victim would not need to prove a fault, but simply the damage and that the damage has been caused by the robot/ autonomous systems. This option draws inspiration from existing rules assigning the liability to market actors for aeroplanes, nuclear power plants or animals. This approach entails more legal certainty for the victim and therefore less and less costly litigation.

- A risk-management approach

A third alternative is a regime based on a risk-management approach, where liability is assigned to the market actor which is best placed to minimise costs and risks in relation to the new technologies. Similarly to the risk-opening approach, the victim does not need to identify the origin of the defect. This would still be a strict liability regime, i.e. the victim would not need to prove a fault, but simply the damage and that the damage has been caused by the robot/autonomous systems. This approach could also increase legal certainty and therefore lead to less and less costly litigation.

- Insurance

All envisaged options should be coupled with voluntary or mandatory insurance schemes. Targeted insurance schemes could be offered to the owners of devices, producers or service providers (depending on the approach followed), to cover the risks linked to liability and compensate damages caused by the use of IoT and robotics. All options and their potential impacts, for instance on innovation, insurance costs and prices, would need to be further analysed. Furthermore, there are other common features to be assessed, like the questions of exculpation of the wrongdoer or capping of the damage.

## **WOMEN IN IT SECTOR**

### **Context**

IBM has a long standing record of supporting their female employees. Women have been working in tech jobs at IBM since the '30s and they became vice presidents already in the '40s. IBM advocated for equal work for equal pay nearly 30 years before the US Equal Pay Act of 1963. Since then, the CEO is Mrs Ginni Rometty - a woman with a tech-focused plan to lead IBM forward. As the IBM financial results are not very good, there are many who criticise her actual performance as a CEO

The European Commission is committed to tackle the digital gender gap. EU New Skills Agenda for Europe addresses digital skills across 10 concrete actions. One of them is the Digital Skills and Jobs Coalition, which brings together stakeholders who commit to take action to increase digital skills in Europe. These actions target four groups: citizens, people in the education system, the labour force and ICT professionals. To tackle the digital gap between men and women the Commission launched a targeted call inviting organisations to take action to equip more women and girls with digital skills and entice them to pursue ICT studies and careers at the end of April 2017.

The Commission also supports EU Code Week, which is a grass-roots movement that aims at getting more people to explore the potential and fun of coding and build their confidence in using and creating with digital technologies. In 2016 46% of the 970,000 participants were women.

The Commission announced, in its Strategic Engagement for Gender Equality 2016-2019 that it would step up efforts to raise awareness and promote women entrepreneurship. To this end, an e-platform for female entrepreneurs (WEgate) facilitates e-access to information on starting-up and growing a business, training and mentoring. It allows exchange of good practices and enables discussions and networking with other women entrepreneurs. In addition, in 2017, the Commission launched 4 projects covering 14 EU Member States to support women entrepreneurs in accessing funding by business angels.

### **LTT**

- Congratulate IBM on the long standing record of supporting women – the tech sector has persistent and deep gender-based asymmetries and they are not improving over time so success stories are very important.
- Despite that there are more women in the tech sector and even more in leadership than 10 years ago, the gap is huge. There are hundreds of thousands of unfilled vacancies and billions of euros of losses in GDP. Among the very few female ICT graduates in tech, even fewer enter the tech sector. Among women entrepreneurs, very few are web entrepreneurs. This lack of diversity is a major concern for European policy makers and employers alike.
- The Commission is determined to tackle the digital gender gap - specifically by supporting the Coalition for Digital Skills and Jobs – a platform for industry for upskilling in tech and by leading Code Week, during which hundreds of thousands of boys and girls

across Europe participate in coding classes. Also, special EU- funded platforms for women entrepreneurs help to connect, exchange expertise and get access to finance

- Women can thrive in digital careers and clearly diversity is an asset. It would be interesting to learn what actions IBM is planning to bring more women in the sector, help them to stay on the job and progress. Also, importantly, what were the lessons learnt.

## **BACKGROUND**

The deep asymmetries in the tech sector are very persistent. In the **European Union**, only 30% of the around 7 million people working in the information and communication (ICT) sector are women. They are under-represented at all levels in the ICT sector, especially in decision-making positions. The ICT sector is rapidly growing, creating around 120 000 new jobs every year. Due to differences in demands and skills – and despite soaring unemployment – there may be a lack of 900 000 skilled ICT workers in 2020.

A Commission study on women active in the ICT sector published in October 2013, found that allowing more women to enter the digital jobs market can create an annual € 9 billion GDP boost in the EU area (current figures are close to € 14 billion in GDP). A policy change is needed particularly because of an alarming drop in ICT female graduates (today only 29 out of every 1000 female graduates have a computing or equivalent) and very few of them actually work in tech professions.

### **Diversity in workplace is appreciated in ICT companies:**

The world's largest IT developers' community, StackOverflow, carries out annual surveys among its members. The report shows that diversity is a very important matter for IT developers, 73% of them underline diversity in the workplace like at least somewhat important. . Secondly, women who work in tech sector are as happy with their jobs as their male colleagues. Moreover, 75% of coders report to be satisfied with their job, and females are slightly more satisfied than men.

**PRESIDENT JEAN-CLAUDE JUNCKER'S State of the Union Address 2017**

Fourth priority for the year ahead: I want us to better protect Europeans in the digital age.

Over the past years, we have made marked progress in keeping Europeans safe online. New rules, put forward by the Commission, will protect our intellectual property, our cultural diversity and our personal data. We have stepped up the fight against terrorist propaganda and radicalisation online. But Europe is still not well equipped when it comes to cyber-attacks.

Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. Last year alone there were more than 4,000 ransomware attacks per day and 80% of European companies experienced at least one cyber-security incident.

Cyber-attacks know no borders and no one is immune. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks.

## ENCRYPTION

### LTT/Speaking points

- The Commission will present the results of the reflection process on the role of encryption in criminal investigations to the Parliament and the Council by October 2017, where relevant accompanied by actions.
- The Commission is grateful for the participation of industry (and this includes nearly all major US companies with a presence in Europe) in the roundtable meetings the Commission organised in relation to the EU Internet Forum on the role of encryption in criminal investigations and for all other input (position papers) received from the companies.
- The Commission is currently not planning on proposing legislation.

### Background

At the 8<sup>th</sup> and 9<sup>th</sup> December 2016 JHA Council meeting, Member States discussed the role of encryption in criminal investigations and called on the Commission to facilitate further discussions and to consider appropriate actions.

The Commission set up a process to engage with relevant stakeholders, establish a problem definition, and assess options on the role of encryption in criminal investigations. The Commission collaborated with EU agencies (Europol, Eurojust, ENISA, and FRA) to assess technical and legal aspects of the role of encryption in criminal investigations.

In the June 2017 progress report on the implementation of the Security Union, the Commission committed to presenting results of the process to the Parliament and the Council by October 2017.

Preliminary results of the process appear to indicate that there is a need to support capabilities of law enforcement and judicial authorities at European and national to address the use of encryption by criminals. Possible options for action will be discussed at an expert meeting with Member States on 18 September 2017.

### Defensive points

***Will the Commission present legislation that defines new obligations for companies that take into account encryption?***

- Following the December 2016 Justice and Home Affairs Council meeting, the Commission is considering the role of encryption in criminal investigations. The Commission currently is not planning to propose legislation. The Commission is nevertheless considering all appropriate policy options.

***Will the Commission mandate the use of backdoors in encryption tools?***

- The Commission acknowledges that banning, limiting, or weakening encryption could have a detrimental effect on cybersecurity and privacy that should be considered carefully when law enforcement authorities aim to address the use of encryption by criminals as part of criminal investigations.

***Will the Commission consider measures for intelligence services to address the use of encryption by terrorists?***

- Following the call from the December 2016 Justice and Home Affairs Council, the Commission is considering the role of encryption in criminal investigations. This concerns measures that law enforcement agencies and judicial authorities can apply on the basis of criminal law at international, European, or national level and does not cover measures or activities of other organisations, e.g. in the context of the protection of national security or intelligence surveillance, which do not fall within the scope of the competences of the European Union as provided by the Treaties.
- 