POSITION PAPER

BUSINESSEUROPE

29/11/19

Review of the General Data Protection Regulation (GDPR)

KEY MESSAGES

1. Revising the GDPR after only 2 years of application is premature as its impact is still being fully understood.
2. National Data Protection Authorities (DPAs) and the European Data Protection Board (EDPB) should cooperate to ensure consistent decision-making truly enable a single set of European data protection rules.
3. Member States should reduce or refrain from utilising opening clauses that diverge from achieving harmonisation.
4. As innovation should be permitted to thrive under the GDPR, a closer Commission review on the extent of its impact on use of certain technologies and tech-neutrality should take place.
5. The Commission should carry out public consultations to introduce various standard contractual clauses on a number of issues businesses, particularly SMEs find difficult to apply.
6. DPAs should ensure flexible application of all legal data processing methods in any situation and not edge towards prioritising one method in practice.
7. The Commission, Parliament and Council should achieve its intentions of fully aligning ePrivacy with the GDPR otherwise creation of an overlapping and contradicting track of privacy law will throw the GDPR application into contention along with its global influence.
8. The EDPB should offer guidance on the use of grace periods in the event of termination of existing international data flow tools (eg. adequacy or standard contractual clauses).

BUSINESSEUROPE a.i.s.b.l.
AVENUE DE CORTENBERGH 168 – BE 1000 BRUSSELS – BELGIUM
TEL +32 (0)2 237 65 11 – FAX +32 (0)2 231 14 45 – E-MAIL main@businesseurope.eu
WWW.BUSINESSEUROPE.EU – Follow us on Twitter @BUSINESSEUROPE
EU Transparency register 3978240953-79

BUSINESSEUROPE

POSITION PAPER

REVIEW OF THE GENERAL DATA PROTECTION REGULATION (GDPR)

CONTEXT

The General Data Protection Regulation (GDPR) was proposed in 2012. It aims to harmonise data protection rules across the EU as well as give greater protection rights and control to individuals. 3 years of negotiations took place before it was agreed in 2015. This was published in the Official Journal of the EU in 2016. It represents the largest change in data privacy law in the last 20 years. 2 years then passed in order to prepare for its application which took place on 25 May 2018. It will shape how the personal data of European individuals is processed. It also has extra-territorial scope so will also apply to those outside of Europe targeting individuals in the EU.

Article 97 of the GDPR, states that the Commission must submit a report on the evaluation and review of the Regulation by 25 May 2020 (two years after coming into effect). In particular, the Commission should examine 3rd country data transfers under Chapter V and cooperation and consistency under Chapter VII. If necessary, the Commission could submit proposals to amend any part of the Regulation based on this review, particularly in light of new developments in technology and its progress in the information society.

Many businesses have experienced the sea-change in privacy law that is the GDPR. It continues to impact many sectors as the attractiveness and functionality of a greater number of products and services rely on the ability to process the personal data of individuals. Businesses prepared as best they could to be fully compliant with the GDPR by the time it came into force. Many continue to learn, just as data protection authorities (DPAs), the finer details of the GDPR and exactly how it relates to their situation. What is clear is that a great number of businesses understand its importance.

The GDPR is also becoming a competitive enabler for Europe as other regions are influenced by it and follow its principles. Privacy protection is fast becoming a major aspect of how consumers view a business. BusinessEurope aims to uphold the GDPR as an important standard for privacy protection. At the same time, we recognise that it could limit the potential for Europe to lead in the global race of future strategic technologies, such as Artificial Intelligence (AI) or blockchain, particularly if applied in a formalistic rather than strategic manner. Our data economy needs to offer citizens protection while permitting businesses to use it to its full potential to enable great technological leaps forward.

That is why this current review and the views of businesses on the ground implementing the GDPR are so important. While some SMEs have struggled to understand the GDPR the information conveyed in this paper represents all size businesses, from a variety of sectors and regions.

Businesses have just invested great time and resources in implementing the GDPR. Opening it up at this stage could cause confusion and extra investment in adjusting to rules that are currently being fully understood. Any adjustments at this point should concentrate on simplification and be voluntary to implement.

We agree that cooperation between businesses with the Commission, the European Data Protection Board (EDPB) Member States and national DPA's is beneficial in enabling Europe to progress along the GDPR learning curve. That is why

BusinessEurope welcomes this review and encourages all parties to build on this cooperation in order to improve application of the GDPR and uphold its success as Europe's digital economy develops. Exchanges of experience between different stakeholders and meaningful consultation processes to develop guidance documents can aid this.

HARMONISATION

A main goal of the GDPR that was supported by the business community since its draft proposal was the initiative to harmonise data protection laws and practices across Europe in favour of the single market. This would make businesses more efficient, create new cross border opportunities and enable all Europeans similar product and service experiences.

Yet not all Member States have fully updated their national laws or still diverge in certain areas. This means that inefficacy for businesses delivering products and services across borders remain. A business wanting to scale up and sell cross border has to do a lot of research before determining their investment. Often there is so much uncertainty that they give up. This divergence also is apparent in relation to use of the one-stop-shop and consistency mechanism.

The lack of harmonisation is partially due to the large number of opening clauses. For example, Article 10 in relation to the possibility of processing of personal data relating to criminal convictions and offences differs across Member States. This means that some businesses in certain jurisdictions can easily do background checks in relation to signing export agreements with other nations while others cannot. This also effects the abilities of employee's whistleblowing within their organisations and externally regarding others. However, more predominantly, even where the GDPR is fully harmonised, DPAs continue to take unilateral action on the basis of their own views where topics are cross-border in reality. Interpretation is based on pre-existing and differing historical frameworks.

Some of the EDPB guidelines that have been drawn up are useful to enable greater harmonisation but often go further than the spirit of the GDPR or have left outstanding questions. As a result, many national DPAs or regional supervisory authorities answered these questions through their own heterogeneous, sometimes conflicting, national or regional guidance and recommendations. Some businesses felt that such guidance and recommendations provided public and private actors with more concrete information (eg. concrete information about how to appoint an internal Data Protection officer (DPO) without a conflict of interest). While this is practical in the first instance and for the predominant amount of companies who are not operating across the single market it hardly opens up opportunities for harmonisation and single market values for the future. At the same time, national or regional guidance cannot always be fully relied upon due to legally uncertain and general caveats stating: "subject to a future, possibly deviating, interpretation by the EDPB".

Voluntary standards are used by businesses in a variety of policy fields to demonstrate compliance with regulation. Certification can aid demonstration of this compliance. Demonstration of accountability aids authority and consumer trust in a number of sectors

as a result. It is also useful for managing third-party risks, making it simpler for companies to ensure their providers are GDPR compliant. As more products and services are connected it will be important that trust is upheld. While Article 42 of the GDPR enables Member States to support their own mechanisms to demonstrate compliance and encourages them to do so at Union level, we are concerned by movements being made at national level. This will frustrate harmonisation further. An SME applying for a certification does not want to have to do it in every jurisdiction in which it operates. If the GDPR is a harmonising instrument then the standards and certifications used to prove its compliance should also be.

As the GDPR continues to influence privacy discussions globally more and more jurisdictions are passing Regulation that is modelled upon it. This presents a greater challenge in that our global competitiveness in the data economy will rely on our ability to seamlessly offer goods and services while complying with a variety of privacy frameworks. While no one size fits all standard and certification scheme could apply to such complex laws, it is clear that fundamental elements in privacy law are being applied in various jurisdictions across the globe. Business of all sizes require standards and certification procedures that can uphold these elements and internationally cross jurisdictions, they should evolve overtime to continuously improve data protection as technology and its use develops.

Improvements:

- We encourage DPAs to rely on the EDPB appropriately to ensure harmonised decision-making takes place in the spirit of the GDPR.
- Eventually, Member States should reduce the large number of opening clauses to achieve harmonisation to allow companies operating across border to establish uniform processes and standards.
- A greater effort to re-draft and draft further EDPB guidance on the basis of full stakeholder and Member State consultation is required, notably in the following areas:
    - The scope and limits of data subjects' rights of access, including portability;
    - The implementation of information obligations;
    - A more precise definition of open terms such as "large scale" and other criteria for high-risk processing operations;
    - Consistent approach to breach notification, and
    - The scope, limits and development requirements for joint controllers to manage the arrangement between them (Article 26) – particularly as existing national guidance conflicts (UK & Germany).
- Member States should recognise appropriate international standards and certification mechanisms to demonstrate GDPR compliance at European level including enhanced frameworks for certification and privacy seals.
- A consistent approach to the use of sensitive personal data for scientific research purposes (Article 9.2.j.).

INNOVATION

While privacy will always be fundamentally upheld by businesses the GDPR should also enable innovation to thrive under its new rules. While it is driving innovation in general in terms of data management it is leading to challenges with regard to business models. Businesses have experienced that some useful technologies coming to market that would aid the societies they work in cannot derive their full benefits or need drastic adjustment under the GDPR:

> Biometrics: the GDPR should provide a more flexible framework for the processing of biometric data in legitimate instances, at the same time keeping the strictness of data security and transparency requirements. For example, entrance authorisation through retina scans for employees of a server farm are difficult to handle in practice whilst being an example of a use case where enhanced user access authentication also has data security implications. Brick and motar stores are moving towards facial recognition to determine user preferences or specifications to buy products, hampering these technologies will not aid Europe to compete in B2C market realities and demands.
>
> Automated decision making: Article 22 has been interpreted as a general prohibition, subject to stringent exemptions in relation to automated decision-making processes that have similar or legal effects on individuals. Legal uncertainty also surrounds the existing derogations included due to its existing narrow interpretation. This could hamper Europe's ambitions to lead in development and roll-out of AI solutions involving the processing of personal data and also impact efficiencies related to automated decision making (subject to appropriate safeguards).

Improvements:

- The Commission should review the extent of how GDPR application is indirectly hampering the use of certain technologies and in the interests of tech-neutrality, deliver solutions on how innovation can indeed thrive.
- The EDPB should review the impact of the Automated individual decision-making and Profiling Guidelines (in relation to Article 22).
- Simplification of data subject information and potential use of standardised icons.

SMEs

Complying with the GDPR has been a huge task and investment for larger companies (eg. deploying more people and changing operations) but for SMEs, fully understanding and complying with the GDPR has been almost impossible, particularly for those companies that do not take part in high-risk or mass data processing. At the same time, SMEs want to remain just as compliant as larger companies so many have taken a "better safe than sorry" approach leading to administrative burdens and costly processes that are perhaps disproportionate to the intentions of the GDPR. For example: data processing agreements are drawn up simply as an insurance and are perhaps not required; maximum time is spent on breach reporting and individuals are being asked for permission to use their data even if not necessary. These overzealous actions from

SMEs are not only to be compliant at fear of DPA retribution, or lack of information/guidance, but also because finding out an answer to these questions often takes even longer than actually carrying out the action itself.

Data controllers are responsible for the processing of personal data that they carry out under the GDPR. As a result, they need to document, in order to demonstrate, that their activities are compliant. Businesses may also have to appoint a data protection officer. While this represents a great investment for larger businesses to appoint and train employees, SMEs face even greater concerns. They usually have difficulties in defining whether their compliance actions are scalable or not. Against this background, a lack of internal rescources with sufficient technical expertise has led to a higher cost for enterprises, particularly for SMEs, and diverging views in the market as a direct result of a large number of different authoritative voices having surfaced in the implementation discussion surrounding the GDPR.

While some SME exemptions already exist for recording of processing activities, they have found to be non-actionable in practice. We welcome the idea of attempting to make things easier for SMEs. However, the restrictions on the application of this exception contained in Article 30(5) are so far-reaching that in practice they prevent SMEs employing workers from applying it. This cannot be the purpose of such a derogation. This problem is worsened by the rigorous interpretation of the term “processing of personal data is not occasional” by the EDPB in relation to paying a salary.

SMEs also find it difficult to define an appropriate basis for legal processing. They find it difficult to understand when alternative legal basis other than consent can be used. In practice, SMEs have been using consent as a legal basis to process contracts and legal obligations alone. Many do not realise that they do not need to ask for consent if they process data to perform legal obligations/contracts.

The introduction of standard contractual clauses would be very helpful for SMEs and business in general. For example, the GDPR indicates that the data processor can only be an external entity whereas various pre-existing pieces of national legislation allowed this entity to be internal. Businesses had to reconfigure many contracts and roles accordingly. The induction of various standard contractual clauses would make relationships between SMEs (as controllers) and larger businesses (as processors) more manageable. It could also help shorten discussions during negotiations. In the case of standard contractual clauses in accordance with Article 28(7), it must be ensured that they are suitable for both higher risk processing and lower risk processing. Otherwise low risk processing would have to meet the same requirements as higher risk processing. This would create further administrative burdens.

Improvements:

- Member States should allocate greater funds to their DPA’s in order for them to answer a greater number of businesses questions.
- The EDPB should revise their reading of Art 30(5) to not include salary payments as occasional data processing for the meaning of this particular SME carve out.
- Consider flexible application under Art 30(5) exemption by weighting the condition of “a risk for the freedoms of the data subject” higher than “occasional” to it should be applicable in practice.
- Consider reporting carve-outs for SMEs that do not process high-risk data.

- Consult and introduce standard contractual clauses on a number of issues SMEs and businesses in general find difficult to manage. They should include different clauses depending on the risk and scope of the task. In particular, obligations related to the cooperation between controllers and processors, especially in case of data breaches and the allocation of responsibility, should be more clearly specified.
- Uniform and recognised voluntary international certifications for providers of software and cloud solutions should be developed in order to allow companies using those services, and in particular SMEs, to assure themselves of GDPR compliance.

DATA PROCESSING

Processing of personal data under Article 6 of the GDPR offers companies various legal grounds in practice. These can be used alone or sometimes together. However, they should not be interpreted so strictly so that one legal method is favoured. If the GDPR favours innovation it should treat all methods equally in practice.

EDPB guidance in relation to performance of a contract under Article 6(1)(b) of the GDPR in the context of online services is not flexible enough to deal with new technological developments or business models. While a clear difference between the contract itself and the individual's personal data can be made in the physical world, the online world involves immediate generation and logging of data with every action. This is often needed to actually deliver the service itself. The complexity of where we are heading through technology should be taken into account in Article 6 of the GDPR otherwise, certain processes will not be permitted leaving European society at a loss of innovative solutions as a result.

Due to the risk of withdrawal of the consent at any time, consent as a legal basis is avoided as far as possible. It should be made clear that in the event of a withdrawal, data processing may also be based on another alternative legal basis.

Moreover, the conditions under Article 10 for processing of personal data relating to criminal convictions and offences cause problems for whistleblowing systems. Under the current framework whistleblowing on external players such as trade partners is not possible. More coherence is also needed in Article 9 in relation to special categories of personal data in order to achieve a comprehensive and predictable framework for healthcare and other specialist fields.

Improvements:

- DPAs should ensure a flexible enough application in practice of all legal data processing methods in any technological situation and not edge towards prioritising one method in practice as the only possibility.

DATA BREACHES

Businesses understand the importance of reacting to a data breach. Not only to comply with the GDPR but also to save their own reputational loss and regain trust. A part of this

is filling in data breach forms in order to notify the national (lead) DPA of the occurrence. Great investments have been made by businesses to ensure that incident management processes are in place in order to carry out such tasks if needed. This also requires continuous training of staff. However, what is not understood by the business community is why these national forms differ across the Member States. If the GDPR attempts to harmonise privacy rules and the Commission supports single market principles requiring businesses that operate across borders to fill in different form types seems an unnecessary burden for all stakeholders. More guidance is needed at EDPB level to ensure a consistent understanding of breach notification criteria as well as best practices in terms of notifying data subjects of data breaches. This is particularly important in the context of the changing landscape of cybersecurity threats, with external actors exploiting vulnerabilities at the data subject level.

Improvements:

- A European standard data breach notification form and guidance should substitute existing national forms. More EDPB guidance would be advisable to address open questions in terms of timeline for notifying breaches, standards for informing individuals and remediation.
- Permit English as a working secondary language to all authorities to report breaches.

THE ACCOUNTABILITY PRINCIPLE

Data controllers and processors are fulfilling their role of upholding accountability through ensuring their processing activities are in line with the GDPR and documenting them to demonstrate this. Some businesses have also had to appoint a DPO for far reaching data processing activities. Although the DPO registration forms and required data sets differ across the Member States. The requirements to appoint a DPO lead to considerable administration placing burdens on companies, particularly where the content and scope of information required isn't relevant for the predominant amount of companies where their core activity isn't processing vast amounts of personal data. As a result, the exemption under Article 13(4) is often useless in practice.

While the risk-based approach is welcome the list of criteria for when a data protection impact assessment has to be carried out is broad and therefore is often applied in full. There are currently disparities in the understanding of the criteria triggering the obligation to complete a DPIA. For instance, some regulators have suggested that any processing operations involving international transfers of personal data or any processing operation involving processing of personal data of employees as vulnerable subjects requires the completion of the DPIA. This appears excessive and not aligned with the risk-based approach as it would make every Data Controller fall into the requirement of completion of DPIAs for the vast majority of processing operations.

In view of the lack of harmonised understanding of high-risk processing activities, a considerable amount of documentation and efforts is dedicated to processing activities with medium or low risk, diverting resources from addressing the true impact of high-risk processing activities and placing a large bureaucratic burden on companies.

Improvements:

- Uniform and pragmatic guidelines regarding the implementation of the Accountability Principle in enforcement decisions and what is the criteria for 'high risk processing of personal data' to understand what DPIA documentation obligations are required. Alternatively, the EDPB could publish and keep updated, a living list of operations where a DPIA is not generally required by a DPA.
- To facilitate compliance, a self-evaluation toolbox could be developed to help businesses, in particular SMEs, assess and plan their compliance. Moreover, further support should be given through EU funded projects which aim to support investments in internal training, in particular for SMEs.[1]
- Information obligations should not apply where processing is carried out for a specific purpose at the request of the subject. Requirements should also not apply to processing between undertakings.
- Guidelines and recommendations of the tasks and position of the DPO.

CODES OF CONDUCT

Before the GDPR came into force many business organisations drew up sectoral codes of conduct to aid guidance of privacy rules to their specific situation. This aided understanding and business compliance. However, the GDPR seems to discourage privacy codes of conduct. It states that drafters of such documents must also establish a supervisor to enforce the code. They should also be fined if they do not enforce it properly. But the process for attaining approval for an EU Code of Conduct is complex, with the conditions/requirements unclear. As a result, sectoral organisations have been put off carrying out these drafting practices for the businesses that once relied upon them. Codes of conduct were used as soft law only to aid company compliance they should never supersede the GDPR. Therefore, blatant flagrancy will always be possible to penalise in practice.

Improvements:

- The requirement of a compulsory supervisor to oversee and enforce sectoral codes of conduct should be withdrawn.
- The Commission should follow up supporting its idea of a GDPR toolbox for businesses to facilitate compliance, including standard contractual clauses and codes of conduct.

THE EMPLOYMENT CONTEXT

Data protection rules also apply in the employer-employee relationship as while businesses must process data of their employees during the context of their work this must be proportionate and not infringe upon their rights.

Yet we have already seen that data subjects' rights are being used in this context to build up pressure on their employers in existing judicial disputes. Enquiries relating to data access are often based on irrelevant considerations. Unfounded requests frequently occur in the context of contractual disputes rather than in the context of data protection

[1] See for example the EU funded SMEDATA Project which aims to help SMEs and their legal advisors effectively apply the GDPR provisions.

disputes. In case of dismissals, more and more employees are using Article 15 to gather information for a court proceeding against their former employer.

Consent in relation to this specific relationship is difficult to determine as if used as a legal basis it must be "freely given". This can hardly be proved in practice if an employee's job relies upon the employer processing their data, even for other legal requirements. Due to the contractual obligation on the one hand and the voluntariness/ revocability of consent on the other, there is legal uncertainty with regard to the fulfilment of a contract. This is particularly evident in the interaction with Article 9 where consent is required for processing sensitive data.

Improvements:

- Specific data access rights should only have to be provided to the employee if they have no access already. They should be required to specify which information and processing the request relates to.
- A basic list of what access rights should include (and not include by default) related to employees could be issued as a guidance.
- Processing of special categories of data should, in individual cases, also fall under the legal basis for the protection of legitimate interests.
- A clarification is also needed that Article 15(3) does not require copies of all documents containing personal data in general.

ALIGNMENT WITH OTHER LEGISLATION

In the interest of better regulation BusinessEurope has always supported the notion of understanding the legal and practical impact of rules within an entire legal framework. While the GDPR provides a high standard of privacy, Europe must also ensure compatibility with other privacy regimes across the globe and not begin contradicting initiatives that would throw this into disrepute.

The EU's privacy framework should also work together simply for businesses on the ground attempting to deliver solutions in an efficient and attractive way. Businesses must also have legally certain conditions to process data. Yet future initiatives, such as the ongoing ePrivacy debate does little to help in this regard. While some Commission non-papers have circulated in an attempt to explain that ePrivacy will not impact the GDPR businesses actually delivering solutions on the ground and attempting to be fully complaint with both laws are not convinced.

The ePrivacy proposal and ongoing debate contradicts the GDPR at a time when companies are just getting to grips with the GDPR itself. It limits the full legal processing abilities of the GDPR denying its full use for companies in practice. In most cases the ePrivacy Regulation would supersede the GDPR. Otherwise, many businesses remain confused as to when only consent would be possible to legally process data (under ePrivacy) or the full possibilities of the GDPR. As a result, many businesses are gearing up to prioritise consent. But this also represents problems as the type of consent in the ePrivacy proposal is different to that of the GDPR (requiring proof that anonymous action does not work, impact assessments, consultation with authorities and a yearly reminder to users that it can be removed).

Improvements:

- The ePrivacy proposal should achieve its intentions of aligning with the GDPR and not create a separate track of privacy law that will throw this whole EU policy framework into contention. If not completely removed, ePrivacy should only cover matters not covered by GDPR eg. in support of confidentiality of communications.

INTERNATIONAL DATA TRANSFERS

The GDPR recognises the importance of international data transfers to enable Europe to compete in the global digital economy. It is clear that as our economy becomes fully digitalised, international trade in goods and services will rely upon the ability for data to cross international borders.

Under Article 45, an adequacy decision can be sought by a 3rd country and the EU to enable data to flow without any further safeguards. While the EU has a number of these with 3rd countries they take some years to complete and can be struck down at any moment. This has left companies that rely on them concerned in the past when their existence is called into question. For example, while the Privacy Shield is a living instrument that needs review and potential updating, if a full overhaul is carried out, appropriate grace periods should be granted in order for international business to continue until more appropriate framework can be agreed by legislators. If this cannot be guaranteed then nor will business investment, to the detriment of European competitiveness and jobs.

A number of other mechanisms are included within Article 46 that enable data to flow internationally, such as the use of standard data protection clauses. The Commission drafts standard clauses to use in contracts between controllers or controller to processor to enable data to flow across international borders. These are perhaps the most important, at least highly used form of international data transfer safeguard that businesses utilise. That is because they are relatively quick and easy to use, they relate to any country (not just those with adequacy decisions) and can handle multi-party situations and different risks of data. SMEs willing to sell up and go global find them useful to use as a result. At the same time, they cannot be modified quick enough to keep up with the state of global technology or business models. For example, processors often use another organisation (sub-processor) in its operations, yet the current clauses supported by the Commission are not fit for this purpose.

Improvements:

- The Commission could establish updated Standard Clauses under Article 46 for (i) Controller-Controller SCC, (ii) Controller-Processor SCC and make these ones fit for the Processor-sub-processor relationship, giving ample adaptation period to implement them.
- The European Data Protection Board should offer guidance on the use of grace periods in case existing adequacy decisions are struck down or updated.