BUSINESSEUROPE

COMMENTS

6 February 2017

COMPLYING WITH THE GENERAL DATA PROTECTION REGULATION (GDPR) IN PRACTICE

BusinessEurope welcomes the opportunity to feed into the debate on the implementation of the General Data Protection Regulation (GDPR).

It is important that stakeholders impacted and responsible for adhering to this new framework are able to give legal and practical feedback on issues emerging on the ground as preparations are made for its full application by the Member States.

Issues are beginning to arise due to Member States preparing at different speeds with little or no coordination or consultation. This risks fragmentation whereas a harmonised approach was originally envisaged. Therefore, this exercise is all the more important to stress these issues directly to the Commission for follow-up.

BusinessEurope's overall objectives in the context of the implementation of GDPR are:

- Ensure consistent implementation across the Single market;
- Identify the appearance of inconsistencies, potentially problematic trends, provisions or sections of the regulation that prove particularly critical for Member States in the concrete application;
- Overall, ensure an implementation which is as business friendly as possible and avoid any kind of interpretation or application that is not sufficiently balanced;

We believe the Commission has a key role to play to coordinate implementation phase, encourage dialogue – or if necessary even impose it, create peer pressure and urge Member States to justify potential implementation modes that differ from the general approach.

Therefore, the answers below to the first set of questions the Commission released are all the more important to address these aspects as soon as possible in the GDPR implementation.

We look forward to continued dialogue on these matters.

AV. DE CORTENBERGH 168
BE-1000 BRUSSELS
BELGIUM
VAT BE 863 418 279

BUSINESSEUROPE a.i.s.b.l.
WWW.BUSINESSEUROPE.EU
Follow us on Twitter @BUSINESSEUROPE

TEL +32(0)2 237 65 11
FAX +32(0)2 231 14 45
E-MAIL: main@businesseurope.eu
EU Transparency register 3978240953-79

GENERAL QUESTIONS:

Are there specific opportunities and challenges in the GDPR implementation in your sector?

All sectors of business are concerned that the original intention of applying a single set of data protection rules will not be achieved by the GDPR. It is clear that the final text leaves too much room for manoeuvre by the Member States and their Data Protection Authorities. This presents a challenge to its original intentions of harmonising data protection rules as in fact, fragmented rules will be applied in practice. The GDPR contains approximately 30 provisions where MS can legislate to determine vague provisions at national level (eg. consent and processing a child's data, special rules for certain organisations, profiling and specific processing situations)

While we welcome the initiative of Article 29 Data Protection Working Party (WP 29) to draft Guidelines and incorporate stakeholders in the process, practically it is difficult to prepare to comply as the Guidelines will not be issued until a later stage. Whereas investment in preparing to comply and organisation needs to take place now to meet the May 2018 deadline. This is also hindering new business opportunities from developing as they will be put on hold until the GDPR is fully understood and applied in practice.

For sectors relying on research and innovation, overly restrictive measures with regards to research and the alignment of the new regime with certain sectors are all challenges presented by the GDPR. Particularly those processing of data for research purposes. The implementation of these provisions will impact abilities to advance concepts such as personalised products and services and real-world data to enhance sustainability.

The one-stop shop needs to be realised in a meaningful fashion, through close coordination and cooperation in EDPB to ensure the consistency mechanism works in practice. We welcome setting up of the European Data Protection Bureau (EDPB) as a single point of contact to ensure cooperation among national data protection authorities. However, transparent detail is needed on the scope, budget and regulation of this independent body.

Is your organisation cooperating with others in this process and sharing best practices?

Although Member States are moving at different speeds, many of our national member federations and their company members are cooperating through ad-hoc working groups. Some attempt to include Member States' authorities in order to shape national application. This is often to actually interpret the GDPR rather than to share best practices. Some are organised cross-sectorally others sectorally. Overall it is difficult to see how best practices will be coordinated and by which regulators (eg. recent case in Bavaria regarding when a conflict of interest arises for a DPO).

What is your experience in cooperating with your data protection authority in that regard?

We welcome the ability to give input on Guidelines with regard to the WP 29. While respecting the independence of those DPAs we stress the importance of comprehensive interaction with business stakeholders who will apply the new GDPR in practice. For example, short deadlines to provide feedback on the Guidelines will not enable business to be the most useful stakeholder it could be in the WP 29 drafting process.

As the situation may differ with each Member State authority it is difficult to give a comprehensive answer. Those that had kept near on daily contact with DPAs agree that creating trust between the business and the DPA is important. Long response times are however common. This could be due to a lack of resources to deal with sector specific issues given the broader responsibilities of the DPA in relation to application of the GDPR. Some members have taken part in working groups set up by DPAs to carry out privacy impact assessments. Too little resources in some Member States make interpreting the GDPR difficult. As a result, companies, will try to interpret the GDPR individually and invest costs in consultants and IT developers. Few companies will be able to adapt without investing vast resources in redrafting privacy policies, data protection process documents and asking for legal support.

At the national level, cooperation with governments and their ministries is also important. At the European level, DG JUST maintains a national group of experts which is steered towards implementing a harmonised GDPR. Yet this body needs to transform from a mere forum of information exchange to a real GDPR coordination body.

SPECIFIC QUESTIONS:

How is your organisation dealing with the requirements of transparency?

Although the GDPR presents increasing demands in terms of the sheer extent of information that now needs to be provided, Businesses are preparing to remain compliant with transparency requirements. This includes techniques to share data through anonymised or pseudonymised means to support transparency and balance privacy rights of individuals. Businesses will also ensure that these requirements do not lead to over-information for customers.

Does your organization have a comprehensive privacy management program? If not: Do you currently work on one? In the case you have one - which changes/adjustments require most work on your side?

While many companies already have privacy management programmes that will be adapted for the new GDPR regime, legal clarity on privacy by design is needed to determine what constitutes compliance and non-compliance in software and data processing services. Practically, this will then include strengthening safeguards and governance to prepare for privacy by design and privacy impact assessments. The availability of technology to deal with the high degree of automated procedures is lacking in some sectors.

How are you adjusting to the change of the rules concerning the controller-processor relationship? Are you revising your contracts with your processor/processors?

EU standard contractual clauses are examples of instruments being used for existing contracts running over May 2018 to reach new GDPR criteria. This also includes more challenging changes to the actual technology processing data. In addition, uncertainty surrounds secondary legislation in relation to the GDPR with regard to local security requirements.

What is your experience concerning data breach notifications so far? How do you adjust to the new rules?

The awareness and experience of data breaches should increase through the new GDPR regime. It is important that notifications are not simply stored but made useful for businesses and authorities. Businesses should receive a receipt for their notification along with statistics (eg. frequency of data breaches and cyber-attacks in similar sectors). The definition of high risk processing is so vague it could be attributed to any kind of processing. This sets burdensome notification obligations and uncertainty that will cause delays in the smooth reporting of data breaches.

Are you processing on the basis of consent? Are you changing/adjusting the way you get consent so as to ensure that it will comply with the new rules?

Yes. This consent must be customer focused and not result in confusion or mistrust. The concept of consent by layers can be useful here as customers and businesses fully understand the processing and can require additional information if necessary.

Which mechanism do you use for your international transfers? Do you see any need to adapt the tools you are using or to develop new tools in light of conditions/requirements of your specific industry, business model and/or type of processing operations involved?

Mechanisms are being updated in order to be fully compliant with the GDPR (standard contractual clauses, adequacy decisions and privacy shield). As an alternative data transfer mechanism, standards contractual clauses can be useful however, the EU-US Privacy Shield itself represents a significant improvement on its predecessor and is an important achievement for privacy rights and companies across all industries. As thousands of companies are already certified and many more are pending, it is a testament to companies' preferential choice when transferring data across the Atlantic. This also demonstrates that the Privacy Shield has been well received. The Privacy Shield is fast becoming a critical part of transatlantic trade.

* * *