European DIGITAL SME Alliance

10 June 2020

General Data Protection Regulation (GDPR) Two-Year Review: Clear guidance for SMEs and stronger European-minded Data Protection Authorities (DPAs)

Position paper

Background

The General Data Protection Regulation (GDPR) came into force in May 2018. Two years after, the GDPR can be considered the most ambitious piece of legislation when it comes to data protection on the globe and it has inspired data protection rules around the world.

At the same time, a harmonised European legal space in terms of data protection is still in the making. This has to do with the nature of the GDPR, which is rather non-specific and open to interpretation, and also the capability of the data protection authorities (DPAs) to enforce the rules and act in the spirit of the GDPR. The capability of the DPAs to fulfil their roles depends on national circumstances (i.e. how they are equipped in terms of resources and staff). At the same time, there seems to be a stronger need for European coordination and oversight. Further, while the GDPR gave individuals more rights and provided a general framework for data protection in the EU, it failed to substantially change the behaviour of big tech companies that exploit personal data as their business model. Concurrently, the GDPR's one-size-fits all approach and openness to interpretation puts burdens on smaller companies, which need to rely on expensive legal advice or consulting to make sure they are compliant.

As an organisation representing European small and medium enterprises (SMEs) in the digital sector, we welcome clear and uniform rules which set the ground for a harmonised digital single market that allows companies, especially smaller ones, to operate and innovate in legal clarity across EU internal borders and beyond. In light of the two-year review of the GDPR, European DIGITAL SME Alliance has consulted its members to define critical areas where the GDPR can be improved. We recommend focussing on three areas:

1.) Increasing legal certainty for SMEs and working towards incentives for privacy-based innovation.
2.) Application of the GDPR must be uniform across Europe and needs strong European-minded DPAs and European oversight.
3.) Making sure the GDPR does not hinder innovation.

+32 2893 0235
VAT: BE0899786252
https://digitalsme.eu
office@digitalsme.eu
123 Rue du Commerce, 1000 Brussels, Belgium
EU Transparency Reg.: 082698126468-52

The following are our recommendations for improving enforcement, application and to make sure the GDPR supports a sustainable digital economy:

1. Increasing legal certainty for SMEs and working towards incentives for privacy-based innovation.

a. Legal certainty & burdens on SMEs

The GDPR is often considered as abstract and broad, leaving room for interpretation. **Aspects related to legal uncertainty and interpretation constitute a problem especially for SMEs**, which do not have the internal resources and expertise to deal with the challenges arising from legal interpretation of the GDPR. Many SMEs need to rely on external legal consultations to ensure that they are GDPR compliant, which constitutes additional costs for them. SMEs struggle to find clear guidance in the GDPR itself.

Furthermore, **formal aspects of the regulation**, such as documentation requirements, **can constitute additional burdens**, and may slow down processes due to high levels of bureaucracy associated with these requirements. Therefore, there is the **need to provide clear and narrow guidelines on the application of the GDPR** and to supply better guidance on documentation requirements or suitable templates in order to allow SMEs to be fully GDPR-complaint in a sustainable manner. Templates for documentation and guides adapted to various sectors would help small businesses comply without having to rely on expensive legal consultants. Here, the role of the DPAs could be strengthened. According to a recent study less than one third of EU DPAs provide specific guidance to SMEs.[1] Standardisation bodies should be involved in the process to develop better guidance. They have the means and the experts, including SME representatives, to define detailed guidelines on several topics, e.g. security measures to be adopted within the scope of GDPR. In order to reach a uniform application of the GDPR across Europe, the certification mechanism within article 42 should be revised and leveraged in order to allow a proper, widely applicable scheme to emerge. Current discussions on reusing Common Criteria-based approaches or schemes based on ISO 17065 are destined to be only marginally useful.

At the same time, the greatest investment is not directly monetary but is associated with dedicating resources to the role of the data protection officer and internal processes in

[1] STAR II, Deliverable 4.1 Draft versions of the guidance & handbook (version 1.1, 2020)

companies. Especially in smaller organisations, data protection officers often receive the title on top of their pre-existing full-time duties without any reduction to their workload or obligations. As such, they do not have enough time to focus appropriately on data protection topics.

b. Positive effects: Trust of customers

While there is little representative evidence about an increase of customer trust due to conformity with the GDPR, several organisations have noted that GDPR compliance **solidifies pre-existing trust and serves as a positive aspect for continued cooperation**. This is especially true for customers who are conducting audits of partners to make sure they are aligned in terms of data protection. Organisations providing technical solutions in privacy innovation clearly state that the GDPR is critical to their competitiveness. In addition, public opinion of the rules seems to be favourable, and by designing specifications after the GDPR, companies can deliver **technology that is accepted by the public**. This points to a general success of the legal framework. The wider public seems to be generally more aware of possible issues in the area of data protection. This creates incentives towards providers of technology to do well and to have secure systems. The accountability factor is significant since organisations must be able to justify their choices, and relevant processes. This leads to more thought-through and in-depth considerations about data protection in business processes and choices.

At the same time, technology solutions providing superior privacy still do not necessary constitute a competitive edge. Europe may need to think about how to establish privacy as a competitive advantage. Some companies still employ **inferior technologies (from a privacy perspective)** and sometimes seem to lack legitimate interest as a legal basis to justify personal data processing. Businesses, consumer organisations and privacy advocates may tackle these issues by bringing class action lawsuits or complaints against such behaviour. At the same time, these proceedings can be rather slow. Perhaps a **softer and faster initial mechanism would help to create a more privacy-innovation friendly environment. For instance, a mechanism to request a general opinion by a DPA could be introduced. Such a mechanism could help to set the right incentives for companies to really act in the spirit of the GDPR and provide a legal framework that enhances privacy-friendly innovation.**

2. Application of the GDPR must be uniform across Europe and needs strong European-minded DPAs.

As the GDPR has only been in force for two years, there have **been very few opportunities for interpretation in the highest courts**. Only a small number of local courts' interpretations of certain aspects of the GDPR by Data Protection Authorities (DPAs) were issued across Europe. These interpretations may create precedents, but they may be insufficient to answer to different cases or scenarios; sometimes they may even be in conflict with another DPA's interpretation. **Across Europe, DPAs and other supervisory authorities are applying and interpreting the GDPR differently**. This may sometimes even be the case within a single country. For instance, some SMEs in Germany report that the activities, performances, and opinions of the various regional DPAs vary wildly, leading at times to uncertainty regarding the interpretation of the rules. There is no stringent line one can follow and different advices on the same matter are confusing businesses. **Thus, a business can never be fully sure whether it complies with the provisions of the GDPR or not.**

Further, while organisations seek advice from DPAs for certainty, the authorities can often only give directions or recommendations and expose the consequences of possible choices. In the end, they must leave the final decision to the organisation itself, which also bears the legal consequences. In addition, DPAs' responses (e.g. to data-breach notifications) can take a long time, leaving companies in an uncertain situation. In addition, it is sometimes difficult to contact DPAs and get information from them, even if only through the website.

Lastly, there is a significant amount of additional national laws or local specific conditions which can be applicable to data protection. This makes proper implementation a difficult and challenging task.

This lack of unity and harmony poses challenges to companies with limited resources such as SMEs, and to companies working with partners in different regions or countries. Without harmonised interpretation of rules and clear guidance developed on a European level, a business can never be fully sure whether it complies with the provisions of the GDPR or not.

A better coordination, communication, and cooperation across DPAs at European and national level would be desirable in order to ensure a uniform implementation of the GDPR, as well as better alignment of the GDPR with national laws or regulations. Going beyond, there may be a need to not only ensure a "European-mindedness" of national DPAs, but to create a strong European oversight authority.

3. Making sure the GDPR does not hinder innovation

a. A framework for sustainable technological innovation

The GDPR has raised considerable awareness about data-protection risks related to new technologies and what this means for concrete processes in organisations. Though some formalities are difficult to comprehend for organisations that implement new technologies, these organisations are at least aware of the necessity to check the safety of the technologies and to integrate measures to ensure the safety and privacy of personal data. Additionally, organisations are more aware of the necessity to check for alternatives not only from a cost perspective but from a data protection angle. The GDPR seems to have increased a focus on European-based new technologies to prevent data transfers to outside of the EU and EEA. Though it is still often used as a commercial argument rather than a necessity, the GDPR has imposed the protection of personal data as a requirement and a significant element to consider when developing new technologies.

This does not necessarily apply to giant tech companies that hold a quasi-monopoly on the market. These companies have vast legal resources and can thus limit the impact of the GDPR and continue their "business as usual", including questionable practices concerning personal data.

b. A burden to flexibility?

The GDPR is a legal document that took years to be drafted, passed, and implemented. During that time, technologies have kept evolving. The GDPR's broadness allows for room to adjust to new technologies as there are no fixed limits defined to restrict data processing technologies. **As such, its broadness and abstraction are positive aspects which allow it to evolve alongside future technologies and ensure that they are safe and respect human privacy.**

However, **technology will always move faster and further than the laws can reach**. The GDPR slows downs businesses by some very formal requirements, e.g. documentation requirements and the need to update such documentation. These requirements may not match the reality of organisations that wish to improve and innovate constantly. Such fast-paced SMEs and start-ups might be slowed down by the GDPR.

Additionally, the GDPR has been developed with the idea of a human controller. With the continuing development of artificial intelligence (AI), there may be areas in which fewer or no humans are involved. This would no longer correspond to the expected reality of the GDPR as there are no specific rules in the GDPR for data processing activities exclusively managed by AI. Though automated data processing is covered by the GDPR, it may be too broad to include all

future technological developments, especially with regards to AI. The latter will contribute significantly to increasingly automated data processing. The GDPR may not be sufficient as it relies heavily on humans knowing and understanding the expectations in data protection, documentation, and noticing issues which may not be flagged in automated AI systems.

c. A burden to innovation?

Some of the innovative technology frontrunners among DIGITAL SME's membership work with innovative new technologies. The hurdles they face can serve as a useful illustration of burdens to innovation of new technologies in Europe. For instance, when it comes to facial recognition, a large problem that has become apparent is the lack of datasets. Companies in Europe cannot use common facial databases due to the GDPR. This is a huge competitive disadvantage compared to the US, China, Russia, and other countries. Thus, other solutions need to be found. For instance, limited access to passport databases or greater freedom in using online data or similar resources would be essential for Europe to be competitive in this area. Another alternative is greater freedom to use photos and other publicly available resources for research purposes. Otherwise, we may need to increasingly rely on providers of these technologies from abroad.

The GDPR must act as an *enabler* for the development of new technologies. Companies need flexible rules to be able to innovate and experiment with technologies. This is essential for companies that would like to innovate in new technologies. Limited liabilities, e.g. establishing reduced ranges of penalties in dedicated small-scale prototyping and evaluation projects, would be useful to support innovation.

As another possible solution to enhance innovation, emphasis could be put on the implementation of anonymisation and in particular pseudonymisation of personal data, to allow more possibilities for processing of personal data for the purpose of developing and testing innovative digital services. The GDPR, specifically refers to pseudonymisation as a type of processing of personal data in article 4(5), and as a type of personal data in recital 26. Distinct approaches to pseudonymise data have emerged across Europe. These approaches, if combined with appropriate organisational, technological, and legal measures, can lead to data sets that can be considered anonymous data, and therefore could be freely processed.

Conclusion

While the GDPR gave individuals more rights and provided a general framework for data protection in the EU, it failed to change the behaviour of big tech companies that exploit personal data as their business model. Concurrently, the GDPR's one-size-fits all approach and

openness to interpretation puts additional burdens on smaller companies which need to rely on expensive legal advice or consulting to make sure they are compliant.

Therefore, Europe needs to increase legal certainty for SMEs and work towards incentives for privacy-based innovation. We must think about how to make sure that we establish privacy as a competitive advantage. The GDPR has imposed the protection of personal data as a requirement and a significant element to consider when developing new technologies. **This does not necessarily apply to giant tech companies that hold a quasi-monopoly on the market. These companies have vast legal resources and can thus limit the impact of the GDPR and continue their "business as usual", including questionable practices concerning personal data.** This is not in line with the spirit of the GDPR, but at the same time, these questionable practices continue also because DPAs are not in a strong position to fulfil their roles and investigate these practices.

Both these aspects would require a stronger and more coordinated role of DPAs across Europe. Without harmonised interpretation of rules and clear guidance developed on a European level, a business can never be sure whether it complies with the provisions of the GDPR or not. A better coordination, communication, and cooperation across DPAs at European and national level would be desirable in order to ensure a uniform implementation of the GDPR, as well as better alignment of GDPR with national laws or regulations. Going further, there may be a need to not only ensure a "European-mindedness" of national DPAs, but to create a strong European oversight authority.

Stronger national DPAs and a strong European oversight would allow for a better enforcement and clearer interpretation of the rules. In addition, such authorities could act more quickly and in line with the spirit of the GDPR, i.e. also tackle questionable practices that are still happening behind the curtains and will only be limited after long judicial proceedings. For this purpose, perhaps a softer and faster initial mechanism would help to create a more privacy-innovation-friendly environment, i.e. a mechanism such as requesting a general opinion by the DPA, which could help to set the right incentives for companies to really act in the spirit of the GDPR and provide a legal framework that enhances privacy-friendly innovation.

Lastly, we need to make sure that the GDPR does not hinder innovation. The GDPR must act as an *enabler* for the sustainable development of new technologies. At the same time, companies need flexible rules to be able to innovate and experiment with technologies. Thus, there is a need to think about limited liability regimes, sandboxes, or similar mechanisms for companies to innovate.

Main contributing experts/co-authors:

Leonard Johard, CTO at Indivd AB

Sebastian Feik (Dipl. Wirtschaftsjurist), CEO at legitimis GmbH

Cécile Faverdin (LL.M.), Consultant Data Privacy at legitimis GmbH

Eugenio Mantovani, Researcher, VUB

For further information on this position paper, please contact:

Ms. Annika Linck, EU Policy Manager

E-Mail: a.linck@digitalsme.eu