WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

POSITION PAPER

Call for evidence Report on the General Data Protection Regulation (Ref. Ares(2024)182158)

Berlin, 8 February 2024

With the General Data Protection Regulation (GDPR) having been published in 2016 a reporting mechanism has been established, requiring the Commission to evaluate the GDPR every four years. With the GDPR being regarded as a regulatory success by lawmakers across the continent, it is nonetheless necessary to point out several aspects in the GDPR, that require closer observation against the background of events having unfolded during the last four years when the last evaluation took place. Following these learnings eco would like to take the occasion and submit the following comments on the current state of the GDPR and its enforcement.

- **Provisions of GDPR should be proportionate and comprehensible**

While the general principles of the GDPR have proven to be acceptable in weighing interest in data processing through organisations, administration and companies against the necessity to provide privacy to citizens there is still room for improvement regarding the comprehensibility of the quite general provisions in the GDPR. Especially for smaller organisations the GDPR seems to create a threshold for processing data, which may adversely affect their opportunities to grow and be successful in the market. Companies, citizens and organizations need overarching and enabling guidance when navigating data processing in accordance with the GDPR. Specific areas of guidance could include providing additional affirmation that all basis for processing personal data should be treated equally (especially affirming the importance of legitimate interest) and updating the 2014 guidance from the Article 29 working party on the use of anonymous and pseudonymous data.

The requirements of the GDPR and their application should be reviewed with special regard to small and medium sized companies (SME), which are seemingly more adversely affected by new administrative requirements and most importantly above all proportionally far more impacted by them. Reducing complexity for small businesses while maintaining core protections for consumers would help mitigate concerns and improve overall compliance.

- **Sanction mechanism should be proportionate**

Recent years have shown that the fines foreseen in the GDPR create a deterrent for data processing in general, albeit largely among SMEs and research institutions, who refrain from processing data in order to avoid costly adaptation of their business models or risk potential fines. Larger companies on the other hand seem to more aggressively object to fines issued by data protection authorities (DPAs) and see clarification through judicial means. It remains to be seen, whether this development leads to a two-tiered system when it comes to data processing, where big actors in the market will be able to gain access to data processing and can develop their business models, whereas SME will simply refrain from processing data unless they are required to do so with respective consequences to their competitiveness.

The amount of fines as well as the growing number of court cases against the decisions of the DPAs also underscore, that further clarification of the GDPR is required in order to be translated into a comprehensible scheme of easily applicable rules for companies.

- **Provisions on data anonymity need to be reviewed**

The goal of companies being able to process data legally when it has been anonymized has proven to be an impediment in the development of digitized business models. This problem is derived not from the challenges safe and secure data processing is posing or the fact, that personal data needs to be employed, but from the fact that the standards for anonymization are set so high, that complying with them is basically not possible. This challenge has proven to be especially cumbersome in developing digital solutions to fighting the COVID-19 disease, where in Germany data protection was held against the deployment of an early warning app, which delayed its public use and led to increased cost. Challenges like the one depicted above have intensified the need for legally compliant and economically acceptable standards for anonymizing personal data and ensuring that the approach to anonymising data is in line with the intent of the GDPR, where data is regarded as anonymous, when the re-identification of the data subject is obstructed by a disproportionate effort in time, cost or manpower. This would allow the processing for certain non-sensitive personal data under restrictions allowing for a more nuanced approach to data protection and further the ongoing process of weighing the right to informational self-determination and other fundamental rights.

- **Legal basis for data processing should be reviewed**

The GDPR has provided companies with several legal grounds for processing data. These grounds were usually regarded as equal. In practice, however, it has proven, that this seems to be not entirely the case. This challenge has proven to be especially true, when the legal basis of “consent” is considered in other legal acts, which are currently being discussed like the ePrivacy Regulation or which have recently been concluded like the Data Act. From the view of the internet industry, it

would be helpful to critically review the developments around the legal bases for data processing and ensure that the different approaches to it are still viable. Otherwise, the current development, where consent is generally regarded as a premium ground for data processing may risk, to narrow the general approach, the GDPR has provided processors with.

Additionally, more scrutiny should be given to the implications that new technologies e.g. Artificial Intelligence bring with them. Here guidance is needed when it comes to using autonomous systems like speech recognition in interplay with the GDPR since it is not clear, under which circumstances their deployment is legit. The current status quo is dominated by fear of restrictive application of the GDPR and crushing fines, which hampers innovation. The EDPB is called upon to give guidance how to safely employ these new technologies in accordance with the GDPR. Bolstering the risk-based approach to address privacy issues as originally contemplated when the Act was passed in 2016, would allow for appropriately reconciling data protection and innovation needs. In this respect, eco sees a particular role for privacy- and confidentiality-preserving models such as Privacy Enhancing Technologies (PETs) and Privacy-Preserving Machine Learning (PPML). Pseudonymous datasets with state-of-the-art technical and organization measures can support privacy- and confidentiality, and hence would merit further attention from EDPB and DPA's.

- **International data exchange needs a solid basis**

The practice of international data exchange has proven to be a challenge to data protection even before the GDPR came into effect. Data is often regarded as only to be safe when it is stored and processed within the field of application of the GDPR. Adequacy decisions are generally regarded as a remedy to this challenge. However, they present only of limited utility, since their elaboration is cumbersome, and their reliability is in question. With the Transatlantic Data Privacy Framework now in place and a lawsuit against it already in preparation, the question remains, how international data exchange, especially across the Atlantic, can be guaranteed under the conditions set by the standards, which are applied, since the GDPR has come into effect. Here, as well as in the provisions mentioned above, more attention should be paid to the fact, that the risk based approach should take into account, how far the actual data processing might interfere with the execution of fundamental rights of EU citizens. From this perspective, it should be clear, that the international transatlantic data flow needs more stability and reliability in its legal foundations.

This becomes especially relevant, when regarding the requirement to deploy state of the art security measures, which sometimes require cross-border data transfers. Advanced Machine Learning technologies are able to look at IP addresses and other traffic metadata from around the world to protect against Distributed Denial of Services (DDoS) attacks, prevent bots, or otherwise guard against personal data breaches. eco regards it as essential, that more clarification about the weighing of

the transfer of IP-addresses to third countries for reasons like cybersecurity and threat prevention should be given.

This topic also holds true in the discussion around the handling of whois. The handling of the database has become complex with the arrival of the GDPR requiring those who have access to it, to withhold data and in some cases also being uncertain, whether domain names can actually be entered in the data base, since they may contain personal data.

- **A uniform approach to data protection enforcement throughout the European Union should be aimed at**

The GDPR while comprehensive is offering a certain degree of flexibility and interpretation. While this approach is generally welcome, the recent developments as well as the problems depicted above underscore the necessity of a uniform approach to the interpretation of the GDPR. With the European Data Protection Board (EDPB), an institution has been created, which is generally able to address these requirements. However, there is also need, to extend both consultation with member states and their national DPAs, which are largely independently reviewing the GDPR, as well as the industry in order to get a better impression of the impacts the enforcement of the GDPR has throughout industry and society.

Many Member States have interpreted the derogations, exceptions and restrictions under the GDPR differently. This has in part led to the creation of differing rules e.g. age of consent, facial recognition technology for enforcement purposes, processing of sensitive and biometric data, scientific research. Due to Member States' leeway for the processing of biometrics data which is based on substantial public interests or national security, GDPR has been applied differently across the EU. It is important to create more consistency, constructive collaboration, and mutual recognition of opinions between DPAs to streamline the processes for organizations.

This should also be given regard when addressing the intended one-stop-shop (OSS) mechanism, that the GDPR created. The OSS is a critical tool for building consistency. Its work should ensure confidentiality of the administrative and proportionate timelines for the right to be heard.

- **Provisions for internal data processing within organisations need to be reviewed**

The provisions for data processing in general need a critical review. Currently there is uncertainty on, whether data within a company or organization may be handed on to e.g. other organisational units within the same organization or daughter entity. Here, it is unclear whether this represents a data processing within a single business unit, a data processing under joint controllership or commissioned data processing. In the opinion of eco, this should be possible without further administrative burden, if the original purpose of the data processing is fulfilled or the person has given its consent for processing the data in general. In practice,

however, processes like these often pose a significant challenge to especially larger business organizations since they create administrative burden. When updating the GDPR it would be sensible to give more scrutiny to measures that may adversely create administrative burden and bureaucracy without actually increasing the level of data protection.

Conclusion

The GDPR has established itself as a feasible and functionable instrument to employ data protection in the European single market. It continues to act as a critical and effective tool for protecting privacy. Given the significant compliance work by industry including many small businesses, and the efforts by nations around the world to mirror many of the key provisions of the GDPR, it would be disruptive to make widescale changes to the law. Not only would such changes create legal uncertainty for businesses and consumers, but they would also disrupt efforts to improve the global flow of data. While generally providing a comprehensive and understandable framework for protecting privacy and citizens' data the GDPR has during the time of its application shown to become increasingly bureaucratic and rigid, narrowing down the field of its application and giving rise to unintended effects like consent fatigue among users. Especially in the digital sphere, where data processing including personal data is central, this is becoming increasingly cumbersome for digital companies to innovate and be competitive in a global market. Especially when it comes to personalisation and individualisation of services and tools, European companies face competitive disadvantages in contrast to their globally active competitors. Here there is room for further improvement. eco understands, that the general approach of the GDPR is a foundation for trust of citizens and companies, which is helpful to preserve. However, the internet industry is concerned, whether this original objective of the GDPR is still in scope with today's enforcement practices. Data Protection is an important objective. It has nonetheless to be weighed against other fundamental rights. More clarity would help the legal certainty for companies.

Additionally, there should be a solution to address the problem arising from instable adequacy decisions with transition periods and guidance to apply compliant solutions for data transfers if the data is properly anonymized.

Finally, we recommend further exploring PETs and PPML and assessing where they can offer alternative solutions. This can foster innovation, including machine learning that is used to advance societal goals or to protect individuals' fundamental rights.