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

eco

Key Points Paper

on the evaluation of the General Data Protection Regulation (GDPR)

Berlin, 28th April 2020

With the General Data Protection Regulation (GDPR), Europe has established the framework for the organisation of personal data protection in the future. Regulation which had previously been of a scattered nature and handled differently by various national data protection laws was, in a central European regulation, pooled, systematised and organised using identical principles. Overall, a somewhat more stringent but fundamentally functioning legal framework has thus been created, which is a major cornerstone and key to success for the development of the Digital Single Market. As provided for in the regulation, the EU Commission's report on the application of the GDPR and its evaluation are underway and are now due on 25th May 2020.

eco – Association of the Internet Industry considers the European GDPR, together with its embodied principles, to be a fundamentally necessary and welcome regulation. Functioning data protection is a central aspect for trust in digital services and their use.

As things stand at present, it is probably too early for a comprehensive and in-depth analysis and evaluation of the GDPR, as the established legal framework still needs to be clarified by a corresponding decision-making system on the part of the supervisory authorities and also, in instances of disputed issues, by necessary case law. For this reason, both the report on the GDPR and a commentary on this can only occur with this caveat in mind. At the same time, in the short time since the GDPR has come into force, a number of issues have emerged which, in eco's view, require further deliberation.

For the evaluation of the GDPR, eco regards the following as constituting key points for the examination of and debate on the GDPR:

- **Application of the GDPR must be uniform and proportionate**

A central point of criticism of the GDPR has been that core problems have been caused in particular for SMEs and non-commercial players by excessive demands and requirements on the one hand, and the regulation's extremely high provisions for fines on the other. Even if data protection provisions should in principle apply equally to all parties and be consistently implemented, special attention should be paid in the enforcement of data protection law to both the resources of the respective players involved and to the proportionality of the measures applied. The current situation in Germany, for example, is regarded as non-transparent, in spite of an associated concept by the data protection supervisory authorities for the calculation of fines.

A factor which should be complied with more in the future and which should be implemented in accordance with the regulation's text is that of taking the lead role of one data protection supervisory authority into account, in addition to cooperation with the other supervisory authorities concerned. In general, it would be desirable for data protection supervisory authorities to endeavour more to ensure consistency and coordination in the uniform implementation of the GDPR.

At this point, it should also be noted that attention should also be paid in future reviews to ensuring that, in addition to the independence of the authorities, greater consideration should be applied to the uniformity of the fines imposed and their proportionality. If the impression among SMEs in particular is that the decisions of the supervisory authorities are inconsistent and unforeseeable, the initial success of the GDPR may go in the other direction, a reversal which would be detrimental to the data protection cause as a whole.

Lastly, despite the high degree of standardisation in the area of data protection, a lack of consistent standardisation across Europe with regard to various details still exists in areas such as the minimum age of consent, which is of particular relevance for offers to end customers.

- **The fragmented nature of the General Data Protection Regulation is creating more bureaucracy**

Uncertainty still prevails among companies as to whether commissioned data processing or joint controllership applies for data processing. Corporate groups in particular are faced with legal data protection hurdles in the internal configuration of their data protection rules and in the exchange of data – also with their own subsidiaries. The bureaucratic workload currently represents an additional burden for all companies, be they corporate groups, SMEs or sole proprietors, and this needs to be addressed going forward.

- **Data exchange outside of Europe must be simplified**

Currently, exchanges with third countries are a problem for businesses, with such problematic exchanges likely to include those with the United Kingdom at the end of the transition period. For the USA, the Privacy Shield in principle provides a solid legal basis; one which is regularly reviewed by the EU Commission and which for many companies forms the basis for data exchange with partners and customers in the USA, and vice versa. However, this is regularly called into question and subjected to re-examination not only by the political players involved, but also on the basis of legal proceedings and lawsuits. Legal certainty cannot be established in this way. Support for the Privacy Shield by political players and data protection supervisory authorities would therefore be desirable. What is needed are permanently reliable, sustainable and comprehensive rules for the international exchange of data with third countries. The EU standard contractual clauses could be helpful here, but they are also currently subject to scrutiny and, in the light of

the GDPR, have in some cases proved difficult to implement when it comes to questions of commissioned data processing. Internationally operating companies urgently need more legal certainty in this area if data protection adequacy decisions are delayed and appear to be contestable in practice.

- **Right to data portability must be clarified**

Two years after the adoption of the GDPR, the right to data portability for individuals still poses a challenge. Even though the Article 29 Data Protection Working Party has already positioned itself in this regard in a white paper, there is still a lack of clarity among companies and users as to how the requirements of Article 20 of the GDPR can be appropriately implemented. The suggestions of the Working Party have proven to be of only limited assistance and give rise to questions concerning the extent to which data portability should be made possible and how a common machine-readable standard can be enabled – and to what extent such a standard for companies is desirable in the first place. From eco's point of view, what would be welcome would be the initiation of a dialogue process to further discuss solutions to the open questions regarding data portability on a pre-legislative level, for example in the form of standards.

- **Purpose limitation giving rise to questions**

The GDPR requires a narrow purpose limitation for the use of collected data. What is essentially intended to be an effective means of ensuring data protection often poses major problems in practice, particularly within the confines of a company. This applies not only to the areas of online advertising, marketing and product development, but also in some cases to simple correspondence or data exchange in the field of HR. From eco's point of view, what would be desirable is a discussion on the possibility of a cautious opening-up of the narrow purpose limitation for the use of data in the future; especially concerning instances where the use of data within an organisation for selected purposes is connected to the original purpose. This would be particularly valid for cases where the data actually used are subject to a high degree of pseudonymization.

In this light, it would also be worth considering defining specific use cases for data processing through precisely defined recipients, who could then use these for their purposes in accordance with the DPA. This would be an important step towards ensuring legal certainty, for example in medical research or in the development of products and services in the IT sector, especially when AI is being used. Furthermore, from eco's point of view, it would be desirable if the legitimate interest term introduced by the GDPR could be specified in more concrete detail. The current situation regarding the application of Articles 6 and 9 of the GDPR is often difficult for companies to grasp, especially given that they are interpreted differently by national or local data protection supervisory authorities. A greater level of standardisation and clear legal authorisation criteria within the framework of the GDPR would thus be both expedient and desirable.

▪ **Summary**

Overall, it can be concluded that the GDPR provides a sound legal framework which both guarantees a high level of data protection and offers businesses an acceptable level of freedom to act. At the current stage of its implementation, a sufficient database does not yet exist to address a large number of details and questions regarding the revision of individual articles of the GDPR. In the coming years, the judicial system will have to determine whether the GDPR can remain a model of success when it comes to points of contention. This Key Points Paper addresses a number of central questions which, in eco's view, require urgent further discussion. If the introduction of an increased use of artificial intelligence is to succeed, associated questions which must be clarified concern not just purpose amendment and anonymisation of data, but also the creation of artefacts or digital twins as envisaged by the EU Data Strategy, and right of access in learning systems. Only in this way can digitalisation and modern future technologies be deployed successfully and in the interest of citizens.

About eco:

With over 1,100 member companies, eco is the largest Internet industry association in Europe. Since 1995 eco has played a decisive role in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of members in politics and international committees. eco's key topics are the reliability and strengthening of digital infrastructure, IT security, and trust, ethics, and self-regulation. That is why eco advocates for a free, technologically-neutral, and high-performance Internet.