BETTER IMPLEMENTATION OF THE GDPR

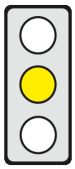
cep**PolicyBrief** No. 2020-01

Centrum für Europäische Politik

KEY ISSUES

Objective of the Communication: The Commission outlines the current state of legal convergence brought about by the General Data Protection Regulation (GDPR) and sets out what remains to be done to improve its uniform application.

Affected parties: Natural persons, companies and entities who process personal data.



Pro: (1) It is appropriate that the Commission will continue to support the successful implementation and the uniform application of the GDPR.

(2) The guidelines of the European Data Protection Board and the cooperation between the data protection authorities (DPAs) encourage the consistent application and enforcement of the GDPR; these instruments should be strengthened in order to reduce legal uncertainty and distortions of competition.

Contra: (1) In order to minimize divergences in the application and enforcement of the GDPR, inter alia, the practices of the DPAs to issue sanctions should be harmonized.

(2) In order to foster compliance with the GDPR and facilitate data transfers to third countries, codes of conduct and certifications must be made usable and transfer instruments brought into line with the GDPR.

The most important passages in the text are indicated by a line in the margin.

CONTENT

Title

Communication COM(2019) 374 of 24 July 2019: **Data protection rules as a trust-enabler** in the EU and beyond – taking stock

Brief Summary

- **Overview of EU data protection law**
  - The EU charter of fundamental rights ("Charter") guarantees the right to the protection of personal data [Art. 8].
  - This fundamental right is reflected in strict EU data protection laws, namely [**cepStudy** EU-Data Protection Law]:
    - the General Data Protection Regulation [(EU) 2016/679, "GDPR"], protecting personal data,
    - the Data Protection Law Enforcement Directive [(EU) 2016/680], protecting personal data processed by the police or criminal justice system,
    - the Data Protection Regulation [(EU) 2018/1725] for data processing by EU institutions and bodies, and
    - the Regulation on Privacy and Electronic Communications [COM(2017) 10, "ePrivacy"], still to be passed, which will protect the confidentiality of electronic communications [cep**PolicyBrief** No. 2017-16].
- **Implementation of the GDPR and status of harmonisation**
  - The General Data Protection Regulation's [GDPR] key objective of introducing uniform data protection rules and ensuring legal certainty "has been largely met" [p. 2].
  - All Member States except Slovenia have updated their national data protection law [p. 3].
  - The GDPR is directly applicable but contains opening clauses and obliges the Member States inter alia to
    - set up independent national data protection authorities ("DPAs") and provide them with powers and sufficient human, financial and technical resources; DPA resources still vary greatly between Member States [p. 4, 18];
    - enact legislation to reconcile the protection of personal data with the freedom of expression and information,
    - align all their sectoral legislation containing data protection provisions – e.g. social codes – with the GDPR; this work is still on-going and must be completed [p. 3, 18].
  - The GDPR also gives Member States scope to further specify its application in some areas, e.g. the processing of personal data for health purposes, or the age at which children can consent to online services [p. 3].
  - To achieve greater harmonisation, further efforts are necessary [p. 18]. In particular, consistent application of the GDPR will be ensured by [p. 3, 4]
    - the Commission, which will monitor harmonization efforts, conduct bilateral discussions with national authorities and take legal action, e.g. infringement procedures, against non-compliant Member States [p. 18],
    - the European Court of Justice and the national courts, which can invalidate provisions that depart from the GDPR,
    - the DPAs, which have intensified their cooperation by way of [p. 4, 6]

Authors: Alessandro Gasparotti and Dr. Anja Hoffmann, LL.M. Eur. | hoffmann@cep.eu
cep | Kaiser-Joseph-Strasse 266 | 79098 Freiburg | Germany | Telephone +49 (0)761 38693-107 | www.cep.eu

- the European Data Protection Board ("EDPB") [Art. 68 GDPR], which is composed of the heads of the DPAs and the European Data Protection Supervisor; the EDPB has adopted various guidelines on key aspects of the GDPR in order to facilitate its uniform interpretation;
- the cooperation and consistency mechanism [Art. 60 et seq. GDPR] which aims to bring about joint enforcement procedures in cross-border cases; the EDPB may adopt binding decisions in case of conflict.

– The Commission will report on the evaluation and review of the GDPR by May 2020 [Art. 97 GDPR].

► **Governance system and enforcement of data protection rules**

– Infringements of the GDPR are dealt with by the DPAs which have multiple powers: inter alia, they can impose fines or limit data processing [Art. 58 GDPR].
– So far, DPAs have [p. 4-6, 18]
  - focused mainly on dialogue but have also imposed fines of up to 50 million euros;
  - handled 516 cross-border cases but should step up their efforts; Member States should facilitate joint investigations.
– Some DPAs have created new tools to assist companies with compliance, e.g. telephone helplines and regulatory sandboxes – areas where innovators can test new products under the supervision of a supervisory authority. However, some stakeholders are requesting more support [p. 5].
– The Commission financially supports DPAs in raising awareness on data protection and facilitating compliance and fosters cooperation between DPAs and competition authorities to avert data protection violations. [p.5, 17]
– Several stakeholders are requesting more cooperation between DPAs, a uniform approach, greater consistency in the advice from DPAs as well as full alignment of national guidelines with those of the EDPB [p. 18].
– The Commission financially supports DPAs to more effectively involve stakeholders in the EDPB's work [p. 6].

► **GDPR's impact on individuals**

– Another key objective of the GDPR is to strengthen the rights of individuals [p. 7].
– Individuals are becoming more and more aware of data protection rules and increasingly exercise their rights, e.g. by requesting access to their data, withdrawing their consent, objecting to advertising communications or contacting DPAs to request information or lodge complaints. However, responses are often delayed [p. 7].
– Some individuals misunderstand the GDPR, believing e.g. that they must consent to all data processing [p. 7].
– Further measures to raise awareness are required. The Commission has launched a new online campaign to encourage individuals to read privacy statements and optimise their privacy settings [p. 8].
– Several NGOs have made use of their new power to launch representative actions on behalf of affected individuals. However, not all Member States have used the leeway provided by the GDPR to allow such actions to be filed even without a mandate [Art. 80 para. 1, 2 GDPR, p. 7].

► **GDPR's impact on businesses**

– Data protection is taken more seriously than ever before and hugely impacts many business sectors [p. 2]. Many businesses report challenges in adjusting their practices to comply with the GDPR – e.g. how to give individuals all the information in a way that is easy to understand – and call for clearer guidelines and legal certainty [p. 8].
– Small enterprises seem to be facing the most difficulties in adapting to the GDPR and are calling for guidelines tailored to their situation. The Commission supplements DPA initiatives by providing information material [p. 9].
– The GDPR provides for various tools – inter alia standard contractual clauses ("SCCs"), codes of conduct, and certification mechanisms – which help companies to demonstrate compliance with its rules [p. 9, 10]:
  - SCCs are model clauses which can be included in a contract between parties who process personal data, in order to lay down the parties' obligations under the GDPR. SCCs can serve as "safeguards", inter alia to allow the transfer of data to recipients in third countries [Art. 28, 46 GDPR].
  - Codes of conduct lay down data protection practices and thus specify the requirements of the GDPR for a specific sector. They are drawn up e.g. by trade associations and approved by a DPA; by adhering to these codes, companies can demonstrate compliance with the GDPR [Art. 40, 41 GDPR].
  - Certification mechanisms can also be used to attest compliance with the GDPR [Art. 42, 43 GDPR].
– The EDPB's guidelines on codes of conduct, certification and accreditation will enable the development of these tools. The Commission will also update existing SCCs and adopt more model clauses [p. 10].

► **Data protection at the global level**

– There is a global trend towards data protection. Several countries are adopting rules which contain principles and structures similar to those of the GDPR, e.g. overarching legislation, enforceable rights and independent supervision; companies increasingly extend rights of individuals under the GDPR to their non-EU based customers [p. 11].
– The global upward convergence may facilitate data flows, e.g. through adequacy decisions which find a third country's data protection level to be "essentially equivalent" to that of the EU. Under the GDPR, the Commission has adopted a decision on Japan and is aiming to reach further decisions, e.g. on South Korea [p. 11].

– Mutual adequacy findings between the EU and third countries may create areas where data can flow freely. Countries with similar values and systems could also establish a multinational framework, e.g. building on the European Data Protection Convention [ETS No. 108] [p. 12].
– In 2020, the Commission will report on the review of the eleven adequacy decisions adopted under the former Data Protection Directive [p. 19], e.g. with Canada and Argentina [p. 12]. Also, the EU-US Privacy Shield [see cep**Study**], with more than 4,700 participating companies, facilitates transatlantic data flows [p. 12].
– In addition, the Commission will inter alia "consider" [p. 12] using its powers under the GDPR to enable the use of certification schemes, codes of conduct and in particular SCCs as "tools" which may facilitate data transfers.
– To tackle digital protectionism, the Commission has developed specific data provisions which it systematically tables in negotiations on trade agreements. The alignment of the data protection may facilitate trade [p. 13].

Policy Context

In May 2018, the GDPR replaced the former Data Protection Directive [95/46/EC]. The Commission takes stock of its implementation, the functioning of the new governance system and its work at global level.

Options for Influencing the Political Process

Directorates General:	Justice and Consumers
Committees of the European Parliament:	Civil Liberties, Justice and Home Affairs (leading), Rapporteur: tba

ASSESSMENT

Economic Assessment

It is appropriate that the Commission will continue to support the successful implementation and uniform application of the GDPR. Since the GDPR came into force in May 2018, there has been progress towards the uniform application of its rules, but further efforts are required. **There is a need for greater legal certainty– e.g. through more and clearer guidelines – as companies still face difficulties in complying with the GDPR's rules**.

Although the GDPR is directly applicable, Member States still have to adapt their national legislation – including sector-specific laws containing data protection rules – and implement the mandatory opening clauses, e.g. clarify the content of certain provisions. All Member States and in particular Slovenia must finalize this work without further delay, otherwise legal certainty will not be possible across the EU.

The lack of clarity of certain GDPR provisions may lead to varying interpretations which could fragment the internal market and distort competition. It is therefore appropriate that the Commission is calling for efforts to achieve greater harmonisation. **The EDPB** recommendations and **guidelines,** applicable EU-wide, **and the cooperation between DPAs** in cross-border cases – which may promote the development of common practices by the DPAs – **encourage the consistent application and enforcement of the GDPR; these instruments should be strengthened in order to avoid legal uncertainty and distortions of competition**. The alignment of national guidelines with those of the EDPB – as requested by stakeholders – should be encouraged as much as possible as it increases legal certainty. Beyond this, **inter alia, the methods used by DPAs for imposing sanctions should be harmonized**, e.g. via guidelines. Otherwise laxer enforcement in some Member States – e.g. where fines are low or rare – would distort competition and might provoke a regulatory race to the bottom, mainly impacting consumer welfare.

To ensure the consistent application of the GDPR across the EU, it is crucial for DPAs to be equipped with sufficient resources to fulfil their mandate and swiftly cooperate with their counterparts. The lack of resources complained of by some DPAs means they may be overburdened, with negative consequences for the internal market: e.g., major companies might move their headquarters to Member States where DPAs fail to consistently initiate investigations, while small companies could be disproportionally affected by the delay in obtaining feedback from DPAs on compliance.

Given that it is in Member States' interest to attract businesses, the creation of new tools to facilitate compliance with the GDPR is appropriate. These tools must not be applied discriminatorily, however**.** This is particularly relevant to sandboxes where a supervisory authority might – arbitrarily – deny access to certain enterprises, e.g. due to the limited resources allocated for the supervision of selected enterprises.

Tools that help to show compliance with the GDPR increase confidence. The EDPB's guidelines on certification encourage the development of EU-wide common practices for the definition of certification criteria and for their approval by national DPAs. Adequacy decisions and the inclusion of provisions on data protection in trade agreements make the transfer of data to third countries easier, reduce the costs incurred by companies and increase legal certainty. This is subject to the proviso, however, that no major data protection deficits arise in the third country which could invalidate the decision by the CJEU (cf. cep**PolicyBrief** No. 2017-25). Thus, regular assessment of existing adequacy decisions is essential.

Legal Assessment

Legislative Competence of the EU

As before, the EU's regulatory powers regarding the protection of personal data arise under Art. 16 (2) TFEU.

Subsidiarity and proportionality with respect to Member States

The GDPR has largely harmonised the law on the protection of personal data in the EU. Although full harmonisation will be reduced by the numerous opening clauses, which give Member States scope for discretion, these are nevertheless in line with the principle of subsidiarity [cf. Müller, Die Öffnungsklauseln der DSGVO, p. 249 et seq.]; resulting variations in the law and the dovetailing of provisions with national law are therefore acceptable. Divergences in the application and enforcement of the GDPR due to differing interpretations of its abstract and complex provisions must however be minimised in order to avoid legal uncertainty and distortions of competition, e.g. by way of guidelines, cooperation or changes to the GDPR.

Compatibility with EU Law in other Respects

In order to foster compliance with the GDPR and facilitate data transfers to third countries, codes of conduct and certifications must be made usable and transfer instruments brought into line with the GDPR.

Adequacy decisions greatly facilitate data transfers to third countries but are subject to the strict requirements of the GDPR and the CJEU regarding recognition of an equivalent data protection level [C-362/14 Schrems v. DPC; cf. cep**Study**]. In 2020, the CJEU will decide whether the "EU-US Privacy Shield" meets these requirements [C-311/18]; the other decisions adopted so far will also have to be assessed in this regard.

The use of some alternative instruments, such as codes of conduct and certifications which can provide data protection "safeguards" under the GDPR, is currently limited. These instruments must be made more usable and all the necessary requirements created for their development. In addition, numerous issues which still remain, despite the EDPB guidelines, must be removed, such as whether a company can be subject to several codes of conduct simultaneously. The Commission must bring the three existing versions of SCCs into line with the GDPR as a matter of urgency and adopt additional clauses, e.g. on the subcontracting of processors. However, not all protection deficits in a third country can be offset solely by contractual "safeguards", for example if its law does not provide for the necessary enforceable rights and effective legal remedies within the meaning of Art. 46 GDPR. This may be the case in the USA. The CJEU will also have to decide the case [C-311/18] on whether data transfers to the USA can nevertheless be based on SCCs. It is likely that this decision will influence the future use of SCCs both in the USA and beyond.

Impact on and compatibility with German Law

In Germany, data protection supervision of the economy is divided between federal and regional (*Länder*) authorities. This leads to differing interpretation and enforcement practices, which in the interest of a uniform application of the GDPR must be avoided by better coordination between the German DPAs. The "Second Data Protection Amendment Act", which is yet to be adopted, aims to bring data protection rules in 154 federal laws into line with the GDPR, e.g. in the German Social Code. It is unclear whether the new Federal Data Protection Act (BDSG) excessively restricts the information obligations and rights of data subjects under the GDPR and is therefore in breach of EU law. It will be for the courts to decide whether these provisions fall within the scope of the GDPR's opening clauses. Legal certainty must also be created with regard to the obligation to reconcile data protection with the right to freedom of expression and freedom of information and in relation to exempting data processing for privileged – e.g. journalistic – purposes from GDPR obligations [so-called "media privilege", Art. 85 GDPR]. The federal states, being responsible for press law, have already adopted provisions on professional journalism which deviate from each other. It is also unclear which provisions apply beyond professional journalism, e.g. for photographers and bloggers. A framework at federal level to ensure the continuance of tried and tested German laws relating to the protection of freedom of expression would be advisable in this regard.

As the Facebook decision by the Federal Cartel Office [B6-22/16] shows, cooperation between data protection and competition authorities is appropriate since major data protection breaches by large corporations can lead to a dominant market position, the abuse of which must be dealt with by means of competition law.

Conclusion

It is appropriate that the Commission will continue to support the successful implementation and uniform application of the GDPR. There is a need for greater legal certainty – e.g. through more and clearer guidelines –, as companies still face difficulties in complying with its rules. The EDPB guidelines and the cooperation between DPAs encourage the consistent application and enforcement of the GDPR; these instruments should be strengthened in order to avoid legal uncertainty and distortions of competition; inter alia, methods used by DPAs for imposing sanctions should be harmonized. In order to foster compliance with the GDPR and facilitate data transfers to third countries, codes of conduct and certifications must be made usable and transfer instruments brought into line with the GDPR.