DIGITALEUROPE

29 APRIL 2020

DIGITALEUROPE Response to DG JUST Roadmap Consultation

Executive summary

The General Data Protection Regulation (GDPR) was a global milestone for data protection and privacy rules, as it not only provided upgraded rights to consumers but also looked to harmonise the rules across Europe, with the aim of fostering the digital single market.

In many respects, the GDPR achieved this goal. However, in view of the two-year review of the GDPR, we look at the areas where GDPR implementation can be improved, focusing in particular on the consistency mechanisms, harmonisation and data transfers.

As much as Member States have made great strides in ensuring consistency, there still remain overlaps that ultimately contradict one of the main objectives of the law – that of harmonising data protection rules across Europe.

In addition, the data transfer mechanisms within the GDPR are critical to business growth, and it is imperative that they remain adaptable to an ever-changing data ecosystem.

Data transfers

Adequacy decisions

The European Commission has only put in place adequacy decisions for a limited number of countries,[1] the last one for Japan in 2019.[2] More countries have recently adopted or are in the process of adopting new data protection laws,

[1] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[2] https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

providing in many instances a similar level of protection to the GDPR,[3] and it is therefore worth considering adequacy decisions for such countries.

As for the UK, it will be important to make sure that commercial data flows are considered as much a priority as law enforcement and judicial cooperation. Greater legal clarity and a better understanding of the steps taken to ensure data flows across the UK and the EU are needed.

The transition period after Brexit (until 31 December 2020) allows the UK to benefit from the continued application of the GDPR. Transfers of UK personal data after the transition period will also likely still be possible under Privacy Shield.[4]

However, to reduce commercial risks associated with relying only on one mechanism, ideally the UK should get the status of an adequate country and the European Commission should be proactive in starting to work on such adequacy finding as soon as possible.

Standard contractual clauses (SCCs)

The European Commission (or DPAs in collaboration with the Commission) should update and provide new SCCs. The new SCCs should be built with a modular approach, which will make them suitable for different scenarios that are not only for commercial practices. New SCCs should be suitable for not only controller-to-controller transfers and controller-to-processor transfers but for transfers between processors and from EEA processors to non-EEA processors.

An example would be a cloud provider that processes data on behalf of its customer. If the customer also offers processor services, for example to its affiliated companies, processor-to-processor SCCs would be appreciated, similar to the approach taken by the European Data Protection Board (EPDB).[5]

A ‘pre-populated’ Appendix 2, setting out the minimum standards or guidance as to the technical and organisational measures that are sufficient, would be useful.

Finally, for swifter execution, we would recommend that formats that are easier to execute be published, as this may ensure easier adoption and provide more flexibility for SMEs.

For the sake of harmonisation and consistency, there should not be various versions and templates. Member States should be encouraged to adopt SCCs

[3] See for example, Brazil’s *Lei Geral de Proteção de Dados* (adopted August 2018), http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

[4] https://www.privacyshield.gov/article?id=Privacy-Shield-and-the-UK-FAQs

[5] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201914_dk_scc_en.pdf

already published in the EDPB's Register for Decisions, or at least use it as a template and adapt to the circumstances where necessary.

Binding corporate rules (BCRs)

The bar for the creation and implementation of BCRs is relatively high. It would be useful if the requirements set forth in the DPAs' Working Papers for BCRs could be interpreted by regulators in a more practicable manner, taking into account the needs and possibilities of the digital industry. For example, there are strict requirements for disclosures due to law enforcement requests, audit requirements, information duties in case of processor BCRs to controllers, which are not easy to fulfil and can in some instances not be fulfilled for practical or legal reasons.

Furthermore, the process has become very demanding and long-lasting, with a current fine-year backlog, as besides the lead supervisory authority (SA) and the two co-reviewers, also all other DPAs concerned take part in the review of BCRs, which finally have to be approved by the EDPB as well.

We would also like to raise that should the EU-US Privacy Shield and the SCCs be further challenged in court, the BCR mechanism might become the preferable venue to secure data transfers. Therefore, it is important to review and streamline the current process to make it more accessible.

In addition, we support further progress in the recognition of BCRs as a certification mechanism – alongside other global schemes being considered for alignment with BCRs such as the APEC CBPRs – to allow organisations to efficiently manage international transfers and certifications globally.

Finally, we would recommend that there be as much transparency with regard to the development of future BCRs, in particular with the development and discussions around formatting and procedures. This will prove critical as the significance and importance of the BCR mechanism will likely become more prominent in the coming years.

Codes of conduct and other certification mechanisms

The GDPR provides for approved codes of conducts and binding enforceable commitments to apply appropriate safeguards as well as for approved certification mechanisms together with binding and enforceable commitments to apply the appropriate safeguards.[6] However, none of these mechanisms have been used at EU level.

[6] Art. 46 GDPR

The European Commission should foster the creation of industry-wide codes of conduct and certificates that address international transfers, to the extent that different sectors and companies present similar personal data processing operations.[7]

EDPB guidance on appropriate safeguards

The EDPB's guidance[8] on derogations is very strict, in particular with regard to the necessity test and the restriction to occasional transfers. As a consequence, derogations can often not be used although they are appropriate, in particular in case of a transfer necessary for pre-contractual measures or contract performance, including performance of a contract with a third party in the interest of the data subject, e.g. because data transfers that regularly occur within a stable relationship would be deemed systematic and repeated, hence exceeding an 'occasional' character.

In addition, gathering valid consent for data transfers seems to be impossible under the EDPB's strict interpretation. Among other thing, this doesn't take into account the various nuances under different models. For example, business-to-consumer consent is much simpler than under a business-to-business model. Therefore, we recommend that other legal bases be taken into consideration.

We therefore encourage the EDPB to revise its guidance regarding appropriate safeguards for data transfers under Art. 46 GDPR.

Consistency and harmonisation

Harmonisation in legislation and enforcement: strengthening the one-stop shop (OSS)

The importance of harmonisation and the GDPR's consistency mechanism cannot be understated, as failure to act consistently provokes legal uncertainties for international companies with cross-border (cross-European) processing activities as well as potential fragmentation of product offerings across EU markets. Differing decisions by DPAs can lead to significant administrative workload and more complexity in enforcing – precisely the elements that were

[7] For example, ISO 27701, providing a globally recognised tool for international data transfers. This standard has been mentioned in CNIL's press release, considering it 'a global standard: it is not GDPR specific, nor does it constitute as such, a GDPR certification instrument as described in Article 42 of the GDPR.' See https://www.cnil.fr/en/iso-27701-international-standard-addressing-personal-data-protection

[8] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

meant to be avoided. It contradicts the idea of a single market and burdens the pan-European growth of national industry.

A key driver of the European data protection reform has been the aim to harmonise the rules across the EU by creating a uniform data protection law. Previously, Directive 95/46/EC had been implemented differently in EU Member States, causing fragmentation. The GDPR's principal purpose therefore was to avoid a patchwork of 28 data protection laws with different interpretations and enforcement regimes.

The most relevant mechanism that the GDPR introduced for consistency and harmonisation in enforcement has been the one-stop shop (OSS), aiming at consistency via a cooperation mechanisms and reduction of administrative burden for organisations with a pan-European footprint. Organisations have welcomed the benefits that the OSS brings. Having a single interlocutor – the lead SA – for all issues related to cross-border personal data processing is highly valued by organisations, as it clearly simplifies procedures.

In many scenarios, non-lead SAs still have a role to play in the OSS context and can still scrutinise or even enforce against controllers with other lead SAs via cooperation mechanisms, including 'joint operations.'[9] The OSS simply does not apply in relation to a number of types of data processing, which to a certain extent reduces the concept's overall utility for business.

For this reason, there is a need to strengthen and promote the OSS, while achieving greater clarity and guidance as regards consistency and cooperation among SAs. The lead SA[10] must be unequivocally recognised by concerned SAs, allowing for the efficiency in investigation and enforcement procedures and promoting consistent interpretation across the EU.

The reality is that national laws implementing the GDPR have made maximal use of the margin of manoeuvre that the text allowed. This is the case for instance regarding the possibility for Member States to deviate from the parental consent principle for children under 16 and lower this threshold.[11] Consequently, Member States adopted different thresholds – from 13 to 16 – thus avoiding a consistent compliance approach for organisations in the EU.

There are simply too many opening clauses based on national law to allow for uniform implementation. As a consequence, companies have to decide whether they comply with national law – thereby possibly infringing EU law – or if they observe the requirements of the GDPR only.

[9] Art. 62 GDPR

[10] Art. 56 GDPR

[11] Art. 8 GDPR

At the moment, there are examples of divergent interpretation by national SAs, for instance regarding the criteria for high-risk data protection impact assessments and the scope of the legal basis for processing, further contradicting the GDPR's harmonisation objectives.

It is unclear whether a provision actually constitutes an 'opening clause' or not.[12] There is uncertainty to which extent (existing) national laws apply. For example, the processing of special categories of data repeatedly references 'on the basis of Union or Member State law.'[13] This language is ambiguous, and it is not clear what is required in terms of the EU or Member State law providing a 'basis.' The different interpretations lead to considerable consequences for data subjects as more administrative burden for business increase barriers to entry for certain markets, as business models and processes cannot be implemented uniformly across Europe.

It is also unclear how harmonisation will be achieved in cases outside the OSS, including in circumstances where the organisation in question, either a controller or a processor, is not established in the EU but still processes personal data of data subjects across the EU (and so must take a harmonised approach).

We would recommend that organisations be allowed to directly request an opinion from the EDPB with safeguards and limitations. Utilising the mechanism[14] under which any SA, the EDPB Chair or the European Commission may request that a matter of general application or with effects in more than one Member State be examined by the EDPB with a view to obtaining an opinion, when a competent SA fails to comply with the obligations under Arts 61 or 62.

Differing interpretations

Harmonisation of the GDPR across all Member States can be achieved through cooperation between the lead SAs and other national SAs, mutual assistances or joint operations. Where these mechanisms are insufficient to reach a consistent implementation of the GDPR across Europe, we urge for stronger enforcement of the consistency mechanism.

At the moment, when enforcing the GDPR, SAs are not obliged to involve the EDPB or start a coherency procedure,[15] even if the matter is of general importance or has implications in more than one Member State. Further, for

[12] See, for example, Art. 85(2) GDPR

[13] Art. 9 GDPR

[14] Art. 64(2) GDPR

[15] Art. 63 GDPR

matters of general importance with implications across several Member States, we would recommend if possible that the EDPB be consulted.

It is possible that national SAs, within their respective areas of competence, take decisions on the enforcement of the GDPR that differ from decisions taken in other Member States on similar issues. For example, fines that have been issued by SAs so far do not rely on common EU adopted criteria. In case of a breach, it is unclear whether any data subject suffered pecuniary loss or other distress as a direct result of the breach. This affects in particular companies from the same industry active in different Member States (e.g. internet service provider X is treated differently in country A than internet service provider Y in country B). There is a lack of consistency in fine calculation, with no common criteria across the EU.

Contrary to national approaches, fine calculation methodology ought to be the result of a European consensus rather than the national approach currently taken, which results in a myriad of different approaches. Otherwise, there is a risk of jeopardising the harmonisation objective of the GDPR and creating considerable legal uncertainty for businesses and citizens. Different decisions can have a considerable influence on the profitability of business models and thus also jeopardise the desired 'level playing field.'

Uncertainties on applicability of Member State law and/or the GDPR

For companies that operate in more than one Member State, the most challenging circumstance occurs when the laws of several Member States may apply to the same controller or processor. For example, if the processing takes place in the context of more than one establishment or takes place in the context of one establishment but involves offering goods and services to data subjects in another.

The most obvious example of a potential conflict here is the age of consent for children, but it also affects the exemptions for data subjects' rights and other issues. It is also unclear how the provisions of local law will operate in conjunction with enforcement action taken under the OSS. Any appeal will be dealt with under the national procedures, leading to a situation where the national courts could render an EDPB decision redundant.

In addition, a processor may process on behalf of controllers who are not subject to the GDPR. Many processor obligations only make sense if the controller is also subject to the GDPR, but the obligations exist irrespective of this. Arguably, a processor could be caught by Art. 3(2) but not a controller. It should be made clear that processors are only on the hook if the controller is caught by Art. 3(2).

Uncertainties on the interpretation of the GDPR and redundant wording

In case personal data is be processed for a purpose beyond or other than the original purpose for the initial collection, the legal basis for processing is unclear, particularly when consent is used in the first instance. However, this appears to ignore Recital 50, which states that, where the processing is compatible, 'no legal basis separate from that which allowed the collection of the personal data is required.' There is a need to clarify how Recital 50 is applied when the user has given specific consent to one purpose. A harmonised level of data protection within the EU requires clear guidance as to when a compatibility of original and new purposes is sufficient and when a new legal basis is necessary in addition to the compatibility test.

It is unclear how lead SAs will deal with situations which require the application of Member State law, where this is not necessarily the national law of their own Member State. For example, where special categories of data are processed, this could trigger various domestic legal provisions, which would need to be applied by the lead SA.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Martin Bell

Privacy and Security Policy Officer

martin.bell@digitaleurope.org / +32 492 58 12 80

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK