DIGITALEUROPE

21 JANUARY 2020

Almost two years of GDPR: celebrating and improving the application of Europe's data protection framework

Executive summary

The General Data Protection Regulation (GDPR)[1] was adopted in April 2016 and has been in application since May 2018. It has arguably been the most globally celebrated piece of EU legislation in the recent past in that it provides a comprehensive, balanced and more uniform set of safeguards that can continue to protect individuals' fundamental rights with current and future technologies.

As we approach the first evaluation and review of this important legal framework, which is due by May 2020, and as Member States finalise their findings on national implementations, it is key not only to celebrate the GDPR's manifold achievements but also to consider how its application can be further improved.

The complementarity between protection and innovation is an objective that a correct understanding of the GDPR principles, concepts and rules should always strive to achieve. Without it, protection might only be formal, and the development of new products and services be unnecessarily stymied.

This paper highlights some of the main interpretation and enforcement challenges that should be tackled to ensure that the GDPR can shore up the EU's industrial competitiveness, from the many facets of the Internet of Things (IoT) to artificial intelligence (AI) and beyond.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

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

Table of contents

GDPR implementation overview

The GDPR has to incentivise organisations to see their data protection compliance and strategy as a business enabler, in ways that reward responsible data-driven innovation.

The collective impact of the GDPR requirements has meant that organisations have had to be particularly thoughtful about the data they process, including the way they collect, use, share, secure and maintain data within the organisation as well as with business partners and providers.

The GDPR has increased accountability and has resulted in greater awareness of data protection issues at all levels. There are many reasons for this, including potential fines and reputational risks, enforcement powers for Data Protection Authorities (DPAs), Data Protection Officer (DPO) requirements, the separate regulatory status and liability for data processors, the ongoing digitisation of the public and private sectors and the public debate that has surrounded the Regulation's adoption.

The threat of strong enforcement has resulted in further investment in data protection compliance across industry. There has been an increased uptake of comprehensive data protection management programmes, with organisations revisiting existing programmes to ensure they are up to date. Such efforts and the fact that the GDPR has inspired other data protection regimes around the world, at least regarding its principles, has led many organisations to address data protection not only for their EU operations but also globally across all their business lines, products, services and locations.

In line with the data protection by design principle, organisations also had to review and reassess the relevance and business need for data, in order to ensure that data is collected, shared and retained only to the extent necessary. All organisations are, however, struggling with their data retention schedules, which are dependent on local laws, and practical guidance from DPAs is limited.

The GDPR requirements surrounding individual rights required organisations to examine their existing processes, update them where necessary or create new procedures to enable users to exercise their new rights.

However, there is still much uncertainty regarding the right to limit processing as well as regarding data portability. In particular, existing guidance on data portability does not address difficult issues that must be solved to make this right fully operational.

Refining data types

The GDPR is poorly equipped for situations involving personal data which, due to the nature of the information (such as professional contact information or aggregate information) and the context where it is disclosed or used (e.g. between organisations to manage their B2B relationships or for analytics or measurement purposes), presents a low risk to individual rights and freedoms.

Uncertainties regarding pseudonymisation and anonymisation need to be reduced. The GDPR's definition of personal data implies that the mere hypothetical possibility to single out an individual is not sufficient to trigger the application of the EU data protection framework. Instead, the test as to whether information is personal or not depends on a *reasonable* likelihood, which should take into account the costs and time required for identification by those who are reasonably likely to access and use the information at hand. However, the very expansive interpretation adopted by DPAs in practice results in almost any piece of information not being deemed anonymous.

The conditions under which datasets can be considered anonymous in specific contexts need to be in line with the GDPR text. Clarity on anonymisation techniques and a realistic assessment of what can be considered as anonymous data in practical scenarios would help. For example, can data be considered anonymous for an organisation but personal for another, e.g. once it is passed on to a third party who can supplement it with other information allowing clear personal references?

Fragmentation: local laws and authorities

In national laws implementing the GDPR, Member States have made full use of the margin of manoeuvre available under the text, and have in some cases gone beyond such margin. This has led to the creation of differing rules, for example, on the age of consent, facial recognition for law enforcement purposes, processing of sensitive data or for scientific research.

Fragmentation is not only due to national laws but also to national interpretation, guidance and enforcement by DPAs, which altogether show that there are diverging views, priorities and approaches.

There remains ambiguity over the functioning of the one-stop shop, with DPAs in some instances sending orders or requests for information, starting audits or imposing fines directly on establishments present in their territory and/or the main establishment, without referring the case to the lead DPA appointed by organisations as required by the GDPR.

DIGITALEUROPE appreciates that the one-stop shop is a work in progress and urges a consolidation of this mechanism in the interest of consistency, harmonisation and organisations' right of defence.

DPAs continue to issue national guidelines on the same topic, leading to contradictory results (e.g., template for processor contracts, cookies, GDPR inventories, DPIA methodologies and clinical trials). Some DPAs have launched national consultations in parallel with European Data Protection Board (EDPB) initiatives on the same matter (e.g., data subject rights).

We see a clear tendency from DPAs and the EDPB to put forward an overly restrictive interpretation of the legal framework, in some instances going against the letter and spirit of the GDPR text or relevant case law.[2] As a consequence, innovation in Europe today is risky and investment into new or improved products and services is stymied.

DIGITALEUROPE believes that going forward more stress should be put on safeguards rather than on limiting the applicability of legal bases for processing or providing unrealistic interpretations of the fairness and data minimisation principles, necessity, co-controllership or purposes. This could be done through technology itself, contractual commitments, organisational security measures as well as through the promotion of industry seals and certifications as envisaged by the GDPR.[3]

Transparency

New transparency obligations under Arts 13 and 14 have led to an overload of information, some of which is only relevant for experts as opposed to generating more effective protection for the average user. This results in very long and complex data protection declarations that have not led to improved transparency for data subjects as intended by the GDPR, but at best serve to fulfil a legal obligation on the part of the controller.

Apart from practical, reasonable and uniform guidance on the interpretation of the information obligations – in particular, regarding the recipients, retention obligations, legal bases and safeguards for international transfers – it is necessary to clarify what essential information should be made available immediately to the data subject as a first layer and what additional information could be made available elsewhere.

Consideration should also be given to clustering information relevant to data protection in order to prevent information fatigue.

---

[2] One such example is the restrictive interpretation of 'necessity,' as we've observed in our response to the recent EDPB consultation on the contract legal basis, available at https://www.digitaleurope.org/wp/wp-content/uploads/2019/05/DIGITALEUROPE-response-to-EDPB-public-consultation-on-draft-Guidelines-on-performance-of-a-contract-for-online-services.pdf

[3] See, for example, the recent EPRS study on *Blockchain and the General Data Protection Regulation*, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

Purpose limitation

The GDPR states that purposes must be 'specified, explicit and legitimate' but does not provide clear requirements as to how concretely or abstractly a purpose may be described. A balance should be struck between specificity and comprehensibility. In particular, DPAs should avoid mixing a data processing activity (the description of the processing, e.g., data storage or invoicing) with a data processing purpose (i.e. the ultimate reason why the processing activities are conducted, for example to perform a contractual relationship or to protect vital interests).

Same processing, multiple legal bases

DPAs' guidance often seems to ignore that the same processing activities may fall under different legal bases simultaneously – particularly so if an extremely narrowly scope is assigned to each basis.

Some examples of processing activities that may be covered by more legal bases are:

- The same personal data may be necessary in order to enforce a contractual duty, thereby falling under the contract legal basis, but also in order to comply with applicable legal requirements, thus being covered by the legal obligation basis.
- The same personal data may be processed to comply with relevant law (for instance, the NIS Directive),[4] thereby falling under the legal obligation basis, but also for the controller's own need to secure or prevent fraudulent use of its products, services or processes, which falls under the legitimate interest legal basis. The same data can indeed also be considered to fall within the contract legal basis to the extent that users will expect the service to provide a certain degree of security.[5]
- The same personal data may be technically necessary to deliver a service, thereby falling under the contract legal basis, but may also be processed for the controller's own R&D activities aimed at improving its products, services or processes, thus being covered under the legitimate interest legal basis.

---

4 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

5 See Working Party 29 Opinion 2/2006 on privacy issues related to the provision of email screening services, p. 6.

Contracts and the GDPR

DPAs have so far interpreted the contract legal basis without any consideration of contract law. In particular, they appear to limit its use to situations where it would be *altogether impossible* to deliver a service absent the processing of the specific personal data at hand.

This reading, however, is not supported by the GDPR text, which refers to processing '*in the context* of a contract,'[6] thus suggesting a broader interpretation. This is in line with civil law, where contracts oblige contracting parties to comply with their provisions and the nature of the contract according to law, ordinary usage and good faith.

From this perspective, a contract's context must take into account all the relevant phases – the precontractual phase, the contract's execution, its performance, monitoring, enforcement and termination. So long as a given contract is legal, processing consistent with the purposes of such contract can legitimately fall within the contract legal basis.

In practice, there may be multiple reasons why processing may be necessary for the performance of a given contract, and each contract's specific context will need to be factored in to determine what falls into the contract legal basis. This might include activities such as enforcement of contractual rights clauses; compliance with contractual warranties; service personalisation; fraud prevention or security of processing.

Consent

DPAs' construction of what constitutes valid consent has been particularly strict, generating a data protection theory that diverges from civil law rules, in particular regarding the freedom and specificity of consent.

Under the GDPR, consent can only be provided for 'one or more specific purposes.' A narrow definition of such purposes can very quickly lead to the necessity of establishing separate legal bases, and thus to more effort or the impossibility to process data. In particular, if the concept of purpose is narrowly construed, obtaining valid consent in scenarios with high-frequency communications between multiple actors may prove either too cumbersome or altogether impossible should no other legal bases be applicable.[7] This applies,

---

[6] Recital 44, emphasis added.

[7] See, in particular pp. 54-57 of the C-ITS Platform final report (January 2016), available at https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf

for instance, to machine-to-machine (M2M) or vehicle-to-vehicle (V2V) communications.

Consent plays an important role but is neither the only nor the default legal ground. It should hence not be emphasised as the primary legal basis for processing, nor should the other legal bases be interpreted and applied as exceptions or in an unreasonably narrow way. We urge the Commission to undertake a broader assessment of consent and the other legal bases as part of its evaluation of the GDPR's effective implementation.

Legitimate interest

Reliance on the legitimate interest legal basis can result in more conscious and protective processing activities. Legitimate interest requires data controllers to consider and balance data subjects' fundamental right with their own or third parties' interests, fundamental rights and freedoms. As such, it should not be viewed as a residual ground – on the contrary, we believe it should be considered the preferred ground for certain types of processing.

By contrast, we are seeing unduly restrictive national interpretations of legitimate interest that rule out reliance on this legal basis for purely commercial interests. This is contrary, for example, to the GDPR's Recital 47, where direct marketing (but one case of commercial interests) is set forth as an example of valid use of legitimate interest.

Data subject rights

The right of access for data subjects (Art. 15) is one of the rights that have been strengthened under the GDPR. Access is the most generic right and arguably the easiest to exercise, which may give rise to potentially excessive requests. Unreasonable requests should be limited, given that complying with the access right can be technically difficult, costly and time-consuming for organisations.

This has particularly been the case in an employment context, where former employees have not only asked for structured personal data but also requested copies of any document where their name may have been included, notably corporate emails. The access right has also been used to harm the right of defence of the organisation by former employees or contractual counterparties, in cases related to conflicts/settlement negotiations that are unrelated to data protection.

In some instances, data subjects have been taking advantage of the GDPR process to advance complaints that should be dealt with as part of the customer care process. This can lead to conflicts with other data subjects' rights (e.g. other

employees or customers/partners), infringement of confidentiality or business secrets or intellectual property rights of the company and customers/partners.

Separate and joint controllers

Complicated questions around joint and separate controllership need clarification. Under the GDPR, the complexity of the already existing concepts remains, and the lines are many times blurred between controllers and processors. These unclear roles often make contract negotiations more complex and time-consuming – and data subject rights not necessarily more protected.

We note with concern that where several organisations are involved in the same processing activities in different capacities, there is a trend from DPAs to qualify them as separate or joint controllers, irrespective of whether the cumulative Art. 26 requirements of deciding jointly both the purposes and the means of processing are met.

This gives rise to problematic situations where organisations are unable to effectively ensure GDPR compliance because they do not have actual control on the purposes and means of the processing activity at hand (e.g., blockchain nodes, clients of certain market research studies, etc.).

Third-country transfers

Ensuring the viability of international data transfers in a way that preserves effective protection of fundamental rights under EU law is a top priority for DIGITALEUROPE. The GDPR sets out a strict set of conditions for such transfers, but also a number of instruments to enable them. It is vital that these instruments remain effective as established by law and that organisations can rely on sufficient flexibility to implement them subject to the relevant legal safeguards.

Because of the limited number of third countries that have been deemed adequate, and because binding corporate rules (BCRs) only apply to intragroup transfers, standard data protection clauses (SDPCs) become an imperative tool for international transfers, both with third parties and within organisations.

Given their utility, we think there would be a real benefit in publishing additional SDPCs, or in amending the existing ones, to deal with other data transfer scenarios which are not yet catered for. For example, from a processor established in the European Economic Area (EEA) to a non-EEA processor and from an EEA processor to a non-EEA controller.

Furthermore, because GDPR codes of conduct and certification mechanisms can in principle allow for a comprehensive assessment of an organisation’s

processing activities, which may include third-country transfers, adherence to codes or certifications – particularly EU-wide ones, once approved – should be considered an appropriate safeguard to enable third-country transfers.[8]

Link to sectoral laws

It is vital that interaction with the GDPR is fully considered when new requirements for data use are introduced in other laws. There are often conflicting requirements and no clear rules as to which standard prevails or which authorities will be responsible for enforcement.

Not following a holistic approach may undermine the GDPR as well as other laws. To provide non-exhaustive examples:

- The proposed ePrivacy Regulation[9] contradicts key elements of the GDPR's risk-based approach. Under the proposed rules, non-invasive types of data processing, including IoT and AI use cases, would be unreasonably restricted. In addition, the GDPR's one-stop shop mechanism would be disrupted: telecoms regulators, as opposed to DPAs, would be responsible for the enforcement of at least some of the rules, without any reliance on the consistency mechanism.[10]
- The Collective Redress Directive, which includes the GDPR in scope, directly conflicts with the one-stop-shop procedure and the standards set out in the GDPR's Art. 80.

The GDPR and AI

The GDPR adequately covers data protection-related matters that arise with current and future technologies, and specifically with artificial intelligence (AI). However, it is particularly crucial to emphasise how unduly restrictive interpretations of the GDPR should be avoided to enable AI to flourish. This includes, notably, the interpretations of the right not to be subject to an automated decision, the purpose limitation and data minimisation principles as well as the purposes of processing and legal bases.

Regarding the legal bases more specifically, consent may be either inadequate, difficult or even impossible to obtain for all the required purposes of processing generated by a given AI application. To have a forward-looking approach to AI,

---

8 See section on codes of conduct and certification below.

9 COM/2017/010 final - 2017/03 (COD).

10 See Hogan Lovells, *Study of proposal for an ePrivacy Regulation*, November 2019, available at https://www.digitaleurope.org/wp/wp-content/uploads/2019/11/Hogan-Lovells-study-of-proposal-for-an-ePrivacy-Regulation.pdf

full use of all applicable legal bases – notably contract, legal obligation, public interest, vital interest and legitimate interest – should be fostered, keeping in mind that the selection of a legal basis in itself does not undermine the broader applicability of the principles and safeguards set out by the GDPR.

Data protection impact assessments

Currently there seems to be no clear and consistent approach to data protection impact assessments (DPIAs). DPAs don't seem to refer to the risk-based approach in their guidance or first GDPR enforcement actions.

In addition, DPA guidance on this topic to date has been largely fragmented and unhelpful. For example, different national lists of when a DPIA is required have led to unrealistic and unmanageable expectations for organisations.

When the DPIA requirement is combined with the accountability principle, it operates to significantly burden product and service development, because businesses must continually prove that their activities do not require a DPIA. This documentation exercise places a burden on organisations, in particular small and medium-sized companies.

Data breach notifications

As the threshold for data breach notifications is extremely low, organisations tend to notify DPAs also of cases that are likely below the threshold in order to avoid potential fines in case of a wrong judgement. In addition, even when not legally required, organisations may proceed to inform individuals due to reputational or contractual considerations; in such cases, the fact that the DPA hasn't been notified should not automatically be interpreted as a GDPR violation.

DPAs, in turn, are obliged to handle every complaint they receive, regardless of the risk level involved. As a consequence, they are overburdened with a large number of breach notifications. DPAs are now spending much of their time and resources in the role of complaint-handler rather than focusing on constructive engagement with organisations.

To address this problem, for both organisations and DPAs, we believe that the data breach notification provisions in Arts 33 and 34 should rely more on a risk assessment, since not every incident is a data breach.

Uniform guidance is required, in particular as to the determination of the level of risk that triggers notification in specific breach situations. It appears that breaches involving special categories of personal data (under Art. 9) are potentially always implicating a likelihood of harm to individuals. Such a one-size-

fits-all approach, without looking at all the details of the case involved, can lead to an overly strict interpretation of data breach notification rules.

The data breach notification obligation in the GDPR overlaps with incident reporting obligations existing under the NIS Directive[11] and other sectoral regulations. In practice, this means that a single security incident could trigger obligations for controllers to notify multiple authorities, in different countries and within different timelines, requiring different types of information in different formats.

Finally, companies face additional uncertainties with regard to reporting personal data breaches. In particular, it remains unclear whether any further misconduct uncovered as part of the notification can be used in the course of a subsequent investigation by the DPA. It is therefore necessary to state clearly that such information must not be used for subsequent investigations.

Codes of conduct and certification

Codes of conduct and certifications are important elements to facilitate and demonstrate compliance with the GDPR framework. To date, however, no EU-wide code has been approved, and the limited number of codes that do exist are all restricted to national application. This inherently fragments the European market and greatly reduces codes' potential to facilitate GDPR compliance.

EU-wide codes of conduct should be promoted more prominently and the conditions for the approval of Codes should be streamlined to achieve more scale and consistent protection across Europe.

Codes of conduct should be applicable to more than a single industry sector, as the GDPR itself does not provide an absolute requirement that Codes can only apply to a specific industry. Especially with regard to certain data processing operations that are similar across different sectors and companies, it might be appropriate to adopt largely similar solutions to achieve compliance.

Certification

The success of GDPR certification mechanisms, seals and marks will be a function of how Arts. 42 and 43 are implemented by all parties involved – DPAs, the EDPB, the European Commission and industry. Implementation must make it practical for organisations to participate in these efforts.

The flexibility available for the creation of GDPR certifications, seals and marks may lead to unnecessary duplication and fragmentation. While it is important to

[11] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

allow for the development of certification mechanisms that cater to specific sectors, products/services or national needs – including competing mechanisms if the market can accommodate them – ensuring EU-wide harmonisation is vital to generate the scale necessary for industry to see value in certifying.

This is particularly important given the possibility for the EDPB itself to approve criteria on the basis of the consistency mechanism, thus resulting in a European Data Protection Seal available at EU level.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Senior Policy Manager for Infrastructure, Privacy and Security

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

Martin Bell

Privacy and Cybersecurity 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

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

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN
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: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK