DIGITALEUROPE

10 JUNE 2020

Two years of GDPR: A report from the digital industry

Executive summary

Ahead of the European Commission's June 2020 evaluation report on the application and functioning of the General Data Protection Regulation (GDPR), DIGITALEUROPE seeks to provide input on the central elements of the GDPR that were a success alongside recommendations for how the GDPR can be improved.[1]

The GDPR's impact cannot be understated as its adoption was a clear global milestone for data protection and privacy rules. It not only provided upgraded rights to consumers but aimed at harmonising the rules across Europe.

However, despite Member States' attempts to ensure a consistent application of the law, fragmentation remains, ultimately contradicting the harmonisation aim of the Regulation. The following report goes into detail on key elements of the GDPR, coming to the main following conclusions:

- More coordinated implementation across Member States is needed in order to create a truly harmonised legal framework.
- The consistency mechanism should be strengthened to ensure a coherent approach to GDPR enforcement across Europe, bolstering the one-stop shop (OSS).
- The European Data Protection Board (EDPB) should continue to collaborate with industry and other stakeholders in producing essential guidance.
- For the GDPR to be even more successful, it must be interpreted to suit modern-day developments, most notably the complexities brought about by emerging technologies such as artificial intelligence (AI) and blockchain.

[1] This paper is a follow-up to the position we published in January 2020, available at https://www.digitaleurope.org/wp/wp-content/uploads/2020/01/Position-paper-on-GDPR-review.pdf.

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

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 business with cross-border (cross-European) processing activities as well as potential fragmentation of product offerings across EU markets. Differing decisions by supervisory authorities (SAs) can lead to significant administrative workload and more complexity in enforcing – precisely the elements that were meant to be avoided. This contradicts the idea of a single market and burdens the pan-European growth of national industry and in particular SMEs.

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 the 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 but also to encourage SMEs to grow. 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 via cooperation and consistency mechanisms, including 'joint operations.'[2] However, 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[3] must be unequivocally recognised by concerned SAs, allowing for the efficiency in investigation and enforcement procedures and promoting consistent interpretation across the EU.

[2] Art. 62 GDPR.

[3] Art. 56 GDPR.

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.[4] 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. Guidance by the EDPB on how to deal with the implementation of the different opening clauses would ensure clarity and consistency.

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.[5] 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.'[6] 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[7] 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

[4] Art. 8 GDPR.

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

[6] Art. 9 GDPR.

[7] Art. 64(2) GDPR.

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 by supervisory authorities

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 consistency procedure,[8] even if the matter is of general importance or has implications in more than one Member State. For matters of general importance with implications across several Member States, we would recommend 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 the myriad national approaches that exist at present, fine calculation methodology ought to be the result of a European consensus. 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.’

In addition, where accountability is clearly promoted by SAs and understood by organisations as a factor in mitigating liability, this will generate a greater focus on accountability beyond a minimum standard, and this should also be taken into consideration when calculating fines.

There should be recognition of the added value of organisations being subject to an independent evaluation of their compliance with applicable data privacy laws, by way of independent certifications in particular. This non-legalistic and value-

[8] Art. 63 GDPR.

driven approach to regulating organisations promotes the value of privacy and of being accountable to both organisations and individuals.

We are referring to independent attestation engagements providing the highest possible level of assurance with regard to the design, implementation and operating effectiveness of internal controls.

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 also 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.

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.

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 further compatible processing

In case personal data is 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.

Data transfers

There is a general need to establish additional and more flexible transfer mechanisms to those currently used by organisations as well as for clear regulatory guidance on appropriate safeguards.

The GDPR provides for different transfer mechanisms that are not yet put in place, such as EU-wide codes of conduct and other certifications, and possibly new standard data protection clauses (SDPCs, also known as standard contractual clauses or SCCs) and adequacy decisions.

These additional, potentially more flexible international personal data transfer mechanisms would complement the mechanisms currently in place, which need to be preserved and promoted.

Adequacy decisions

The European Commission has only put in place adequacy decisions for a limited number of countries,[9] the last one for Japan in 2019.[10] More countries have recently adopted or are in the process of adopting new data protection laws, providing in many instances a similar level of protection to the GDPR,[11] 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.[12]

---

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

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

[11] 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.

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

In view of the uncertainty over the long-term stability of Privacy Shield in light of ongoing court proceedings, and 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 data protection clauses

The European Commission, or data protection authorities (DPAs) in collaboration with the Commission, should update and provide new SDPCs. The new SDPCs should be built with a modular approach, which will make them suitable for different scenarios. New SDPCs should be suitable for not only controller-to-controller transfers and controller-to-processor transfers but also 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 SDPCs would be appreciated, similar to the approach taken by the EDPB.[13]

A 'pre-populated' Appendix 2, setting out the minimum standards or guidance on sufficient technical and organisational measures would be useful.

To ensure easier adoption and provide more flexibility for SMEs, we recommend that published formats be easier to execute.

For the sake of harmonisation and consistency, there should be a limited range of versions and templates. Member States should be encouraged to adopt SDPCs 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, considering 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 to controllers in case of processor BCRs, which are not easy to fulfil and in some instances cannot be fulfilled for practical or legal reasons.

[13] EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8)GDPR), available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201914_dk_scc_en.pdf.

Furthermore, the process has become very demanding and long-lasting, with a current five-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 encourage the setup of a clear and fast-track process to ensure a broader creation and implementation by industry.

We also want to raise that should the EU-US Privacy Shield and the SDPCs be further challenged in court, the BCR mechanism might become the preferable venue to secure privacy-enhanced 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 wider recognition of BCRs. On the one hand, as a certification mechanism to manage global international transfers, alongside other global schemes being considered for alignment with BCRs such as the APEC CBPRs. On the other hand, as it requires implementation of all aspects of the GDPR (notice, consent, data processing agreement, security measures, audits) it should be recognised along those lines, in other words as a certification for GDPR compliance, not just transfers.

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.[14] However, none of these mechanisms have been used at EU level.

The European Commission should foster the creation of industry-wide codes of conduct and certificates that address international transfers.[15]

[14] Art. 46 GDPR.

[15] 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'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.

EDPB guidance on appropriate safeguards

The EDPB's guidance on derogations is very strict, in particular with regard to the necessity test and the restriction to occasional transfers.[16] 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 things, 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.

Sectoral interpretation

Although the GDPR has improved data protection accountability and awareness, it has not addressed specific sectoral concerns. This has led to areas where the application of the GDPR provisions is unclear. In this section, we identify challenges and barriers faced by specific sectors, namely healthcare and finance, and propose possible ways to mitigate these.

Clear guidance by the EDPB and increased use of codes of conduct are among possible solutions which could bring more clarity to the applicability of the GDPR. It would also strengthen the overarching framework for the governance of data sharing in the EU that would boost growth and create value.

The EU Data Strategy includes the creation of common European data spaces in different sectors.[17] However, these data spaces and the associated free movement of data across the EU can only happen once the GDPR's implementation and interpretation challenges are resolved.

[16] EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

[17] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, COM(2020) 66 final.

Legal fragmentation: local laws and regulations

One key objective of the GDPR was to reduce fragmentation amongst EU Member States and provide legal certainty for individuals and businesses across the EU.[18] Although, the GDPR has, to a large extent, contributed to this objective, it has left a margin for national legislators to maintain or introduce more specific provisions or further conditions to adapt the application of certain rules of the GDPR.

Consequently, these national margins have contributed to an even more fragmented legal landscape than was originally foreseen. For instance, Member States may maintain or introduce further conditions, including limitations, regarding:

- The GDPR allows Member States to maintain stricter rules with regard to the processing of genetic data, biometric data or data concerning health.[19] This means that there is no unified applicability of the GDPR across the EU. Oftentimes, it is not the GDPR that restricts the sharing of health data, but rather the stricter Member State rules that deviate from the GDPR. This has resulted in Member States adopting different approaches to processing of health data, making it difficult to access data and electronic health records from various institutions, locally and in a cross-border context. The fragmentation of rules across the EU's internal borders makes it a complex challenge for organisations to pool data from multiple Member States for a single project, especially in health-related scientific research. Increased harmonisation of rules across the EU would help to harness the full potential and value of data.
- Processing for scientific research purposes. Member States do not consistently apply the derogations for scientific research processing set out in the GDPR.[20] In addition, although the GDPR expressly states that Member States may adopt laws to enable processing of health data for scientific research purposes,[21] some Member States rely on consent as the primary legal basis instead.
- The processing of personal data relating to criminal convictions and offences[22] allows Member States to regulate through national law.

[18] See Communication from the Commission to the European Parliament and the Council, Data protection rules as a trust-enabler in the EU and beyond – taking stock, COM/2019/374 final, and Council position and findings on the application of the General Data Protection Regulation (GDPR) (January 2020).

[19] Art. 89 GDPR.

[20] See ArticleArts 5(b) 'Purpose limitations' and Article 5(e) 'Data retention'GDPR.

[21] See Arts 6, 9 and 89 GDPR.

[22] See Art. 10 GDPR.

Fragmented national requirements on this type of processing are particularly relevant for the financial services sector. Financial services institutions are bound by laws on anti-money laundering, prevention and detection of terrorist financing, fraud prevention and detection, and by insider risk controls to process such data. Widely divergent regimes across Member States make it difficult to operationalise measures needed to comply with the rules.

- Processing of biometric data in the employment context. Member States may implement more specific national rules to process special categories of personal data where it is necessary for a legal obligation in the field of employment law. Divergence of national legal frameworks has created considerable hurdles for companies operating cross-border. For instance, some Member States allow technical and organisational measures that are indispensable to comply with security and breach notification requirements but undermine the protection of employees' data. Some of these measures cannot lawfully be implemented in other Member States, as they may violate some national employee data protection laws.
- In addition to the EDPB's guidelines on video devices,[23] guidance more specifically addressed to data processors would help deal with the currently fragmented approaches between Member States.

The GDPR and national rules complementing it have only recently been applicable. However, sector-specific legislation is still currently being revised in many Member States. Therefore, there is a need for clarity and guidance on Member States' sector-specific legislation.

In addition to removing fragmentation, further clarification of the rules will also help to build trust in the data economy.

For example, in the financial sector, although the GDPR is not in direct tension with open banking, there is a lack of public understanding about how the technology behind open banking works, which can lead to fear and uncertainty about the use of customers' data in an open banking context. More general guidance around best practices for privacy-compliant data handling within the financial sector would be welcomed.

Codes of conduct

The European Commission's upcoming evaluation report should also highlight how codes of conduct could take into account the similarities in personal data

[23] DIGITALEUROPE's views on the guidelines are available at https://www.digitaleurope.org/wp/wp-content/uploads/2019/09/DIGITALEUROPE-response-to-EDPB-consultation-on-video-devices.pdf.

processing within and between some sectors as a suitable way to contribute to the proper application of the GDPR.[24]

The recently published EU Data Strategy encourages the establishment of a code of conduct for processing of personal data in the health sector.[25] The European Commission could also map national initiatives that could be replicated at EU level by industry.[26]

Consent in the healthcare sector

A narrow interpretation of consent creates particular barriers for secondary use of data in healthcare. In the health sector consent must be obtained from patients to re-use their data for other purposes than initially foreseen. This is very impractical and often impossible, especially where there is no direct relationship with the patient.

A broader assessment of consent vis-à-vis other legal bases would be useful in this respect. An alternative ground for certain types of processing could be public or legitimate interest. The EDPB indeed considers that legitimate interest can serve as a legal basis for processing for scientific research purposes if it is combined with appropriate conditions.[27] Further guidance and clarity from the EDPB on these would be welcomed.

Anonymisation

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 likely to access and use the information at hand.[28]

However, DPAs are adopting excessively strict interpretations of what constitutes anonymous or anonymised data. In addition to unnecessarily hindering data processing that has no impact on individuals' rights, such interpretations make it

[24] See section on codes of conduct below, pp. 20-21.

[25] See pp. 29-30, COM(2020) 66 final.

[26] See for example the Finnish model for secondary use of data, https://media.sitra.fi/2019/05/07121654/a-finnish-model-for-the-secure-and-effective-use-of-data.pdf.

[27] EDPB Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR).

[28] Recital 26 GDPR.

difficult for organisations to agree on whether and how parties can use the data shared in a collaborative project.

In many cases, this results in a less privacy protective outcome for data subjects, as organisations agree on the lowest common denominator for what equates as anonymised data. Companies, on the other hand, will not be able to generate new products and services using non-invasive data.

We would therefore welcome clarity on the data conditions under which datasets can be considered anonymous in practical scenarios, such as health or finance, and updated guidance on anonymisation techniques.

These uncertainties could be addressed, for example, through a code of conduct or certification schemes from the security and engineering community. Such code or certification could offer solutions to provide increased certainty, for instance by recognising:

- A ‘relative’ anonymisation model. This would provide traceability back to the source records without representing a risk for subject identification by the parties involved in the specific context, considering the policy and contractual requirements as well as the security measures applied. Defining the necessary standards and required governance is key to this ‘relative’ anonymisation model. Its benefits, for instance, would lie in enabling healthcare research by facilitating different data-sharing settings: from institutions to researchers, between pharmaceutical companies (for example to limit the need for a placebo/standard-of-care arm in a clinical trial) as well as from pharmaceutical companies to government-funded research initiatives.
- An ‘opt-out’ model to apply whenever relative anonymisation may not be sufficient. While guaranteeing limited risks to individuals thanks to high levels of governance and standards, this option would make it possible for individuals to request that their data not be used. This model could cover research fields where the nature of activities conducted gives a higher risk of re-identification than usual, and where further de-identification may impact the ability to conduct the research. Examples in this respect are rare diseases, genetic research and research for personalised medicines.
- An ‘opt-in’ model, alternative to ‘opt-out,’ where a patient may elect to take part in health-related research governed by a dynamic framework. This framework may change over time due to new research areas identified. The downside of this model is that it is unsuitable to any use of ‘legacy data.’ Even in this model, it may be difficult to rely on consent as the legal basis, as it may not meet the required specificity criteria.

The EDPB should also look beyond traditional anonymisation techniques and consider new privacy-protective solutions, such as differential privacy.

Differential privacy helps address re-identification as information is gleaned from a given database by adding noise to the otherwise correct results of database queries. In practice, the noise helps prevent results of the queries from being linked to other data that could later be used to identify individuals. In healthcare, for example, such techniques can increase privacy of individual health records and lead to advancement in future research.

Legal bases

Same processing, multiple legal bases

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

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

- The same personal data may be necessary to enforce a contractual duty, thereby falling under the contract legal basis, but also necessary 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),[29] 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 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.[30]
- 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, thus being covered under the legitimate interest legal basis.

[29] 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.

[30] 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,[31] 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 consider all the relevant phases – the pre-contractual 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.

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, making it more difficult 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, such as machine-to-machine (M2M) or vehicle-to-vehicle (V2V) communications, may prove impossible should no other legal bases be applicable.[32]

Another unfortunate adverse effect is consent fatigue, which can be avoided if a different legal basis, such as contract or legitimate interest, is used for expected

[31] Recital 44 GDPR.

[32] 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.

processing activities with a low privacy impact. From this perspective, we are concerned that consent is being emphasised as the primary legal basis for processing in a number of scenarios – the other legal bases should not be interpreted and applied as exceptions to consent or in an unreasonably narrow way.

Legitimate interest

Reliance on the legitimate interest legal basis can result in more protective processing activities. Legitimate interest requires data controllers to consider and balance data subjects' fundamental rights and freedoms with their own or third parties' interests. It is due to this balancing exercise that reliance on this legal basis results in more conscious processing. As such, it should not be viewed as a residual ground but rather considered the preferred ground for certain types of processing.

For instance, consent cannot be used as the legal basis to process the data of employees as there is an imbalance between employer and employee. Reliance on legitimate interest, on the other hand, is necessary to enable companies to provide various services to employees, such as training courses.

By contrast, we are seeing unduly restrictive national interpretations of legitimate interest that rule out reliance on this legal basis for purely commercial interests.[33] This is contrary, for example, to the GDPR's Recital 47, where direct marketing is set forth as an example of valid use of legitimate interest.

Archiving and research exemption

As researchers and scientists work around the clock to gain insights into the COVID-19 disease, public and private-sector stakeholders are in discussions about the most effective and appropriate ways to share personal data for scientific research in combatting the disease. The GDPR and Member State laws bring a complexity to the matter of sharing personal data, and special categories of personal data such as health data in particular.

However, what the COVID-19 pandemic has highlighted is the importance of sharing personal data by both private and public organisations to fight against communicable diseases, whilst respecting the principles of data protection laws.

[33] See the Q&A on legitimate interest on the Dutch DPA website, available at https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken.

The GDPR embeds a risk-based approach to allow for consideration of risks and harms and it is important to obtain clarification as to how the GDPR applies to the processing of personal data for research purposes by the private sector.

Processing of personal data for scientific research

The GDPR provides that the processing of personal data for scientific research purposes should be interpreted in a broad manner, including for example technological development and demonstration, fundamental research, applied research and privately funded research.[34]

We welcome the approach of the European Data Protection Supervisor (EDPS) in its preliminary opinion on data protection and scientific research whereby the EDPS clarified that not only academic researchers, but also not-for-profit organisations, governmental institutions and profit-seeking commercial companies can carry out scientific research.[35]

Profit-seeking companies can carry out scientific research and it is important to note that scientific research be defined broadly. We would welcome clarification that the fact that research is carried out for profit or commercial purposes should not prevent it benefitting from the 'scientific research' provisions.

We would welcome greater clarity as to the scope of what can be considered scientific research – particularly in the age of big data, where the data analytics activities of many organisations may qualify as research. Therefore, we call for a clarification that developing technologies which have wider public and societal benefits (for example, to help detect or treat diseases), even in a commercial context, would constitute 'scientific research.'

In addition, a clear recognition that use of personal data purely for validation and benchmarking of algorithms – which are necessary for meaningful search for the improvement of algorithms, including for testing whether an algorithm is biased – constitutes processing for research purposes.

In addition, there is a fundamental inconsistency between the requirement of Art. 9(2)(i) that processing for scientific research purposes must be based on 'Union or Member State law' and Art. 89(1), which does not mention any such requirement.

Recital 45 GDPR provides some clarification by stating that the GDPR 'does not require a specific law for each individual processing,' hence authorising research

[34] See Recital 159 GDPR.

[35] European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research, January 2020, available at https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf, p. 11.

that falls within the general framework of a legal instrument at either EU or Member State level. However, this requirement is particularly challenging for private organisations as laws are not needed to permit activity but rather to restrict it. Accordingly, clarification should be provided as to how private organisations can seek to comply with this provision.

Public interest

The right to the protection of personal data is not an absolute right – it must be considered in relation to its function in society and be balanced against other fundamental rights in accordance with the principle of proportionality.[36]

The Finnish system for the reuse of health and social data based on public interest is a good example of a model that recognises the secondary use of data for purposes deemed of public interest in sectors like healthcare, mobility and government services.[37]

Consequently, more stress should be put at EU level on recognising public interest as a valid ground for processing in cases in which societal benefits outweigh individual privacy concerns.

Codes of conduct and certification

Codes of conduct and data protection certifications, seals and marks are ways for organisations to demonstrate their commitment to, and compliance with, the GDPR. They can help controllers and processors demonstrate data protection in a practical, objective way to all stakeholders including clients, customers, partners, employees and regulators.

Codes of conduct

Successfully adhering to a code of conduct demonstrates that an organisation has a competent understanding of how to apply the GDPR in practice. Codes are rigorous accountability exercises for adherents and serve to increase transparency. Given the value that codes of conduct have to offer, it is critical to improve the current approval process.

The EDPB's guidelines and accreditation process for monitoring bodies lead to fragmentation and slow down the whole process as each Member State is required to submit its individual accreditation requirements to the EDPB for its opinion. This leads to a situation where, for example, the UK's Information

[36] See Recital 4 GDPR.

[37] https://stm.fi/en/secondary-use-of-health-and-social-data.

Commissioners Office (ICO) requirements do not take into consideration the unique needs of micro, small, and medium-sized enterprises (SMEs).

A more streamlined approach, in which all accreditation criteria of all Member States would be assessed together, would result in an EU-wide applicable accreditation requirement. This would shorten the overall procedure and greatly improve European harmonisation.

Accreditation requirements for codes of conduct should reflect the needs of different stakeholder groups and take a risk-based approach that considers the type of data processed, the size of the code members and the governance arrangements. Too stringent accreditation requirements for a monitoring body would make it impossible to elaborate small-scale codes of conduct.

Finally, the GDPR does not limit a code's applicability to a specific industrial sector, and consideration should be given to codes of conduct that span multiple industry sectors and relate to similar data processing operations.

Certification

We welcome the efforts of DPAs, the EDPB, the European Commission and industry on the issue of certification. However, we are concerned that the flexibility available for the creation of GDPR certifications, seals and marks may lead to unnecessary duplication and further fragmentation by Member States.

We urge that European certification mechanisms should replicate already internationally recognised and widely adopted standards.[38] This approach comes with many advantages, such as:

- Improving cooperation amongst European and international DPAs, reducing unintended barriers for companies by proving accountability in home jurisdictions;
- Providing European-certified organisations with an international competitive advantage; and
- Faster adoption as new mechanisms will not need to reinvent the wheel but will build upon already implemented ones.

Implementation must be practical for all organisations, regardless of size. Whilst many organisations have adopted various accountability mechanisms, these may not adequately address the requirements of companies throughout the supply chain, many of whom are SMEs.

[38] See for example IEC/ISO 27701 as internationally recognised standards that have been globally adopted and implemented.

Certification criteria should reflect the needs of different stakeholder groups and risk factors. Consideration should be given to a certification regime to account for organisations of all sizes and the full range of risk factors. This view supports the GDPR requirements that the specific needs of SMEs be accounted for.[39]

In this regard, system and organisational control reports, specifically SOC2 reports, can serve as a useful example of how certification criteria could be applied on the basis of Trust Service Principles.

Finally, we would welcome clarification from the EDPB as to the variances between codes of conduct and certification, as they each have their fundamental features.[40]

Data subject rights

The GDPR strengthened and streamlined users' rights, generating greater user control. Nevertheless, there is still a need for clarity and guidance on the scope and nuances of data subject rights.

Data portability

The GDPR provides users with the ability to request the personal data they have provided to a controller and then have that data transferred to another controller.[41] Data controllers are required to provide the data in an interoperable format that is 'structured, commonly used and machine-readable.'[42]

This right serves the twin objectives of strengthening users' control over their data and promoting competition between service providers, avoiding lock-in situations. We believe that the scope of the right to data portability is broad enough to fulfil these intended goals.

The right as established under the GDPR is in itself sufficient to ensure portability. However, from a practical standpoint there is a need to develop industry standards to be effectively put in place by all players to ensure direct portability between service providers.

---

[39] Art. 42 GDPR.

[40] Cost is an important consideration here. Most notably, audits by an accredited certification body necessitate a certain degree of cost, which should be proportionate to the size and scale of the data processing activities. The cost of certification for SMEs should generally be lower than for larger firms but can be expected to cost more than equivalent codes of conduct in order to allow profitability of the accredited certification bodies. Another factor to be considered is the type of processing, with certification more suited for higher-risk processing justifying the higher cost of completing a successful audit.

[41] Art. 20 GDPR.

[42] Art. 20(1) GDPR.

In addition, while it has been clarified that the scope of portability does not include derived or inferred data, and therefore that machine-generated data is out of scope,[43] there remain complexities and nuances to such right that would require further clarification.[44]

Right to erasure

Another key data subject right is the 'right to erasure.'[45] Data subjects can request an organisation who processes their personal data to erase such data, without undue delay.

However, under certain circumstances organisations are permitted to reject such requests. Most notably, organisations can reject the deletion of a user's personal data if the data is considered to be within the 'public interest' or if it conflicts with 'freedom of expression.'[46]

As more data is being shared with multiple parties for more services, the difficulties of the right to erasure become evident. Emerging technologies further compounds such difficulties.

For example, blockchain would make this right almost impossible as the technology relies on the input of data that is then transferred into a blockchain algorithm that is highly secured, incorruptible and cannot be tampered with. Therefore, the right to erasure renders blockchain technology itself mute.

It is clear that the right to erasure is highly complex and can pose great difficulties for organisations if interpreted expansively. Therefore, we recommend that guidance be provided on the interpretation of the right to erasure with a focus on emerging technologies.

Conclusion

The importance of the GDPR cannot be understated. One of the core purposes of the GDPR was to create one harmonised personal data protection and privacy landscape across all Member States – a cornerstone for the achievement of Europe's 'Digital Single Market.'

[43] See pp. 8-9 of the Article 29 Working Party Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01, endorsed by the EDPB.

[44] DIGITALEUROPE's views on the current guidelines are available at https://www.digitaleurope.org/wp/wp-content/uploads/2019/01/Position%20Paper%20-%20DIGITALEUROPE%E2%80%99s%20views%20on%20Article%2029%20Working%20Party%20draft%20Guidelines%20on%20the%20right%20to%20data%20portability%20(WP%20242).pdf

[45] Arts 17 and 18 GDPR.

[46] Art. 17(3), letters (c), (d) and (a) GDPR respectively.

Although in many respects the GDPR achieved this goal, their remain some gaps that need to be addressed in order to prevent further fragmentation in the EU.

We believe that the GDPR as a legal mechanism is robust and fit for purpose in facing the challenges of the future, such as the widespread roll out of AI. However, it is important that the GDPR be fully implemented across the EU and that Member State derogations be minimised, including through DPA cooperation and coordination.

In addition, we welcome the EDPB's role in producing reliable GDPR guidance and that stakeholders continue to have the opportunity to provide input.

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, Eli Lilly, 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, Ricoh Europe PLC, Roche, 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: Nederland ICT, 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