Position Paper

GDPR Review – Recommendations for the EU's Data Protection Framework

May 2020

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und neue Medien e.V.
(Federal Association
for Information Technology,
Telecommunications and
New Media)

Rebekka Weiß, LL.M.
Head of Trust & Security
P +49 30 27576 161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

1 Introduction

The General Data Protection Regulation (GDPR) came into effect two years ago and has become one of the most discussed, celebrated and well-known pieces of EU legislation. Its importance for economy and society, especially in the digital environment, cannot be overstated. While we welcome the awareness for data protection that the GDPR has brought, the current evaluation process gives us reason to pause and review the legal framework in order to improve its application and legal obligations. Even if the GDPR itself will not be amended in this review, we are convinced that the evaluation should be used to prepare an improved data protection framework - especially given the upcoming legislation proposed in the data strategy and the ePrivacy Regulation.

One of the GDPR´s aims was to provide a comprehensive, balanced and uniform set of rules and safeguards to protect the fundamental rights of citizens, while at the same time enabling free data flow, data use as well as current and future technologies. Whether these objectives were achieved, has been at the centre of many debates. It is the balance between protection and innovation that we will focus upon in this paper because we are convinced that without it, protection might only be formal, and the development of new products and services be unnecessarily slowed down or stopped. We will highlight some of the main interpretation and enforcement challenges that should be tackled to ensure that the GDPR supports EU's industrial competitiveness, especially in the fields of AI and IoT.

2 Key aspects

The past two years have emphasised some room for improvement in the data protection framework, which would bring the GDPR closer to achieving its aims. Amendments should be made with regard to specific provisions to improve implementation and legal

certainty (see Chapter 3).

In our view, the EU should focus on the following five aspects in the evaluation and with regard to all other data related legislation that is to come:

- Improve harmonization and accelerate the coherence mechanism
- Prevent regulatory overlaps
- Strengthening research and access to health data
- Provide clarity with regards to anonymized data
- Strengthen CoC and certification as instruments for compliance and protection of data

2.1 Harmonization and Coherence

The GDPR has built a European data protection framework that is less harmonized then many had hoped. With a couple of dozen opening clauses for national laws and different interpretation by the DPAs in many Member States, harmonization has not yet been achieved. The Commission should therefore assess which tools can be used to complete a more coherent framework and work with the EDPB to improve the coherence mechanism.

2.2 Prevent Regulatory Overlaps

Regulatory overlaps must be avoided. As the ePrivacy Regulation is still being discussed and new legislation has already been proposed by the Commission in its Data Strategy, the Commission must ensure that data-related directives and regulations have a defined scope and that their applicability is clear for controllers so that rules do not overlap.[1]

New regulation should therefore always undergo a compatibility check with existing regulation. The current discussion surrounding the ePrivacy Regulation shows that (if not amended) there will be massive difficulties in defining the scope of application of the GDPR and the ePrivacy Regulation.

The same will be true for the data spaces the Commission introduced in its data strategy: In general, we welcome the EU's plans to create data spaces for strategic sectors. A sector

[1] Please see our elaborations on the scope of applicability in our latest Position Papers on the ePrivacy Regulation: https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Datenschutz/e-Privacy.html

focused approach can build a basis for prospective horizontal standards. To achieve this, however, the framework has to be developed in a coherent way where all sectorial approaches can fit together. With regard to all regulatory action in the field of data and data protection, we stress the necessity of coherence.

2.3 Research and Access to Health Data

The current global COVID-19 crisis has shown the importance of using data for research, the need for high quality health data and access to it. The GDPR fell short of harmonizing the framework in that regard. The restrictions of Article 9 still prevent innovative data driven projects in the health sector, such as research and AI applications that would need health data for the training of its algorithms, unintentionally.[2]

We provide detailed suggestions on how to improve research and access to health data in section 3.11.

2.4 Clarity on how to anonymize data

The use of anonymized data is of strategic relevance for data-driven business models. It could e.g. provide clarity on how to process data for secondary use and is still one of the central aspects surrounding the application of the GDPR. The added value of anonymised data is obvious: In the field of research, for example for artificial intelligence (AI) training or product development, significant progress can be made even without personal data. Anonymized data is therefore essential for the data economy and for the success of the German and European data strategy. The course initiated by the AI strategy, namely the promotion of AI applications and the establishment of Europe as a centre of excellence for AI will only succeed if data can be used to train AI. Anonymisation is one of the most promising solutions to reconcile this requirement with the legitimate interests of data protection. The political significance of the discussion on anonymization could therefore hardly be higher.

Uncertainties regarding 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

[2] We provide detailed suggestions on the necessity to improve access to health data in our latest Press Release (German): https://www.bitkom.org/Presse/Presseinformation/Bitkom-und-breites-Verbaendebuendnis-fordern-Zugang-zu-Gesundheitsdaten-fuer-die-private-Forschung

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 extensive interpretation adopted by DPAs results in many data sets not being considered anonymous.[3]

The conditions under which datasets can be considered anonymous in specific contexts need to be in line with the GDPR. Clarity on anonymization techniques and a realistic assessment of what can be considered as anonymous data in practical scenarios would help.[4]

The concepts of absolute and relative identifiability should also be revisited, ensuring that the determination of whether anonymous data can be re-identified depends on whether the controller or processor has it in his possession.[5] The existence of data elements anywhere, that if combined with data rendered anonymous enable identification, should not be sufficient. Rather, the decisive factor must be whether the controller or processor has the required data in its possession, or could reasonably obtain such data and is therefore able to re-personalise anonymous data.

2.5 Strengthen Codes of Conduct (CoC) and Certification

Approved codes of conduct are a crucial, robust but innovation-friendly transfer mechanisms. Bitkom has always promoted them and is working with other stakeholders in several working groups regarding CoCs.[6] One of the biggest benefits in our view is that CoCs can be developed by companies and industries themselves, which enables a more modern, practicable approach, which also gives flexibility of incorporating state-of-the-art technical and organizational measures, while meeting all legal requirements as set out in the GDPR. Another key advantage of codes of conduct is their thorough approval and oversight system and their confirmation by the DPAs or the European Data protection Board. Also, the compliance to a code must - in addition to the general oversight by data protection authorities - be supervised by an accredited, independent monitoring body.

CoCs have the potential to ensure a cross-border data protection framework while ensuring a rigorous oversight. At the same time, codes of conduct for third country transfers can further contribute to the proper application of GDPR and ensure a high level of data protection for European citizens, even when their personal data is processed outside of the

[3] Further elaborations can be found under section 3.16 in this Paper.
[4] Bitkom provided extensive suggestions on how to achieve more clarity and legal certainty for anonizing data here: https://www.bitkom.org/Bitkom/Publikationen/BfDI-Konsultation-zur-Anonymisierung (German Position Paper).
[5] See again our Position Paper: https://www.bitkom.org/Bitkom/Publikationen/BfDI-Konsultation-zur-Anonymisierung (German Position Paper).
[6] See f.i. here: https://www.bitkom.org/Bitkom/Publikationen/Entwurf-fuer-einen-Code-of-Conduct-zum-Einsatz-DS-GVO-konformer-Pseudonymisierung

EU. Consequently, it is important that the supervisory authorities stick to the enhanced but lean procedures under GDPR for any approvals of codes of conduct regardless whether they are related to Art. 46.

Furthermore and with regard to another effective instrument under the GDPR, the Commission should work with the involved stakeholders to speed up the process of certifications under the GDPR.

3 Suggestions for the amendments of specific provisions

The GDPR has created a good basis for data processing in the non-public sector in the European Union on the basis of uniform rules. Experience to date, however, shows that the intended harmonisation is at risk and that the implementation of the regulations is causing enormous difficulties in practice. From Bitkom's point of view, some improvements in regulation and improvements in the uniform application of the existing regulations are necessary. The following chapter is intended to shed some light on the current issues and propose solutions to improve the GDPR implementation and application.

3.1 Harmonization & Coherence

Requirement: The coherence mechanism must be mandatory for matters of general importance or with implications in more than one Member State. Greater use must be made of the urgency procedure under Art. 66 GDPR.

Situation: Unclear legal concepts are interpreted differently by national supervisory authorities (e.g. data portability, scope of requests for information etc.). This contradicts the harmonisation objective of the GDPR. In some cases, national data protection supervisory authorities issue instructions for action, without being clear whether these are permanent or whether they are still to undergo the coherence procedure and subsequently be repealed.

Problem: The lack of consideration of the coherence mechanism leads to legal uncertainty for businesses and citizens. In addition, the different interpretations lead to considerable financial consequences, as business models and processes cannot be implemented uniformly throughout Europe. It is possible that national supervisory authorities, within their respective areas of competence, take decisions on the enforcement of the DPAs which differ from decisions taken in other Member States in comparable situations. This is particularly true for different companies from the same industry in different Member States (e.g. Internet Service Provider X is treated differently in Country A than Internet Service Provider Y in Country B). This endangers the harmonisation objective and creates consid-

erable legal uncertainty for companies and citizens. Different decisions can have a considerable influence on the profitability of business models and thus also endanger the desired "level playing field".

Solution: Art. 64 para. 2 DSGVO should be amended as follows: "Any supervisory authority, the chair of the Committee or the Commission may request within a reasonable period of time that a matter of general application or with implications in more than one Member State be examined by the Committee in order to obtain an opinion, in particular if a competent supervisory authority fails to comply with the obligations to provide assistance pursuant to Article 61 or to take joint action pursuant to Article 62."

3.2 Scope of the right of access under Article 15 GDPR - Disclosure of documents

Requirement: Clarification that Art. 15 GDPR only covers the information listed in Art. 15 GDPR, but not the copies of underlying documents.

Problem: It raises the question of how the right of access under Art. 15 can be distinguished from other claims, such as Art. 20 GDPR as well as claims under public law, criminal law, civil law and in particular labour law claims for handing over documents and providing information. Art. 15 GDPR must not be developed into an all-encompassing claim to information. This would circumvent legal requirements and mechanisms that must be applied in other claims and procedures.

Solution: In Recital 63, the following sentence is inserted after sentence 6 "This right shall not include the right to obtain copies of original documents".

3.3 Scope of the right of Data Portability under Art. 20 GDPR

Requirement: Clarification that the right to data portability does not cover data which are automatically generated by the service when the data subject uses the service (e.g. log files, traffic or location data).

Facts: Art. 20 GDPR gives the data subject the right to receive personal data concerning him/her that he/she has provided to a data controller in a structured, common and machine-readable format.

Problem: The term "provided" is interpreted very broadly by supervisory authorities. It also includes data that is generated, for example, in the provision of a service by an IT system or, for example, in the network technology of a telecommunications network. This data is

necessary for the operation of a telecommunications network, but is not provided by the data subject. If the data were to be made available, the data subject would not benefit in any way if, for example, he/she were to change provider, but would involve considerable expense for the service provider. Furthermore, the broad interpretation ignores the fact that the legislator has deliberately chosen to base its decision on the data "provided" by the data subject. In the legislative process, the legislator explicitly decided against extending the right to data transferability to all processed personal data, regardless of whether the data were also provided by the data subject. The starting point was to make it possible to transfer the account data, audio or picture files from one social network to another.

Solution: In recital 68, the following sentence is inserted after the first sentence: "Data which are automatically generated by the service during the use of a service and which are by-products of the use of the service (e.g. log files, traffic or location data) are not data provided by the data subject".

3.4 Notification of personal data breaches

Requirement: Limiting notifiable data protection incidents by introducing a clear materiality threshold.

Facts: Due to the changed legal definition of a data protection incident, increased employee sensitivity in companies and the new framework for sanctions of the GDPR, the number of reported incidents has increased significantly. There is no obligation to report data protection incidents only if the violation of the protection of personal data is not expected to lead to a risk to the rights and freedoms.

Problem: The application of the undefined legal term "risk" leads to considerable legal uncertainty. In order to avoid sanctionable errors, all incidents are reported in case of doubt, regardless of the risk potentially associated with a data protection incident. The sharp increase in the number of potentially reportable incidents is overburdening companies and authorities without increasing data protection in an effective way.

Solution: In recital 85, the following sentence is inserted after the second sentence: "A foreseeable risk to the personal rights and freedoms of natural persons should be presumed where the breach of the protection of personal data concerns specific types of personal data, personal data subject to professional secrecy, personal data relating to criminal offences or administrative offences or suspected criminal offences or administrative offences, personal data relating to bank or credit card accounts or authentication data such as passwords or comparable non-publicly accessible identifiers. “

3.5 Use of different means for data protection notices and information obligations

Requirement: Clarification that the use of different means is allowed to provide the necessary information f.i. in data protection notices under certain circumstances.

Facts: According to Art. 13 GDPR, data protection information must be made available at the time of collection, but information that need to be provided to the user according to Art. 13 GDPR is very comprehensive.

Problem: If data is collected, e.g. when a contract is concluded by telephone, data protection information would have to be read out at that moment, e.g. or a pre-recorded tape would have to be played. Since Art. 12 para. 1 GDPR requires that this information be made available in an easily accessible form, it is unclear whether a so-called media break, i.e. a reference to e.g. data protection notices on the Internet, is permissible.

Solution: In Recital 58, the following sentence is inserted after the first sentence: "It should suffice if this information is not directly but easily accessible. Different media can be used."

3.6 Record of categories of processing Article 30(2) GDPR

Requirement: If the same category of processing is carried out on behalf of a large number of controllers (≥ 1000), it is sufficient - in order to complete the list pursuant to Art. 30 para. 2 GDPR - to provide the full list of names and contact details of controllers within a reasonable period of time, upon request by the supervisory authority.

Facts: The processor must list the names and contact details of each controller on whose behalf the processing is carried out in a list of processing categories.

Problem: For mass market products (e.g. cloud solution for business customers), a separate entry in the directory must be made for each individual customer, while the category of processing always remains the same. In addition, the directory has to be adjusted continuously due to the changing customer base. This can generate several thousand entries for a processing category. This leads to double data storage in addition to the customer data systems, which is also prone to errors.

Solution: In recital 82, the following sentence is inserted after sentence 2: "Where data processing categories apply to more than 1000 controllers, it is sufficient for the processor

to make the details of the controllers available within a reasonable period of time upon request by the competent supervisory authority".

3.7 Processing, deletion and return of personal data, Art. 28 (3)(g) GDPR

Requirement: In a contract between controller and processor, technical feasibility must be taken into account in the choice of the controller as to whether data are to be deleted or returned after the end of processing.

Fact: A contract must provide, inter alia, for the processor to either erase or return all personal data after completion of the processing services, at the choice of the controller, and to delete the copies that are kept.

Problem: In certain cases, due to the technical implementation of the processing, it is not possible to delete or return data selectively. Nevertheless, according to Art. 28 para. 3 g) GDPR, this option must be included in the agreement on order processing.

Solution: Art. 28 para. 3g) is worded as follows: "upon completion of the processing services, all personal data shall be deleted or returned and the existing copies deleted at the choice of the controller, taking into account the nature of the data processing and the technical feasibility of the processing, unless an obligation to store the personal data exists under Union or national law".

3.8 Misuse of the right to data access, Art. 15 GDPR

Requirement: The abusive incentive to assert information rights is prohibited.

Facts: Claims for information under Article 15 GDPR have increased considerably. Since May 25, requests for information have nearly doubled in many companies, and had even tripled during the introductory phase.

Problem: A considerable proportion of the information requests are generated by professional providers who encourage the assertion of information claims. These providers often pursue their own commercial interest towards the controller by generating the highest possible number of information requests.

Solution: Opinion of the European Data Protection Board that the incentive provided by providers with their own commercial interests to assert claims for information constitutes

a violation of the principle of data avoidance or data minimization which is to be prohibited.

3.9 Anonymization

Requirement: The established and so far legally permissible anonymization of personal data for the purpose of further processing remains possible and is incentivized.

Facts: To date, the anonymization of personal data for the purpose of further processing of these anonymous data has been established and agreed upon with data protection authorities. Business models based on this are commercially successful.

Problem: The anonymization of personal data for the purpose of further processing of this anonymous data is being questioned because of the allegedly new processing concept of the GDPR, although the term does not differ from the definition in Directive 95/46 EC.

Solution: The processing concept of Art. 4 No. 2 GDPR corresponds to the processing concept of Art. 2 b) of Directive 95/46 EC. The European Data Protection Board should clarify that anonymization permitted under Directive 95/46 EC is also permitted under the GDPR. Previously established procedures should be reviewed with a sense of proportion and, in this assessment, the continuation of provisions from Directive 95/46 EC in the GDPR should be taken into account.[7]

3.10 Grounds for processing - scope

Request: Clarification of the scope of the three legal bases, performance of a contract, processing on the basis of legitimate interests of the controller and consent, and their relationship to each other.

Fact: Currently, personal data is being processed in comparable situations on very different legal bases, depending on the legal opinion of the data controller. The supervisory authorities do not provide sufficient assistance.

Problem: The processing of personal data in comparable situations on the basis of different legal bases hinders harmonisation under the GDPR and leads to legal uncertainty for the data controllers. Depending on the legal basis, data controllers must take into account very different requirements for processing. It is unclear where the purpose of the pro-

[7] For details regarding Anonymization please see the Bitkom Position Paper on the public consultation of the BfDI in Germany (German Position Paper):
https://www.bitkom.org/Bitkom/Publikationen/BfDI-Konsultation-zur-Anonymisierung

cessing, which is covered by the legal basis of "performance of a contract", end and the need for a new legal basis such as consent or protection of the data controller's legitimate interests begins.

Solution: Guidelines of the European Data Protection Board, which provide assistance to data controllers on the scope of the legal basis for processing provided for in the GDPR, in particular for the performance of a contract, processing for the purpose of safeguarding legitimate interests and consent. The current Guidelines do not elaborate enough on the scope and the relationship between the different legal bases for processing.

3.11 Uncertainties on the applicability of Member State laws and/or GDPR

In the GDPR's current version, it is partly unclear whether a provision actually constitutes an opening clause or not (e.g. with regard to Art. 85(2) GDPR). Hence, there is uncertainty to which extent (existing) national laws apply.

With regard to national legislation based on the GDPR's opening clauses, there is partly reason to doubt whether national law can actually be assessed as compliant implementation (e.g. § 4 German Federal Data Protection Act). As a consequence, companies have to decide whether they comply with national law – thereby maybe infringing EU law – or if they observe the requirements of the GDPR only.

It is unclear whether the GDPR is applicable if a controller which has no establishment in the EU, collects personal data on the territory of the EU but without triggering Art. 3(2) GDPR, i.e. not offering goods or services or monitoring behaviour of data subjects. Example: a controller from outside the EU asks data subjects within the EU to participate in a survey or trial, not offering any goods or services in return.

3.12 Uncertainties with regard to further processing of data

A harmonized 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 of Art. 6(4) GDPR.

In addition, it is unclear what Art. 89(1) GDPR in conjunction with Art. 5(1)(b) renders a further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes as not incompatible with the initial purposes. What is meant by "appropriate safeguards" has to be further specified; otherwise the intended privilege will not be achieved due to existing legal uncertainties.

Furthermore, the relationship between consent and other forms of legal justifications of processing of personal data remains unclear. Example: when consent as the original legal basis is withdrawn, there is uncertainty regarding the possibilities of further processing on the basis of a legal justification as set out in Art. 6(1)(b) to (f) GDPR - is the change to an alternative legal basis permissible?

3.13 Uncertainties with regard to clinical trials

In the area of clinical trials - contrary to the objectives of GDPR - diversification on the following topics and differing interpretations in the EU Member States are obvious:

- Legal basis for data processing in clinical trials
- Question of controllership in clinical trials

These topics are very relevant for the set-up of global clinical trials in Europe. The related legal uncertainties hinder standardization and drive complex discussions with clinical trial sites, Ethics Committees and clinical trial service provider. This has already led to massive delays in starting such trials, giving rise to medical and ethical questions as patients with life-threatening diseases are concerned. The role of Europe as one of the main regions where clinical trials are conducted is at stake.

Until today, we often notice a lack of aligned interpretation regarding the term "scientific research" as mentioned in Recital 33 and Article 5(1)(b) GDPR. In April 2019, the German Data Protection Conference (DSK) published its decision on the interpretation of Recital 33: "... data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognized ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose".

In its decision, the DSK elaborates on the following:

It is not allowed to generally extend the usage of collected data to certain areas of scientific research. Only in a limited number of cases a broad consent can be used (limited to situations where at the time of collecting the data it is not possible to fully describe the purpose of data collection in detail). In such "single cases" a number of additional measures need to be implemented, providing transparency, trust and data security.

Amongst the listed measures, one point particularly raises concerns, generally prohibiting the transfer of personal data to third countries not ensuring an adequate level of data protection.

Leaving aside the imprecision of this decision by German supervisory authorities, it raises the concern that if these rules are applied, they would have a severe impact on any transatlantic co-operation between institutions or companies in Germany and (for instance) US research institutions with a transfer of (pseudonymized) patient data in scope.

The One Stop Shop mechanism of Art. 56 GDPR is interpreted inconsistently by local supervisory authorities. This provokes not only legal uncertainties for international companies with cross-border processing activities but also leads to a significant administrative workload in case of incidents, both elements were meant to be avoided by the One Stop Shop approach of GDPR.

The GDPR does not connect "profiling" as defined in Art. 4(4) GDPR with any special legal, technical or organizational requirements. It, therefore, does not have any independent (legal) meaning within the GDPR framework. The term is only mentioned in the context of other provisions ("...including profiling"). Moreover, the term profiling is in practice often mixed up with the term "automated decision making". Hence, to avoid any unnecessary confusion the term "profiling" and its definition should be deleted.

3.14 Data Subject Rights

Art. 13 and 14 GDPR provide for very detailed and comprehensive sets / catalogues of data privacy information requirements. In many cases that leads to a technical and organizational effort that is disproportionate to the specific situation / circumstances of data processing (in particular in situations where data processing takes place at the request / wish of the data subject).

The relation between paragraph 1 and paragraph 2 of Art. 13 GDPR respectively Art. 14 GDPR is not clear. (When) can the transparency requirements provided for in paragraph 2 be waived because they are not necessary for fair and transparent processing?

In many situations, it is difficult / not possible to fulfil data privacy information obligations in a practical way, both for the company and for the data subjects. This applies e.g. to the collection of personal data via telephone. A fully fletched / comprehensive privacy statement, e.g. by tape announcement, is time-consuming and hardly likely to have the desired effect of a more transparent data processing. In this context, a clear positioning on the topic of media discontinuity ("Medienbruch") would be desirable (see also above).

It remains unclear if all information on data subject rights under Art. 13 or 14 GDPR need to be provided, also in cases where a specific data subject right does not apply. Example: is a controller obliged to inform about the deletion right if data are only processed as long as it is necessary for compliance with a legal obligation? Or would in such case information about the right to erasure not even be misleading as it would not apply?

The exceptions from data deletion requirements stipulated in Art. 17(3) GDPR do not contain the right to restrict further processing instead of deletion and/or to make use of standardized deletion routines in case deletion would require disproportionate technical or organizational efforts. In particular where controllers have to rely on third party providers which only provide for standard deletion routines this can lead to significant compliance risks for controllers.

3.15 Transfers to third countries

There is a strong need for a set of standard contractual clauses for cross-border transfers between an EU-based processor and a non-EU-based sub-processor. Until today, conclusion of the standard contractual clauses set EU controller to non-EU processor is necessary. This mechanism does however not correspond to the contract or service chain and often requires a significant clarification / explanation effort on the part of the controller and / or processor.

It would be highly appreciated if the Commission were to make use of Art. 28(7) GDPR to lay down standard contractual clauses for the matters referred to in Art. 28(3) and (4) GDPR. Such standard contractual clauses may have the potential to serve as a widely used and accepted best practice template and, thereby, may lead to a significant reduction of cost and time consuming contract negotiations between controller and processor.