Independent German Federal and State Data Protection Supervisory Authorities

Report on Experience Gained in the Implementation of the GDPR

November 2019

Table of contents

Introductory overview

The following report on experience gained in the implementation of the General Data Protection Regulation (GDPR) was drawn up by the Conference of Independent German Federal and State Data Protection Supervisory Authorities (*Datenschutzkonferenz* (DSK)) and adopted at its 98th Conference on 6 November 2019. Since the date of application of the GDPR the German supervisory authorities represented in the DSK have gained experience of its application in practice. By publishing this report the DSK would like to contribute that experience to the evaluation and review process required in accordance with Article 97 of the GDPR and, following on from that, to make suggestions for improving some aspects to ensure optimal implementation of the Regulation.

In July 2019, one year after the GDPR's date of applicationapplication, the European Commission's assessment was rightly a positive one. The GDPR, it concluded, was ensuring that increasing numbers of EU citizens were aware of data protection legislation and of their rights, and businesses were adapting their practices, increasing the security of their data and turning data protection into a competitive advantage. The Regulation had, the European Commission reported, given the national data protection authorities more powers in regard to enforcement. Within the first year, the national data protection authorities had, where necessary, made effective use of these new powers and they were working together more closely within the framework of the cooperation mechanism, it stated.

The DSK shares the view that the GDPR's regulatory concept and objectives have largely proved a success. It feels that the GDPR has ensured that progress has been made on achieving the goals of improving the protection of fundamental rights and creating a harmonized Digital Single Market, and that these goals are in fact achievable.

The fact that now, for the first time, there is a risk of incurring heavy fines for violations of data protection provisions has proved a key aspect of public perception as well as a driver for developing broad-based awareness of privacy and data protection. Authorities and businesses are facing up to the resulting challenges. Nevertheless, some uncertainty remains and there are shortcomings when it comes to implementation. There are diverse requirements (in the GDPR itself, e.g., the Recitals and in guidelines) which controllers must fulfil, necessitating comprehensive data protection management on their part. Those requirements first need to be interpreted – and there are countless data protection consultants offering such interpretations. There is still a very great need for guidance from the supervisory authorities, which they have met by doing a great deal of consultancy work. The core of this work consists in weaving a common thread out of the increased number of legal and information resources so that they can give controllers pragmatic recommendations for action. The task now is to maintain and expand on the resulting increased level of acceptance of data protection law and of the work of the supervisory authorities.

Thus, the greater demands made on the supervisory authorities on account of the huge rise in the number of complaints, effortful international cooperation (in the Internal Market Information System (IMI)) and more intense consultancy work has not always been matched by an appropriate increase in human and material resources. In accordance with Article 52(4) of the GDPR, each Member State must ensure that its supervisory authority is provided with those resources which are necessary.

As a result, some supervisory authorities are not in a position to carry out the requisite number of inspections without cause, and controllers have identified a shortfall in the number of checks being

carried out and they are letting up in their own efforts to ensure compliance with data protection regulations.

In addition to the topics which must, in accordance with Article 97(2) of the GDPR, form part of the Commission's evaluation and review of the Regulation, the report at hand also focused on identifying whether, based on experience gained implementing the GDPR in the course of its first year of validity, there is any need to make any changes – both in terms of amending existing provisions and possibly introducing new ones. Account was hereby also taken of the Regulation's Recitals.

This report does not look into possible problems implementing the GDPR in legislation applicable at federal and federal state level in Germany. Nonetheless, where individual national implementing provisions appear problematic or deserving of criticism, this may result in the need to adapt the GDPR's flexibility clauses.

Questions of clarification, interpretation, definition and translation were not taken into account either or were reduced to essential points. Contentious issues which began to emerge during the legislative process and which have proved problematic in the course of implementation were likewise largely ignored.

The following key issues have emerged in the course of implementing the GDPR:

1. Making life easier & practicability
2. Data breach reports
3. Purpose limitation
4. Data protection by design
5. Supervisory authorities' powers and sanctioning practice
6. Provisions on competence & cooperation and consistency
7. Direct marketing
8. Profiling
9. Accreditation

It has become clear that problems arise when it comes to implementing the **information and transparency requirements** set out in Articles 13 and 14 of the GDPR in practice, for instance during data collection by telephone. The main question here is whether it is sufficient to provide more general information in the first instance and subsequently give specific information only upon request. The extent and content of the information duties could possibly be defined in a more practicable, citizen-centred way. One question which is sometimes raised in practice is whether the regulations in the GDPR are actually **suitable for everyday use**. The report at hand focused on how the duties to provide information, the duty to communicate data protection officers to the supervisory authorities and the right to a copy in accordance with Article 15(3) of the GDPR could be more easily applied.

Based on the supervisory authorities' experience, growing concern about possibly incurring a penalty under the GDPR is leading to **data breaches** often being reported although no data breach has, in fact, occurred or whose risks have already been eliminated. That explains the exorbitant rise in the number of data breach reports.

When it comes to **purpose limitation**, questions in particular arose in practice in relation to the legal basis and requirements for the further processing of personal data where the purpose of the processing changes.

Data protection by design has hardly caught on in practice, given that the scope of the GDPR specifically does not include producers. The principles of data protection by design/by default do in fact relate to producers, but the GDPR does not impose any obligations on them in their capacity as controllers. This thus raises the question of whether obligations should also be imposed on producers, suppliers, importers and traders as is already the case under product liability law.

Within the context of **supervisory authorities' powers and sanctioning practice**, questions specifically around the term "processing operation" in point (b) of Article 58(2) of the GDPR, cooperation between the supervisory authorities and their right of information in regulatory fines proceedings have proved especially pressing. In another issue referred to in point (b) of Article 97(2) of the GDPR, the supervisory authorities' experience of **provisions on competence & cooperation and consistency** are also addressed in detail.

When it comes to **direct marketing**, the question of admissibility is raised in various contexts which could be resolved by creating a specific legal basis.

Profiling is regarded as one of the key data protection policy challenges of our times. Although a generally accepted definition of this term is already available, most of the provisions in the GDPR (e.g. those on automated decision-making) do not cover profiling as such. As a result, assessments usually have to be based on the general elements set out in Article 6 of the GDPR. The DSK calls for the applicable legal framework to be tightened in order to be able to set effective and enforceable limits to the use of personal data for the purposes of profiling.

As regards the key issue of **accreditation**, further clarification in the GDPR might be able to resolve a major question which has arisen in Germany regarding competence and thus ensure oversight by the German data protection supervisory authorities.

A short table of other suggested amendments lists concrete textual changes, including a brief explanation, which cannot be assigned to any of the above key issues but which would also make it easier to apply the GDPR.

The DSK also includes as an Annex its Hambach Declaration on Artificial Intelligence – Seven Data Protection Requirements of 3 April 2019 by way of information. The Hambach Declaration addresses the prevailing topic of scientific debate: data protection in the field of **artificial intelligence** and automated decision-making. Although the demands made in the Declaration refer to future cases and legislative contexts, the German data protection supervisory authorities believe that it is essential that these principles be observed in future evaluation and review processes.

Key issue no. 1: Making life easier & practicability

In its consultancy and case work and in its dealings with controllers, the German data protection supervisory authorities have often met with a lack of understanding for the rules and regulations in the GDPR, the extent of the information obligations and the record of processing activities, as well as for the need for privacy and data protection impact assessments. Small and medium-sized enterprises (SMEs) in particular as well as not-for-profit associations in Germany feel that the GDPR requirements place an excessive burden on them and they have called for exemptions to be made.

I. Information obligations

1. Outline of the problem

The obligations to provide information and transparency set out in Articles 13 and 14 of the GDPR form part of the core of the General Data Protection Regulation (GDPR). The German supervisory authorities feel that the matter set out in in Article 12(1) of the GDPR, among other provisions, namely that data subjects be provided with information about their data protection rights in an intelligible and appropriate form, represents one of the key innovations of the Regulation.

Some of the German supervisory authorities reported hearing concerns that complying with these information obligations may possibly impose too great a burden on controllers in non-profit societies/associations and SMEs, for instance. However, even small entities may be processing data in a manner which has far-reaching consequences for data subjects.

Some controllers have, further, referred the German supervisory authorities to problems which arise in the fulfilment of the obligation to provide information in certain contexts, such as arranging appointments or concluding a contract by telephone, and the associated data collection.

One possible solution would be to make an exemption for non-profit societies/associations and SMEs employing fewer than 250 people in analogy with Article 30(5) of the GDPR. Another possible solution, which takes the risk to data subjects as its point of reference, would be to reduce the information obligations in cases in which the data processing is of a very limited extent and where the processing meets the expectations of data subjects.

2. Assessment

The supervisory authorities are in principle in favour of making things easier in individual practical contexts, but warn against introducing general exemptions from the obligations imposed on controllers.

The experience which supervisory authorities have gained when advising businesses whose data processing is chiefly done in the context of customer relations has shown them there is a need, in certain cases, to relieve controllers of some of their information obligations. A distinction can here be drawn between digital and analogue contexts.

It is, as a general rule, easy to meet information obligations in a digital context. Under sentence 2 of Recital 58 of the GDPR, information may be provided in electronic form at the point where data are collected. Where the controller is a website operator, it can be expected to provide the requisite information "in a concise, transparent, intelligible and easily accessible form, using clear and plain language".

However, in certain analogue contexts the need, in accordance with Article 13 of the GDPR, to provide information at the time when data are collected raises practical questions. Especially in the case of verbal or telephone contact in a business setting it is unrealistic to expect the controller – when taking an order, accepting a business card or making note of an appointment – to provide comprehensive information in accordance with Article 13(1) and (2) of the GDPR, that is to state the legal basis and the competent data protection supervisory authority or to advise on rights of information and complaint as well as other rights accorded to data subject and much else. Such information will likely often be met with incomprehension on the part of the data subject and might be regarded as bothersome.

Article 13(4) of the GDPR pragmatically rules out the obligation to provide information where and insofar as the data subject already has that information; especially in the context of B2C relations, when they place an order many customers will already be aware of the information the controller is required to provide. Nevertheless, it is in principle impossible to assume that customers are aware of the legal basis for the data processing, for example (see point (c) of Article 13(1) of the GDPR). This is not of interest, however, every time an order is placed or an appointment is arranged, for instance. Data subjects have often complained about information overload in such situations. Taking the risk-based approach, for example when commissioning a handicraft business with low-risk data processing, it would, from the data subjects' perspective, be sufficient for them to be told where they can find the relevant information.

In keeping with the Working Paper put forward by the Article 29 Working Party (Guidelines on transparency under Regulation 2016/679; WP 260 rev.01), the German supervisory authorities advocate permitting a tiered approach when it comes to fulfilling the obligation to provide information in accordance with Article 13 of the GDPR. In appropriate cases, the requisite information can, for example, also be provided when forwarding an order confirmation, by displaying it in a shop or in other similar ways. General exemptions should, however, be avoided as they would go against the purpose of the provision.

3. Proposed amendment

Insertion of a new paragraph in Article 13 of the GDPR:

5. The information referred to in paragraphs 1 and 2 shall only be provided if requested by the data subject in cases where the controller is responsible for data processing which the data subject can expect or must expect given the specific circumstances and

(a) both the disclosure of data to third parties and their transmission to third countries is ruled out,

(b) no data are processed which are subject to the provisions of Article 9,

(c) the data are not processed for direct marketing purposes and

(d) neither profiling nor automated decision-making will be carried out.

The data subject shall be informed about this possibility.

In addition, an exception should be made to the obligation to provide information at the time when data are collected in those cases in which data are processed on the basis of point (d) of Article 6(1) of the GDPR.

The aim is to indicate that a risk-based approach is being applied when it comes to making things easier in everyday life.

II. Right to a copy pursuant to Article 15(3) of the GDPR

The right of access under Article 15 of the GDPR is one of the core rights accorded to data subjects. Without information about how their personal data are processed data subjects cannot effectively assert other rights, such as the right to rectification or erasure, or to lodge a complaint with a supervisory authority.

Nevertheless, the scope of the right of access is a matter of controversial debate, especially the extent to which Article 15(3) of the GDPR accords a "right to a copy". Such a right could enable data subjects to require that the controller hand over all personal data processed in their original context. In practice, data subjects have asked controllers to hand over all the documents containing personal data it has, sometimes without further specification. This right can, for example, require an authority to provide a copy of the entire case file or that a company hand over each and every business email sent and received by a former employee.

It would be desirable to clarify the scope of the right granted under Article 15(3) of the GDPR.

III. Duty to communicate the contact details of data protection officers pursuant to Article 37(7) of the GDPR

1. Outline of the problem

Article 37(7) of the GDPR currently establishes a duty to communicate the contact details of data protection officers to the supervisory authority. Controllers and processors must guarantee that the information communicated is always up to date. They must store these communications and, where necessary, notify the competent supervisory authority of any corrections to be made.

The duty not only to publish the contact data but also to communicate them to the supervisory authorities and to keep them up to date creates additional work for controllers. This leads to unnecessary data processing on the part of the supervisory authorities when they receive the initial communication and notifications to amend and delete specific information. In some cases Article 37(7) of the GDPR is interpreted to mean that the supervisory authorities have to keep a register of data protection officers (including an obligation to ensure its completeness and eliminate inconsistencies *ex officio*). Completeness and correctness can, however, only ever be striven for but never fully attained. Given that, in the non-public sector, no decision can be taken on whether the duty to designate a data protection officer exists without more detailed knowledge about the controller's organizational structure or business model, extensive data collation is necessary in the context of hearings.

2. Assessment

Given the duty of publication (first clause of Article 37(7) of the GDPR), it is in practice unnecessary for the supervisory authorities to store contact data on the data protection officer(s). Up-to-date contact details on the data protection officer(s) could be notified whenever a supervisory authority makes initial contact with controllers.

To relieve the burden on controllers, processors and data protection supervisory authorities, this reporting duty and the needless data processing, which is also unsuitable given the lack of currency of the notifications, should be dropped.

3. Proposed amendment

The second clause in Article 37(7) of the GDPR ("and communicate them to the supervisory authority") should be deleted.

Key issue no. 2: Notifications of personal data breaches

I. Article 33(1) of the GDPR

1. Outline of the problem

Under Article 33(1) of the GDPR, in general each personal data breach must be notified to the supervisory authority. An exception is only made when the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. No. 12 of Article 4 of the GDPR defines a personal data breach as a breach of security leading to destruction, loss, alteration or unauthorised disclosure; it thus corresponds to point (f) of Article 5(1) of the GDPR. According to Recital 85 of the GDPR, a breach of security may result in physical, material or non-material damage.

Since under previously applicable German legislation (section 42a of the Federal Data Protection Act, old version) only breaches of specific types of data needed to be notified, the number of notifications has increased considerably in Germany. Controllers are also faced with the difficulty of assessing when there is no risk to the rights and freedoms of natural persons. It is likely that this risk will often be dependent on factors of which controllers are not aware. Further, many controllers notify alleged breaches without first having done a risk assessment because they are afraid of incurring hefty fines. The very broad scope of paragraph 1 ("unlikely to result in a risk") thus leads to very many trivial and minor cases being notified, placing a heavy burden on the supervisory authorities and, ultimately, resulting in them failing to spot the truly relevant cases.

2. Assessment

A risk to the rights and freedoms of natural persons cannot, generally, be entirely ruled out. The notification obligation should therefore be limited to those cases which are likely to result in more than merely a minimal risk to the rights and freedoms of natural persons.

Further, Article 33(1) of the GDPR should be expanded to include those cases in which it is not known whether a personal data breach has occurred but it be assumed to be the case. Often, a breach of data security has occurred but it is not known whether it has led to any personal data breach within the meaning of Article 4 no. 12 of the GDPR.

An example: A dump (copy) of an extensive customer database was freely accessible on the Web for many months but logfiles which can block access are available only for a few days. There can be no finding of a breach within the meaning of Article 4 no. 12 of the GDPR (depending on how "disclosure" is defined).

Where it is probable that a personal data breach has occurred, there should be an obligation of notification to the supervisory authoritie if there is likely to be a high risk to the rights and freedoms of data subjects.

3. Proposed amendment

Insertion of new sentences 1 and 2 in Article 33(1); sentence 2 to become sentence 3:

In the case of a personal data breach which is likely to result in more than minor risks to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55. Further, the controller shall notify a breach against the requirements of the security of processing pursuant to Article 32(1) of the GDPR

which probably led or will lead to a personal data breach without undue delay and, where feasible, within 72 hours of having become aware of the breach of security if the personal data breach will likely result in a significant risk to the rights and freedoms of the data subjects.

Key issue no. 3: Purpose limitation

1. Outline of the problem

Purpose limitation is one of the basic principles of data protection legislation. It is of very great practical relevance to data subjects to know whether data they have disclosed to a controller for specific purposes may be used for other purposes. The GDPR therefore makes special requirements in respect of uses for other purposes and requires controllers to provide information when data processing for other purposes is permitted.

There is disagreement as regards the application of Article 6(4) GDPR, namely whether a separate legal basis is needed for processing for purposes other than that for which data were collected where the conditions of Article 6(4) of the GDPR in terms of compatibility of the two purposes are met. When processing data which is strictly purpose limited under the law which permits them to process the data, for instance, controllers rely on the fact that, under sentence 2 of Recital 50 of the GDPR, no separate legal basis is necessary for them to be able to process data for other purposes if the new purpose is compatible with the old one. By contrast, however, data subjects who have, for example, disclosed personal data to a controller without any legal obligation to do so have a keen interest in being able to take a decision about whether to disclose their data again before they are processed for another purpose. Making reference to point (a) of Article 5(1) read in conjunction with Article 6(1) of the GDPR and to sentence 8 of Recital 50 of the GDPR, German supervisory authorities have, in such cases of conflict, called for data processing for purposes other than that for which the data were collected to also require a legal basis.

Notwithstanding this specific question, the scope of the privileges accorded to science and scientific research in point (b) of Article 5(1) read in conjunction with Article 6(4) of the GDPR has proved to be too wide in practice.

2. Assessment

In accordance with point (a) of Article 5(1) read in conjunction with Article 6(1) of the GDPR, each data processing must meet at least one of the conditions referred to in Article 6(1) of the GDPR in order to be lawful. Lawfulness (point (a) of Article 5(1) of the GDPR) and purpose limitation (point (b) of Article 5(1) of the GDPR) are two separate data processing principles. Article 6(4) of the GDPR concerns the principle of purpose limitation. If this provision were supposed to have included an exemption to the need for a legal basis, then, given the significance and consequences of such an exemption, that should have been explicitly included in the Regulation.

Article 6(4) of the GDPR only refers to the compatibility of the two purposes. Sentence 1 states that where processing occurs for a purpose other than that for which the personal data were collected and it is not based on the legal basis provided under point (a) of Article 6(1) of the GDPR or specific Union or Member State law, then it must be ascertained whether the two purposes are compatible. According to the wording of the provision, that does not mean that ascertaining compatibility in a case where processing for a purpose other than the original purpose is a substitute for a legal basis, but that where processing for another purpose has another legal basis, it must be ascertained whether the two purposes are compatible. The rule itself thus actually does imply that all processing for purposes other than those for which data were collected must have a legal basis.

Therefore, the assertion made in sentence 2 of Recital 50 of the GDPR is confusing, namely that if the two purposes are compatible "no legal basis separate from that which allowed the collection of the personal data is required".

Even though sentence 8 of that Recital states that the principles set out in the Regulation are always applicable, this cannot entirely eliminate the confusion, since the contradiction between sentence 2 (which only refers to the legal basis) and sentence 8 of Recital 50 of the GDPR (which refers to all principles) remains. Some regard the fact that sentence 2 was retained in Recital 50 to be an editorial error following the trialogue negotiations. In practice, it creates huge difficulties when it comes to enforcing the requirement of the lawfulness of processing for another purpose, and it should therefore be deleted.

3. Proposed amendments

Deletion of sentence 2 of Recital 50 of the GDPR.

Clarification in Article 6(4) of the GDPR: Further processing of data on the basis of paragraph 4 to be limited to that which is carried out by the same controller.

Key issue no. 4: Data protection by design

1. Outline of the problem

Producers, suppliers, importers, traders etc. should be subject to the obligations as it is already regulated by product liability law (Germany's Product Liability Act and Council Directive 85/374/EEC).

In practice, the term "data protection by design", a requirement applicable to controllers laid down in Article 25(1) of the GDPR, is not broad enough to cover the target group.

Controllers do not generally develop hardware and software themselves. They are largely reliant on available hardware and standard operating systems and application software. Monopolies and oligopolies often exist on the supplier side, as a result of which suppliers are able to dictate what products are used as well as the terms and conditions of that use.

The GDPR's data protection by design/by default principles are geared to producers but do not impose any obligations on them in that capacity. The call for data protection by design/by default thus often comes to nothing if it is directed only at controllers.

In the interests of promoting privacy and data protection, the GDPR should, therefore, also oblige software producers to comply with this design principle. In practice, it will in particular apply to the producers of complex software, such as operating systems, database management systems, standard office bundles and very specific specialist applications.

The following two examples make this clear:

1. Operating systems

Controllers which operate servers, desktop computers, laptops, tablets, smartphones or similar devices are reliant on using one of the few, generally pre-installed, operating systems available on the market. As the law currently stands, these controllers are obliged to find and remedy any weak points which are relevant to privacy and data protection, as well as misconfigurations and functions which are, in their eyes, undesirable. The producers are under no obligation to deliver products without such faults.

2. Front door lock cylinders with app

Locking systems are now available for front doors which do without a physical key. Users identify themselves using an app on their smartphone. Data are exchanged between the app and the producer (which is located in a third country with no adequate level of data protection).

a) Where an enterprise uses such systems, the enterprise itself is the controller and thus responsible for data processing into which it has no insight. The producer is not a tangible presence in such contexts.

b) Where natural persons use these systems in the course of a purely personal or household activity, there is no controller within the meaning of the GDPR. No-one is responsible under the GDPR, and the duties laid down in the Regulation come to nothing. Privacy and data protection would benefit greatly if the importer or trader, for instance, could be held accountable.

2. Assessment

As the law currently stands it contradicts the principles of data protection by design and by default.

Contrary to sentence 4 of Recital 78 of the GDPR, producers are in no way encouraged "to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations".

There are, thus, not only considerable loopholes in terms of the privacy of personal data (as well as of other data, see also Directive (EU) 2016/943), the technical and administrative burden also increases exponentially when one attempts to eliminate shortcomings decentrally which have been caused centrally. Burdens are imposed on all controllers and processors, with SMEs carrying a disproportionate burden.

As the law currently stands it thus also contradicts generally applicable law. Under product liability law, which was harmonized on the basis of Council Directive 85/374/EEC, producers are liable for damage arising on account of their products. Importers, suppliers etc. are also liable for such damage. This harmonization also needs to be transferred to personal data privacy.

The aim should, therefore, be to impose greater responsibility on producers for products which affect privacy and data protection.

3. Proposed amendments

The following (underlined) amendments would impose obligations on producers etc. under the GDPR but would also leave their enforcement to consumer protection law and, possibly, competition law.

Article 4

Definitions

For the purposes of this Regulation:
[…]

(27) "producer" means the producer as defined in Article 3 of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. Point (a) of no. 16 shall apply accordingly. If the producer determines the purposes and means of the data processing, the producer shall also be the controller within the meaning of no. 7.

CHAPTER IV

Controller and processor, producer

Section 1

General obligations

Article 24

Responsibility of the controller and of the producer

[…]

4. The producer shall be required to develop and design its products, services and applications with due regard to data protection law and the state of the art to ensure that controllers and processors are able to fulfil their data protection obligations without having to make unreasonable modifications to those products, services and applications. The producer shall provide the requisite information upon request, thus supporting controllers and processors when it comes to drawing up records of processing activities (Article 30), notifying personal data breaches to the supervisory authority (Article 33) and communicating personal data breaches to data subjects (Article 34).

Article 79

Right to effective judicial remedy against a controller, processor or producer

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

2. Proceedings against a controller, a processor or producer shall be brought before the courts of the Member State where the producer, controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller, processor or producer is a public authority of a Member State acting in the exercise of its public powers.

Article 82

Right to compensation and liability

[…]

7. Where the damage is based in whole or in part on actions or omissions by the producer, the producer, in addition to the controller or processor, shall be liable to the data subject. The producer shall also be liable to the controller and the processor.

Key issue no. 5: Powers of the supervisory authorities and sanctioning practice

I. Powers

1. Outline of the problem

The term "processing operations" as used in point (b) of Article 58(2) of the GDPR creates problems when it comes to applying the provision. The GDPR contains various duties which are independent from a concrete processing, such as designating a data protection officer (Article 37 of the GDPR) or a representative (Article 27 of the GDPR), or the duty to maintain a record of processing activities (Article 30 of the GDPR). It is therefore not clear for supervisory authorities on which legal basis they can issue a reprimand in the case of breaches of these duties.

2. Assessment

The principles which processing must comply with are set out in Article 5 of the GDPR and detailed further in other provisions in the Regulation. The GDPR contains duties which are independent of these processing principles. At least when it comes to the designation of a data protection officer or representative, or the duty to maintain a record of processing activities it is not apparent that these constitute one of the principles of processing set out in Article 5 of the GDPR. Therefore, a breach of these principles does not lead to processing becoming unlawful in an individual case. It is, however, necessary to be able to issue reprimands following such breaches in practice. To avoid contradictions arising, this option should be available for all contraventions of the Regulation.

The sanctions in Article 83 of the GDPR, by comparison, also do not take processing operations as their point of reference, only "infringements of this Regulation" (paragraph 1) and "infringements of the following provisions" (paragraphs 4 and 5).

3. Proposed amendments

No limitation of the powers under Article 58(2) of the GDPR to processing operations.

Article 58

Powers

2. Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that ~~intended processing operations are~~ it is likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where ~~processing operations have~~ it has infringed provisions of this Regulation;

[…]

(d) to order the controller or processor to bring processing operations, measures or the fulfilment of obligations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

II. Point (e) of Article 83(5) of the GDPR: Sanctions, elements of a breach against an order issued by the supervisory authority pursuant to point (a) of Article 58(1) of the GDPR

1. Outline of the problem

Under point (a) of Article 58(1) of the GDPR, the supervisory authority can order the controller/processor "to provide any information it requires for the performance of its tasks". This right on the part of the authority to request information obliges the controller/processor to assist the authority in the performance of its tasks.

Under point (e) of Article 58(1) of the GDPR, the supervisory authority also has the investigative power to obtain "access to all personal data and to all information necessary for the performance of its tasks". This right of access enables the supervisory authority not only to obtain information but also to inspect internal documents, databases and procedures (e.g. Ehmann/Selmayr, *Datenschutzgrundverordnung* Art. 58 margin no. 16). Given this distinction, the failure or the refusal to provide information can be subsumed under point (a) of Article 58(1) of the GDPR.

In accordance with point (e) of Article 83(5) of the GDPR, a fine can only be imposed in the case of non-compliance with an order pursuant to Article 58(2) of the GDPR or in the case of failure to provide access in violation of Article 58(1) of the GDPR. By contrast, penalties can be imposed for infringements of the duty to cooperate, for instance the refusal to provide information in accordance with point (a) of Article 83(4) read in conjunction with Article 31 of the GDPR.

2. Assessment

The supervisory authorities are in disagreement as to whether this is the right place for a provision dealing with the failure to provide information or the refusal to grant access. First, Article 31 of the GDPR is understood by at least some of the writers of commentaries to mean that the duty to cooperate is triggered by a request on the part of the supervisory authority which does not need to constitute an administrative act, i.e. which tends to occur during preliminary investigations during the clarification of the facts. However, a distinction needs to be drawn between such clarification of the facts and the formal assertion of an authority's right to information under point (a) of Article 58(1) of the GDPR. As a result, different penalties should also be imposed for infringements of these different duties.

Second, the authorities criticize inconsistencies in interpretation, since point (a) of Article 83(4) read in conjunction with Article 31 of the GDPR sets a considerably lower fines corridor than, for instance, the failure to grant access in accordance with point (e) of Article 83(5) read in conjunction with Article 58(1) of the GDPR.

Thus, the same penalties should be imposed in the case of infringements of point (a) of Article 58(1) of the GDPR as in the case of the failure to grant access in violation of points (e) and (f) of Article 58(1) of the GDPR. Constituent elements of an infringement against an order in accordance with point (a) of Article 58 (1) of the GDPR should, therefore, be included in point (e) of Article 83(5) of the GDPR.

3. Proposed amendment

Amendment of point (e) of Article 83(5) of the GDPR:

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2), non-compliance with an order to provide information, or failure to provide access in violation of points (a), (e) and (f) of Article 58(1).

Key issue no. 6: Provisions on competence & cooperation and consistency

I. Article 46(4) read in conjunction with Article 64(2) of the GDPR

1. Outline of the problem

It is not clear from the text of the legislative act whether the consistency mechanism needs to be triggered for each administrative arrangement which is to serve as the basis for the international transfer of data and is thus submitted to the competent supervisory authority pursuant to point (b) of Article 46(3) of the GDPR for authorization. This is provided for in Article 46(4) of the GDPR for all cases referred to in paragraph 3. Point (e) of Article 64(1) of the GDPR, however, only refers to the authorization of contractual clauses referred to in point (a) of Article 46(3) of the GDPR.

The background is as follows: The European Data Protection Board (the Board) issued an opinion regarding the ESMA/IOSCO administrative arrangement pursuant to Article 64(2) of the GDPR. Whether this procedure should in future be applied to all administrative arrangements or only to multilateral agreements is still a contentious issue between the ITES and COOPESG.

2. Assessment

There is a real need for clarification as to whether administrative arrangements as referred to in point (b) of Article 46(3) of the GDPR need to be submitted to the Board. From the German perspective they should. Nevertheless, the consistency mechanism as referred to in Article 64(2) of the GDPR should be applied in such cases to give the Board the option of refusing to comply with a request for an opinion if an administrative arrangement does not meet the conditions of Article 64(2) of the GDPR (matter of general application or producing effects in more than one Member State).

3. Proposed amendment

Article 46(4) of the GDPR should be revised as follows:

4. In cases referred to in point (a) of paragraph 3, the supervisory authority shall apply the consistency mechanism in accordance with sentence 2 point (e) of Article 64(1), in cases referred to in point (b) of paragraph 3 the consistency mechanism in accordance with Article 64(2).

II. Experience of the application and functioning of the provisions of Chapters V and VII

1. Outline of the problem

Experience gained in the application and functioning of the provisions of Chapters V and VII are one of the matters to be dealt with pursuant to Article 97 of the GDPR. More specifically, the question arises of whether longer deadlines are necessary.

2. Assessment

It has so far not been possible to fully test, in practice, the time limits and deadlines laid down in the GDPR.

Nevertheless, experience dealing with requests for opinions in accordance with Article 64(2) of the GDPR has shown that the time limits make it more difficult to appropriately deal with and discuss more extensive matters and more tricky individual cases.

3. Proposed amendment

The time limit set in Article 64(3) of the GDPR should be increased from eight weeks to three months and that in Article 66(4) of the GDPR from two to four weeks. Accordingly, it would then be necessary to examine whether the period of validity of provisional measures (Article 66(1) of the GDPR) should also be extended. At the very least, however, one should consider extending all the time limits in the cooperation and consistency mechanism by 50%.

III. Article 64(7) of the GDPR

1. Outline of the problem

Article 64(7) of the GDPR currently only requires the competent supervisory authority to provide the Board with an amended draft decision based on the Board's opinion (or that it give notification that it does not intend to amend the decision). The Board is, however, not required to give any further response to the lead supervisory authority beyond that.

This issue was first identified in connection with the consistency mechanism regarding the list of processing operations subject to the requirement for a data protection impact assessment (point (a) of Article 64(1) of the GDPR). Many users of such lists were not sure whether these are binding in nature once they have been adapted, pursuant to Article 64(7) of the GDPR, to the Board's opinion. This now creates huge problems when the consistency mechanism is triggered in relation to binding corporate rules (BCRs), since external entities (the enterprise making the request) will then also be affected. Thus, if the Board's opinion is initially negative or it includes necessary changes and the enterprise thereupon amends its BCRs (part of the competent authority's draft authorization), the lead authority and the enterprise are no longer given concluding feedback to indicate whether the Board's concerns have been fully met and the amended decision has therefore become binding.

This has become a matter for much discussion with the Board's Secretariat. An addition should therefore be made to the provision in Article 64 of the GDPR to clarify when the consistency mechanism has finally been concluded.

2. Assessment

There does indeed appear to be a loophole in respect of which procedure follows after an amended draft decision.

3. Proposed amendment

Insertion of a second sentence in Article 64(7) of the GDPR:

The Board shall give its opinion on the amended draft decision within four weeks.

If the Board does not give an opinion within four weeks, this is deemed to constitute approval.

Key issue no. 7: Direct marketing

1. Outline of the problem

When the GDPR became applicable specific provisions of domestic law ceased to have effect, specifically those which provided for the balancing of various interests. Only Recital 47 of the GDPR provides any indication of how this balancing is to be done: "The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest." In practice, questions arise which could be better resolved if the legislator set specific requirements, for instance:

Is it permissible to provide customers' data on to third parties for advertising purposes?

Is it permissible to retain and use data in lists or other summaries concerning the members of a group of people which are limited to the data subject's membership of that group, that person's profession, sector or business name, name, title, academic degree, address and year of birth (but not telephone and fax number, email address and date of birth) for advertising purposes?

Is advertising for charitable purposes thus to be assessed differently than that for business purposes?

2. Assessment

Direct marketing affects many sectors and many data subjects.

Member States have very different traditions in this regard, which means that the expectations of data subjects of which account needs to be taken when weighing up various interests may also differ. The legislator should, therefore, create more detailed provisions to ensure EU-wide harmonization in terms of application.

3. Proposed amendment

The European legislator should make statutory provisions in the GDPR in relation to direct marketing which, as a matter of principle, at the very least require that various interests are weighted.

Key issue no. 8: Profiling

1. Outline of the problem

The creation of personal profiles and their – commercial and political – analysis are two of the key data policy challenges of our times. Data processing tools enable incredible quantities of data from the most varied of contexts to be collated and analyzed. Combined with ever more refined means of applying self-learning mechanisms, this opens up diverse opportunities for (purportedly) predicting and possibly nudging individual behaviour. Although this trend poses a challenge to various fundamental privacy principles (e.g. the data minimization or purpose limitation requirement), the GDPR is vague in this regard and has to all intents and purposes not changed since 1995. It was not possible, during negotiations on the GDPR, to arrive at a detailed, modern EU-wide rule on profiling and scoring.

Although the GDPR does contain a definition of profiling in no. 4 of Article 4, and the term is referred to in various Recitals and articles (e.g. Recital 60, Article 21, Article 22, Article 13 and 14 of the GDPR), most of those provisions do not apply to profiling. Instead, the core restrictive regulation is the ban on automated individual decision-making with authorization proviso (Article 22 of the GDPR). As the law currently stands, profiling as such thus often needs to be assessed on the basis of the general elements of Article 6 of the GDPR. For example, businesses often do not regard profiling based on the content of Internet communications and metadata for advertising purposes as automated decision-making, as a result of which profiling is not covered by the general prohibition set out in Article 22 of the GDPR.

2. Assessment

The DSK is of the opinion that, against the backdrop of the problems described in the above, the provisions of the GDPR on profiling need to be amended. These new rules should serve to tighten the statutory framework so as to establish effective and enforceable limits to the use of personal data for profiling purposes. Data subjects should benefit from greater transparency around what profiles are being created, and they should at the same time be given more control over how their data are processed to create profiles. To that end, the prohibition of automated individual decision-making set out in Article 22 of the GDPR should be expanded to include data processing for profiling purposes. The only possible legal bases for profiling should be – apart from having a specific legal basis – consent or a contract. That would ensure that profiling is only possible if the data subject is aware of it and has consented to it.

The Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/279 adopted by the Article 29 Working Party and endorsed by the Board are an important tool which can be used when assessing profiling from the perspective of privacy and data protection. They can, however, be no substitute for a statutory regulation.

Key issue no. 9: Accreditation

1. Outline of the problem

Germany's national accreditation body and the German supervisory authorities are currently in dispute over the application of Article 41 of the GDPR. The German accreditation body is of the opinion that it must also be involved in accreditation pursuant to Article 41 of the GDPR, while the German supervisory authorities feel that accreditation within the meaning of Article 41 of the GDPR should be their sole purview. In the course of this debate Germany's accreditation body asked the supervisory authorities to help ensure that the wording is clarified.

2. Assessment

Germany's national accreditation body concludes from Regulation (EC) No 765/2008 that it has general competence for accreditation in Germany. That is why it has so far assumed that a similar procedure will be conducted for accreditation pursuant to Article 41(1) of the GDPR as is provided for in Article 43(1) of the GDPR, which the supervisory authorities are involved in. The German supervisory authorities, by contrast, point out that Article 41(1) of the GDPR refers to the supervisory authorities as the only body responsible for accreditation. The wording of sentence 2 of Article 43(1) of the GDPR differs significantly from that of Article 41(1) of the GDPR. Also, the GDPR does not contain any specific reference to accreditation pursuant to Article 41(1) of the GDPR, with the exception of point (p) of Article 57(1) (drafting and publishing of criteria) – with the GDPR, incidentally, being much more specific than Regulation 765/2008. In the opinion of the German supervisory authorities, it must be assumed that the term "accreditation" as used in Article 41 of the GDPR does not refer to the same thing as "accreditation" within the meaning of Article 43 of the GDPR and Regulation No 765/2008, but rather that it represents another type of "approval" to which Regulation No 765/2008 does not apply.

3. Proposed amendments

The word "only" should be inserted before "by the competent supervisory authority" in Article 41(1) of the GDPR for clarification.

In addition, the word "accredited" (DE: *akkreditiert*) in the same provision should be deleted and replaced by "approved" (DE: *anerkannt*) merely for clarification.

List of additional proposed amendments

Relevant provision of GDPR	Proposed amendment, plus brief explanation
Article 4	The GDPR currently lacks a definition of "anonymization". It would be useful in practice and it should be aligned with the requirements set out in Opinion 05/2014 on Anonymization Techniques.
Articles 13 and 14	The categories listed in paragraph 2 of Article 13 and paragraph 2 of Article 14 of the GDPR should be aligned by including the information referred to in point (b) of Article 14(2) in paragraph 2 of Article 13 rather than in paragraph 1.
Article 18(1)	Right to restriction of processing: In addition to the grounds listed in points (a) to (d) of Article 18(1) of the GDPR, the right to restriction of processing should also apply to those cases in which the requisite erasure is not carried out only because the data need to be retained pursuant to point (b) of Article 17(3) of the GDPR in order to comply with retention periods.
Article 21(2)	Right to object to direct marketing: The words "in addition to the right to object under paragraph 1" should be inserted to make it clear that paragraph 2 does not represent a sub-case of paragraph 1, but that, in contrast to paragraph 1, it also applies when data are not processed on the basis of points (e) and (f) of Article 6(1) of the GDPR.
Article 24(2)	It appears that the wording in Article 24(2) of the GDPR could lead to misunderstandings. The German version should be aligned to the English version by replacing "*Anwendung*" (application) with "*Einführung*" (implementation) and "*Datenschutzvorkehrungen*" (data protection provisions) with "*Datenschutzschutregelwerke*" (data protection policies).
Article 27	A duty to publish the representative's contact details should be introduced in Article 27 of the GDPR in analogy with Article 37(7) of the GDPR (data protection officer), as in many cases it is unclear whether the controller/processor has met its duty to appoint a representative and where that representative is based.
Article 40(4), Article 41(1) and (4)	Clarification as to whether the establishment of an accredited supervisory body is obligatory (in analogy with the Board's guidelines of 12 Feb. 2019) or only optional.

Resolution adopted at the 97th Conference of the
Independent German Federal and State Data Protection Supervisory Authorities

Hambach Castle

3 April 2019

Hambach Declaration on Artificial Intelligence

Seven Data Protection Requirements

Artificial intelligence (AI) systems represent a substantial challenge to freedom and democracy in our legal system. AI developments and applications must observe fundamental rights in line with democratic and rule-of-law principles. Not everything which is technically possible and economically desirable can be allowed to become reality. That most particularly applies to the use of self-learning systems which process massive quantities of data and interfere with the rights and freedoms of data subjects on account of automated individual decision-making. Safeguarding fundamental rights is the task of all levels of government. The legislature must set key conditions within the framework of which AI is to be used, and the supervisory authorities must implement them. Only if the protection of fundamental rights and data protection keeps pace with digitalization will it be possible to ensure that, in future, decisions about people will be taken by people not by machines.

I. Artificial intelligence and data protection

Artificial intelligence (AI) is currently a matter of intense debate because it promises to generate new added value in many areas of business and society. The Federal Government published its Artificial Intelligence Strategy on the basis of which Germany is to become a global leader in AI development. "AI made in Germany" also aims to ensure that even when AI is used extensively those fundamental values and rights of freedom which apply in Germany and the EU continue to play a key role in defining our life together in society. The independent German federal and state data protection supervisory authorities expressly welcome this approach to shaping AI in line with fundamental rights.

As yet, no generally recognized definition of AI is available. The Federal Government defines AI as the "designing of technical systems so that they can handle problems independently and themselves adapt to changing conditions. One of these system's characteristics is that they can 'learn' from new data […]."[1]

[1] Bundestag Printed Paper 19/1982 re 1., The Federal Government's Data Ethics Commission also highlights pattern recognition, machine learning, and heuristic searches, interference and planning methods as important bases for AI (Recommendations of the Data Ethics Commission for the Federal Government's Artificial Intelligence Strategy, 9 Oct. 2018).

AI systems are already being used in medicine, for instance, to support research and treatment. Neuronal networks are already able to automatically recognize complex tumour structures. AI systems can also be used to identify depressive disorders based on a person's behaviour in social media or based on voice modulation when a person uses a language assistant. When it is placed in the hands of physicians such knowledge can be used to benefit patients. If it gets into the wrong hands, however, it can be put to improper use.

One particular AI system has already been used to assess job applications, the aim being to ensure that decisions were not influenced by human prejudices. However, the enterprise in question had previously hired mainly male applicants and used these successful applications to train the AI system. As a result, the AI system rated female applicants very much worse although gender was not only not a pre-defined assessment criterion, it was unknown to the system. This shows the risk that discrimination which is inherent in the training data will not be eliminated but reinforced.

These examples clearly show that AI systems are often used to process personal data and that processing holds risks to the rights and freedoms of humans. They also show how important it is to attend to the development and use of AI systems at political, social and legal level. The independent German federal and state data protection supervisory authorities regard the following requirements as making a constructive contribution to this key social-policy project.

II. AI data protection requirements

The General Data Protection Regulation (GDPR) sets key legal requirements as regards the development and use of AI systems which process personal data. They serve to protect the fundamental rights and freedoms of natural persons. The principles set out in Article 5 of the GDPR apply equally to the processing of personal data by AI systems. In accordance with Article 25 of the GDPR, controllers must implement these principles by taking technical and organizational measures, which need to be planned at an early stage (data protection by design).

1. AI must not turn people into objects

The inviolability of human dignity (Article 1 para. 1 of Germany's Basic Law, Article 1 of the European Charter of Fundamental Rights) means that, especially when it comes to government action based on AI, people must not be turned into objects. Fully automated decision-making or profiling by AI systems are only permissible under strictly limited conditions. Under Article 22 of the GDPR, decisions which produce legal or similarly significant effects may not be based solely on automated processing. Where Article 22 of the GDPR does not apply, the general principles laid down in Article 5 come into play. These principles specifically protect the rights of the individual based on the requirements of lawfulness, fairness and transparency. Where AI systems are used, data subjects also have the right to obtain human intervention, to express their point of view and to contest the decision.

2. AI may only be used for constitutionally legitimated purposes and may not outweigh purpose limitation

Further, AI systems may only be used for constitutionally legitimated purposes. The principle of purpose limitation (point (b) of Article 5(1) of the GDPR) also applies. Article 6(4) of the GDPR sets clear boundaries when it comes to changing the purpose of data processing. The principle that

expanded processing purposes must be compatible with the original purpose also applies to AI systems. The same goes for using personal data to train AI systems.

3. AI must be transparent, comprehensible and explainable

Personal data must be processed in a manner which is easily understandable for the data subject (point (a) of Article 5(1) of the GDPR). In particular, this requires transparency of the processing in which information about the process and possibly also the training data used are easily accessible and comprehensible (Article 12 of the GDPR). Decisions made on the basis of AI systems must be comprehensible and explainable. It is not sufficient for the outcome to be explicable: the processing and decision-making must also be understandable. The GDPR also requires that the logic applied must be adequately explained as well. These transparency requirements must be continually fulfilled where AI systems are used to process personal data. Controllers are accountable (Article 5(2) of the GDPR).

4. AI must avoid discrimination

Self-learning systems are heavily dependent on the data entered. An inadequate data basis and system design can produce outcomes which are, in effect, discriminatory. Discriminatory processing violates the rights and freedoms of data subjects. Among other things, they breach certain requirements made under the GDPR, for example the principles of fairness, legitimate purpose and appropriateness.

These tendencies towards discrimination are not always readily identifiable at the outset. Before applying AI systems, the risks to the rights and freedoms of individuals therefore need to be assessed so that countermeasures can be taken to reliably eliminate hidden discrimination. Risk monitoring must be carried out whenever AI systems are used.

5. Principle of data minimization applies to AI

Huge quantities of training datasets are typically needed to train AI systems. The principle of data minimization (point (c) of Article 5(1) of the GDPR) also applies when personal data are used in AI systems. The processing of personal data therefore always has to be limited to only that which is necessary. Assessing necessity can reveal that it is sufficient to process fully anonymized data to achieve the legitimate purpose.

6. AI needs accountability

Those involved in using AI systems must define and clearly communicate the relevant responsibilities and take whatever measures are necessary to guarantee the lawfulness of the processing, data subjects' rights, the security of the processing and controllability of the AI system. Controllers must ensure compliance with the principles set out in Article 5 of the GDPR. They must also meet all requirements as regards the rights of data subjects under Article 12 et seqq. of the GDPR. Controllers must guarantee the security of the processing as required by Article 32 of the GDPR and thus also prevent manipulation by third parties which can have an impact on the outcomes produced by AI systems. When applying AI systems in which personal data are processed it will as a rule be necessary to carry out a data protection impact assessment pursuant to Article 35 of the GDPR.

7. AI needs technical and organizational standards

In order to be able to guarantee that processing complies with data protection requirements, technical and organizational measures as referred to in Articles 24 and 25 of the GDPR must be taken when designing and using AI systems, for instance pseudonymization. It is not sufficient to assume that an individual data subject will seemingly disappear in among the huge quantities of personal data. No specific standards or detailed requirements for these technical and organizational measures are yet available to ensure that AI systems comply with data protection requirements. Gaining new insights in this area and developing best practice examples are important tasks incumbent on the business and scientific communities. The data protection supervisory authorities will actively support this process.

III. Developments in AI need regulation

The data protection supervisory authorities monitor application of data protection legislation, enforce that legislation and are tasked with ensuring that fundamental rights are effectively protected whenever it is updated. Given the great momentum with regard to AI technologies and their diverse areas of application, it is not yet clear where the limits to their development will be set. Equally, it is impossible to make any generalized statements as to the risks which processing personal data in AI systems pose. Ethical principles also need to be observed. The scientific community, data protection supervisory authorities, users and, in particular, politicians are called to keep abreast of AI developments and regulate these developments in line with data protection principles.