Platform Privacy - Research for a self-determined life in the digital world

Plattform Privatheit

Alexander Roßnagel and Christian Geminn

# MOVING DATA PROTECTION FORWARD

## PROPOSALS FOR AMENDING THE GENERAL DATA PROTECTION REGULATION

Policy Paper

Edited by Michael Friedewald, Alexander Roßnagel, Christian Geminn und Murat Karaboga

# Imprint

## Research Papers of the Platform Privacy, No. 2

### Editors

**Platform Privacy**
Michael Friedewald[1], Alexander Roßnagel[2,3], Christian Geminn[2], Murat Karaboga[1]
(1) Fraunhofer Institut for Systems and Innovation Research ISI
(2) Universität Kassel, Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG)
(3) Hessischer Beauftragter für Datenschutz und Informationsfreiheit, Wiesbaden

### Authors

Alexander Roßnagel[1], Christian Geminn[2]
(1) Hessian Commissioner for Data Protection and Freedom of Information, Wiesbaden, Germany
(2) Kassel University, Research Center for Information System Design (ITeG), Kassel, Germany

### Series

| | |
|---|---|
| ISSN (Print) | 2942-8874 |
| ISSN (Online) | 2942-8882 |
| DOI | https://doi.org/10.24406/publica-2621 |

### Publication

April 2024, 1st Edition
Fraunhofer Institut for Systems and Innovation Research ISI, Karlsruhe

### Suggested citation

Roßnagel and Geminn (2024): *Moving data protection forward – Proposals for amendment of the GDPR*. Ed. Friedewald et al.: Research Papers of the Platform Privacy, No. 2. Karlsruhe: Fraunhofer ISI.

### Disclaimer


The information has been compiled to the best of our knowledge and belief, in accordance with the principles of good scientific practice. The authors believe the information in this report to be accrate, complete, and up to date, but assume no responsibility for any errors, express or implied. The representations in this document do not necessarily reflect the views of the client.

Table of contents

## Moving Data Protection Forwards

The General Data Protection Regulation (GDPR) has improved the standing of data subjects and especially of consumers in many places. Yet, it does not realise its full potential. On the one hand, the GDPR has created significant and continuing legal uncertainty, which often affects consumers adversely. This uncertainty results mostly from the fact that the GDPR remains abstract and omits clarifying specifications – both concerning its understanding and its practical implementation. This entices providers of digital services and others to use the existing room for manoeuvre to the disadvantage of consumers. On the other hand, certain consumer-friendly provisions simply were unsuccessful during the creation of the GDPR. This concerns for instance an adequate protection from scoring. Both hinders the innovations that the GDPR has brought into the European data protection practice. They are unable to unfold their potentials when it comes to protecting consumers and other data subjects.

Issues exist on two levels. First, there are issues that result from deficits in the text of the regulation (= normative deficits). Regarding these deficits, we suggest 33 alterations of the text in order to improve it – from the point of view of consumers. Strengthening the position of the consumer and reducing the asymmetry of power between controller and data subject is in line with the pronounced goal of the GDPR to have the processing of personal data serve mankind, to safeguard the fundamental rights and freedoms of data subjects and to contribute to the well-being of natural persons – with respect to the rights of the controllers.

In some places however, extensive specification and clarification through guidelines issued by the European Data Protection Board is irremissible. Beyond that, there are conceptional issues that cannot be resolved with smaller alterations of the text of the norm (= structural deficits):

### Normative deficits

Weaknesses in the text of the GDPR are on the one hand the result of legislative errors and on the other hand the result of the use of numerous indeterminate legal terms as well as provisions that remain at a very high level of abstraction. The lack of clear, definite, and unambiguous provisions has caused many problems of interpretation and understanding, legal uncertainty and legal disputes in recent years. Currently, clarification can occur in a non-binding manner through thematic guidelines issued by the European Data Protection Board and in individual cases in a binding manner through the courts and ultimately the European Court of Justice. The latter takes years, and a judgement may already be outdated on the day it is rendered due to the rapid development of technology. A single word from the legislator could often remedy this situation.

One example is consent and its relationship to other grounds for processing. Ambiguities in the wording of Article 6(1)(1) of the GDPR lead many data controllers to invoke other grounds under Article 6(1)(1) of the GDPR in addition to consent when consent is revoked (thus giving them grounds to continue processing the data concerned) – despite the statement of the Article 29 Working Party that "if a controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an individual withdraws consent".[1] The issue could be resolved by clarifying in the Regulation that a controller who seeks consent must also comply with the rules of consent.

[1] Article 29 Working Party, *Guidelines on consent under Regulation 2016/678*, WP 259 rev.01, 2018, p. 23.

There are numerous other places in the text of the GDPR where a single additional word or phrase could resolve the existing legal dispute and thus significantly reduce legal uncertainty.

## Conceptional deficits

These weaknesses stand alongside those deficits that cannot be eliminated by mere changes of the wording of individual provisions of the GDPR. On the one hand, these are deficits that are already inherent to the basic principles of data protection law as they were shaped decades ago and which are put under pressure by new and emerging possibilities of data processing. On the other hand, they are deficits that result from the specific shaping of the regulation itself.

Looking at numerous modern technologies and practices, there are clear frictions and open conflicts with the data protection principles which emerged in a completely different technological environment. They were primarily intended to contain the information power of the state, typically the processing of personal data in public administration and on a manageable number of large mainframe computers. However, international data traffic and the ubiquitous availability of immense computing power have led to a drastically increased threat to informational self-determination in comparison to threats that existed in previous decades. Against this backdrop, data protection principles must be consistently enforced, but they must also be further developed to ultimately prevent erosion or even fading into irrelevance if the conflicts with technological reality become insurmountable.

Another weakness of the GDPR is that it is too risk-neutral. It does take into account the risks of data processing in order to reduce the burden on data processors. However, it lacks risk-adequate differentiations of the data protection principles, the lawfulness of data processing and the rights of the data subjects. Even where data processing causes very different risks to fundamental rights, the same abstract provisions apply – for example, for the low-risk customer list of a local craftsman's business as well as for the higher-risk data processing forms of the internet of things, big data, artificial intelligence, cloud computing and data-driven business models. The reason for this risk neutrality is that the GDPR follows an exaggerated manifestation of the principle of technology neutrality. This principle is supposed to minimise the risk of circumvention of legal provisions by making data protection regulations "not depend[ent] on the techniques used" (Recital 15(1) GDPR). Properly understood, a technology-neutral regulation makes sense if it is intended to prevent legal provisions from hindering or excluding further technical development. It should therefore be formulated in such a way that the legal provisions are also applicable to further developed technologies. This disqualifies provisions for individual manifestations of a specific technology application. However, there should still be provisions designated to certain technical functions – especially if they cause particular risks to fundamental rights (as is the case with tracking, facial recognition, profiling or scoring). The GDPR has almost completely failed in this regard. Its highly abstract provisions cause legal uncertainty in all attempts to apply them to concrete techniques and instead strengthen the chances of enforcement of powerful interests.

## Revising the GDPR

A revision of the GDPR should put those aspects of data protection law into the spotlight that promote consumer protection. For instance, consent is used as a means to completely exempt the data controller from certain obligations under data protection law. This could be prevented by simply declaring certain obligations and rights non-derogable. While this restricts the self-determination of data subjects, it also shields them from being tempted to waive central rights in situations of direct or indirect social or psychological coercion. Paragraph 6(1) of the German Federal Data Protection Act (Bundesdatenschutzgesetz) in the version applicable before 25 May 2018 could serve as a model for this. It states: "The rights of the person concerned to information

[…] and to correction, deletion or blocking […] cannot be excluded or limited by a legal transaction."

Furthermore, the protection of consumers could be increased through objectification – especially in so-called "take it or leave it" situations, for instance by requiring consent forms or general terms and conditions to be objectively checked and approved by a competent authority before coming into force. Such pre-formulated texts should be considered anti-competitive if they pursue purposes that are unrelated to the promised services or otherwise insufficiently take into account the interests of the data subject. The market share of the service provider and thus the dependence of the data subject in using this offer could be taken into account. As the market share increases, the responsibility for fair contract conditions would also increase. Or the existence of required data protection functions in technical systems could be verified in the context of an approval process that tests the quality of the system in certain areas – including the risks of its use. Existing examples of such an approach are the ex-ante approval procedures of motor vehicles and medical devices. There are also proposals to verify the quality of data, the quality of statistical models and the non-discriminatory and comprehensible nature of the results of certain high-risk algorithm-based decision-making systems by a body designated for this purpose. This approach was taken up to some extent in the Artificial Intelligence Act.

Another approach is indicated by Art. 80 GDPR, namely the collectivisation of the exercise of rights: The determination and pursuit of a right is no longer left solely to the private initiative of a data subject but is professionally assumed by an association. The GDPR has significantly strengthened legal protection in data protection. The right to lodge a complaint and to an effective judicial remedy are in principle placed with the data subject. However, Art. 80(1) GDPR allows certain bodies, organisations, or associations to be entrusted with their exercise.

The issues surrounding Art. 6(1)(1)(f) GDPR must also be taken into account. Even if there are no grounds for processing according to (a)-(e), personal data may still be processed if the controller can assert its own interests or the interests of third parties. These interests can "override" the interests or fundamental rights and freedoms of the data subject. In addition, the necessity of the processing must be established. However, it is the controller who carries out the balancing and the determination. Therefore, there is a risk that in practice controllers may tend to overestimate the necessity of the processing and the importance of their interests, as well as to underestimate the interests of the data subject. A correction of a misjudgement can at best occur only afterwards when risks of the processing in question have already materialised for the data subjects. The time lag between the processing and the correction can increase considerably in the event of a legal dispute about the assessment made. On top of this, the data subject must be able to establish that unlawful processing is occurring in the first place. In a second step, the data subject must then be willing and be able to take action against the processing. In order to strengthen the data subject, the Union legislator should not indiscriminately leave the balancing of interests to the controllers but should adopt rules that apply in typical processing situations (e.g. advertising or profiling) or in typical business models (e.g. search engines, social media). This is yet another area where clear requirements would help to strengthen the position of the consumer and reduce power asymmetries.

However, much would already be gained for consumers if – against the background of the practical experience of the last years – the most obvious and easily remediable weaknesses of the GDPR were eliminated.

The success of the consumer-friendly innovations of the GDPR must not solely depend on the interpretation of the applicable text from 2016. Instead, there need to be specifications that anchor provisions that are more friendly to fundamental right and that frame the rights of consumers and the obligations of controllers more clearly directly in text of the relevant articles of the

GDPR. Even small changes of the text can achieve the necessary specifications or at least significantly increase the clarity of existing provisions and strengthen the position of consumers.

The innovations of the GDPR can only unfold, if sufficiently concrete provisions ensure an effective application. Legal uncertainty must be avoided. However, in many places the GDPR goes too far in the direction of openness and thus prevents – for lack of specification – that legal obligations are taken seriously, and that data protection is appreciated in all its facets. The success of the innovations of the GDPR depends on these specifications. The proposed recommendations are meant to improve the GDPR with regard to its consistency and implementation in order to constructively advance the Regulation.

The proposed changes and amendments therefore focus on the material provisions of the GDPR (Articles 1 to 50) and relate to the following topics:

- the material and territorial scope of the GDPR (Articles 2 and 3),
- the principles relating to processing of personal data (Article 5),
- the lawfulness of processing (Article 6),
- personal data of children (Articles 6, 8, 9 and 35),
- transparent information (Articles 12 to 14, 24 and 26),
- the rights of the data subject (Articles 15 to 23; in particular Article 20),
- automated decision-making (Articles 13, 14 and 22),
- data protection by design and by default (Article 25).

Furthermore, but to a lesser degree, adaptions in the procedural and supporting provisions of the GDPR (Articles 51 to 99) are required:

- the powers of the supervisory authorities (Article 58),
- the tasks of the European Data Protection Board (Article 70)
- administrative fines (Article 83).

For more details on these recommendations as well as on the aforementioned conceptional issues of the GDPR, please refer to:

*Roßnagel, Alexander / Geminn, Christian*, Datenschutz-Grundverordnung verbessern: Änderungsvorschläge aus Verbrauchersicht, Baden-Baden 2020.

English excerpts can be accessed here:

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-Data-protection-report-on-the-General-Data-Protection-Regulation/F514013_en

*Roßnagel, Alexander / Geminn, Christian*, The GDPR Five Years On – A retrospective from the viewpoint of consumers, Revue européenne de droit de la consommation / European Journal of Consumer Law 1/2024, 109.

## Proposals for amendment

### 1. Processing in the course of a purely personal or household activity

The complete exemption of invasive data processing from the material scope of the GDPR in Art. 2(2)(c) should be retracted. Instead, there should be a risk-adequate differentiation also in the context of personal or household activity. A complete exemption from the material scope should only apply for low-risk processing. For application with heightened risks select provisions of the GDPR should apply.

### 2. Territorial scope

*Expansion of the territorial scope of the GDPR to include every type of processing of personal data of data subjects in the European Union.*

To extend the territorial scope of the GDPR to any form of processing of personal data of data subjects in the European Union, in accordance with a consistent application of the residence principle, the following amendment to Article 3(2)(a) is recommended:

> "2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to,
>
> (a) the *addressing of data subjects in the Union* ~~offering of goods or services~~, irrespective of whether a payment of the data subject is required, ~~to such data subjects in the Union~~;"

Since the offering of goods or services is no longer required, it is no longer necessary to differentiate this offering from other activities. The circle of controllers or processors covered is expanded by the fact that every contact with a person in the Union is sufficient for the application of the Regulation. At the same time, the Regulation does not apply if the initiative for the ultimate processing of personal data does not come from the controller or processor, but from the data subject himself.

### 3. Principles relating to processing of personal data

*Amendment of the GDPR with an obligation to data avoidance in Art. 5(1)(c).*

*Modernising and risk-adequate evolution of the principles.*

In order to supplement the principle of data minimisation with the principle of data avoidance, the following amendment to Article 5(1)(c) is recommended:

> "1. Personal data shall be …
>
> c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation') *and processed in data processing systems whose selection and design are geared towards the goal to process as few personal data as possible ('data avoidance')*;"

Through the phrase "to process as few personal data as possible" the principle of proportionality is brought to bear. What is crucial is that not only data minimization takes place according to a purpose that the person responsible has selected, but also avoidance of the processing of personal data through a system design that takes the purpose into account.

## 4. Relation between consent and other grounds for lawful processing

*Clarification in Art. 6(1)(1) GDPR that a controller in addition to consent or as substitute for consent cannot rely on another ground for lawful processing while creation different legal effects on the data subject.*

In order to make it clear that a controller cannot rely on any other ground for processing in addition to consent, the following amendment to Article 6(1)(1) is proposed:

> "1. Processing shall be lawful only if and to the extent that ~~at least one of the following applies~~: (a) either the data subject has given consent to the processing of his or her personal data for one or more specific purposes; *or one of the following applies*:
>
> ~~(b)~~ *(a)* processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; …"

The adjustments make it clear that consent and the other grounds for processing can only be used alternatively. By inserting an "either – or" and thereby differentiating consent from the legal permissions and deleting "at least", it is impossible to equate consent with the legal permissions and to combine them with them. After the change, there are only two – mutually exclusive – ways to justify data processing. This prevents a controller from being able to base data processing on another ground after obtaining consent. Anyone who obtains consent must also accept the rules of consent regulations.

## 5. Determining the purpose of a contract

*Specification of Art. 6(1)(1)(b) GDPR: objective (functional) specification of the processing of personal data that is necessary to fulfil a contract independently from the phrasing of the contract.*

To objectify and clarify the permissive status of the current Article 6(1)(1)(b), the following change to the text is proposed:

> "(b) processing is objectively necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;"

By referring to the objective necessity of processing personal data for the performance of a contract, the permission is linked solely to the functional necessity for the agreed service. It is no longer possible to use contractual wording to justify data processing beyond this, which – such as informing friendly companies or informing the customer about other products – is not necessary for the fulfillment of the main contractual obligations. This data processing is only possible if it is justified by overriding legitimate interests or if the data subject has given consent.

## 6. Personal data of children I

*Consideration of the special protection that children merit when assessing the compatibility of a new purpose with the initial purpose, if the data of a child are to be used for another purpose.*

In order to take due account of the fact that the personal data of a child is involved when examining the compatibility of an old purpose with a new one, Article 6(4)(1)(d) GDPR should be supplemented to take this circumstance into account.

> "(d) the possible consequences of the intended further processing for data subjects, in particular where the personal data of a child is concerned;"

The addition obliges the controller to pay particular attention to the consequences of further processing for children in the event of a change of purpose. To date, this obligation can only be found implicitly in Recital 38(1) and should be explicitly included in the Articles to strengthen the position of children in data protection.

## 7. Personal data of children II

*Transfer of recital 38(2) GDPR to the articles, prohibiting the use of personal data of children for the purposes of marketing or profiling.*

In order to incorporate the assessment of Recital 38(2) into the text of Article 8(1), the addition of a new sentence 2 is proposed:

> *"This shall not apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles."*

Sentence 2 becomes sentence 3. With the addition, Recital 38(2) GDPR changes from an interpretive aid to directly applicable law and thus strengthens legal certainty.

## 8. Personal data of children III

*Exclusion of the consent of a child from the processing of special categories of personal data according to Art. 9(2)(a) GDPR.*

For children, consent to the processing of special categories of personal data in accordance with Article 9(2)(a) GDPR should be excluded in order to adequately protect them against taking on particular risks. The addition of one word is suggested for this purpose:

> "(a) the *adult* data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;"

This addition means that no one can rely on the personal consent of a child for the particularly risky processing of special categories of personal data. The consent of the legal guardian remains possible.

## 9. Transparent information

*Focussing of information on the actual circumstances of the respective processing that is about to occur.*

To be able to fulfill the obligation to inform the data subject about the data processing concerning them, only information about the data processing that can be described completely and precisely with all the necessary information should be permitted. For this purpose, the following change to Article 12(1) is proposed:

> "1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to *current* processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means."

The inclusion of the word "current" makes it clear that the information is intended to relate to the data processing currently envisaged, for which the scope, purpose and procedures are established and fully known. This prevents the obligation to provide information from being fulfilled by referring to a data protection declaration in which all conceivable future data processing is summarized with vague references to future possibilities. Future changes in data processing that have not already been determined and therefore cannot be described precisely must lead to new, then current, information.

The change should be accompanied by a clarification in Recital 60 that high complexity of data processing does not excuse inadequate information.

## 10. Information to be provided by the controller

*Addition of a basic rule to resolve the conflict between the right to access and the protection of trade secrets: provision of the highest amount of information possible while protecting trade secrets and intellectual property; obligation to provide a maximum of information while still taking these opposing interests into account.*

In order to provide the highest possible level of information about data processing when protecting legally recognized secrets and intellectual property rights, the controller should be obliged to look for ways to provide the most comprehensive and accurate information possible without compromising the secret. To this end, Article 12 should be supplemented with such a basic rule on practical concordance between information and secrecy in a new paragraph 7:

> *"7. If the information to be provided to the data subject endangers the rights and freedoms of other people, such as trade secrets or intellectual property rights, the controller shall ensure the highest possible level of information while preserving these rights and freedoms."*

The previous paragraphs 7 and 8 become paragraphs 8 and 9. Adding a new basic rule to resolve the conflict between the right to information and the protection of secrets will particularly improve the level of information in automated decision-making.

In accordance with the new version of paragraph 7 of Article 12, the considerations in Recital 63 sentences 5 and 6 must be adapted to the new basic rule. References to appropriate procedures to protect trade secrets or intellectual property rights (e.g. adding "noise") could be included here. It is also possible to move it to Recital 58 or 60 of the GDPR.

## 11. Timely relevant information about data collection

*Presentation of information that is adequate to the situation, the interests and the decisions involved.*

*Focusing of information on the actual circumstances of the respective processing that is about to occur.*

In order to ensure that the controller provides the data subject with the relevant information "at the time when personal data are obtained", the wording of the opening words of Article 13(1) and (2) should be supplemented as follows:

> "1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the *respective* time when personal data are obtained, provide the data subject with all of the following information *that relate to this obtainment:* …
>
> (2) In addition to the information referred to in paragraph 1, the controller shall, at the *respective* time when personal data are obtained, provide the data subject with the following further information *that relate to this obtainment and are* necessary to ensure fair and transparent processing: …"

The additions ensure that the information is provided at the right time and therefore appropriate to the situation, namely at the time of data collection and before a necessary or possible decision of the data subject. This strengthens the self-determination of the data subject and, in particular, increases the transparency of complex processing operations.

## 12. Information on recipients I

*Duty to provide as much information as possible on recipients of personal data.*

In order to provide sufficient information about the recipients of personal data, which enables the data subject to take legal action, or at least makes this significantly easier, the wording of Article 13(1)(e) should be slightly adjusted:

> "(e) the recipients *as far as they can be determined* or categories of recipients of the personal data, if any;"

The same change should be made in the wording of Article 14(1)(e).

The addition obliges the controller to name all known recipients of personal data. If it is possible for him to specifically name a recipient, he cannot resort to simply naming categories of recipients. Specifying categories of recipients is therefore only permitted if a specific recipient cannot (yet) be named at the time of the information.

## 13. Information regarding automated decision-making I

*Clarification that information on the "logic involved" entails the criteria for the decision and their balancing.*

*Clarification that a division of labour or cooperation in the context of automated individual decision-making must not lead to an omission or limitation of information to be provided to the data subject; obligation to inform about divided / cooperative automated decision processes that has to be met by every cooperating partner concerning their contribution to the process including the interfaces to all other contributions.*

To settle the dispute about the scope of the information that a controller has to provide about the existence of automated decision-making, the text in Article 13(2)(f) and 14(2)(g) should be clarified.

> "(f/g) the existence of automated decision-making, ~~including profiling, referred to in Article 22(1) and (4)~~ and~~, at least in those cases,~~ meaningful information about the logic involved *including the criteria for the decision and their weighting*, as well as the significance and the envisaged *and possible legal and factual* consequences of such processing for the data subject."

The addition strengthens the interests of the consumer, who would receive significantly better insight into automated decision-making processes via the information to be provided. In particular, he or she should be able to recognize which criteria influence the decision and how. He or she also learns what effects data processing has on him or her. A separate provision is proposed below for profiling. The deletion of "referred to in Article 22(1) and (4)" is due to the fact that this wording may lead to the confusion that the obligation to provide information only applies if the data processing is based on paragraphs 1 and 4, but not if the data processing is based on paragraphs 2 and 3.

Furthermore, a division of labor in the context of automated decisions in individual cases must not lead to information about this procedure being omitted or shortened. Therefore, in automated decision-making processes based on the division of labor, the controllers should be obliged to

coordinate their information in such a way that each cooperation partner is informed about his or her part in the process, including the interfaces to all other parts.

## 14. Information regarding profiling I

*Addition of an obligation to provide information for every profiling, even if it is not directly linked to an automated individual decision but is instead used for other assessment purposes.*

To adequately inform the data subject about the additional risk of data processing each time data is collected that is also to be used for profiling, Article 13(2) should be supplemented with a new point (g) and Article 14(2) should be supplemented with an identical point (h).

> "(g/h) the use of the data for profiling as well as its extent, contents, goals and purposes."

The additions increase the transparency of processing. In particular, the data subject should be able to clearly see what possible long-term consequences may arise from processing through profiling. This should make it easier for a consumer to decide whether they want or tolerate profiling and select a service that corresponds to this decision.

## 15. Facilitating the provision of information

*Amending Art. 13 GDPR with rules that facilitate the provision of information in everyday contact/communication.*

When collecting data in everyday contacts, mainly in non-digital environments, on the one hand to make it easier for those responsible to deal with data subjects, but on the other hand to provide the necessary transparency to data subjects who expect information about the processing of their data in such contexts and to prevent abuses, the German Data Protection Conference[2] proposes a provision in Article 13,[3] which is adopted below. Thereafter, Article 13 should be supplemented with a new paragraph 5.

> *"5. The information in accordance with paragraphs 1 and 2 will be communicated only at the request of the data subject, if the controller carries out data processing that the data subject expects or must expect based on the specific circumstances and*
>
> *1. both the disclosure of data to other bodies and the transfer to third countries are excluded,*
>
> *2. no data are processed that fall under Article 9,*
>
> *3. data are not processed for direct marketing purposes and*
>
> *4. neither profiling nor automated decision-making occurs.*
>
> *The data subject must be made aware of this possibility."*

The new paragraph avoids an excess of unwanted information, relieves common, non-digital contacts of overly bureaucratic requirements, but at the same time excludes high-risk data processing. If so desired, information can instead be requested at any time.

[2] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder.

[3] Datenschutzkonferenz, Erfahrungsbericht, 2019, p. 8.

## 16. Information on recipients II

*Obligation of the controller to log all recipients of personal data; obligation to present the contents of the log to the data subject.*

To ensure sufficient information about the recipients of personal data, which enables the data subject to take legal action, or at least makes it significantly easier, a new sentence 2 in Article 24(1) should establish an obligation to record the transfer and the recipient (see below; Nr. 23). Accordingly, the wording of Article 15(1)(c) should be adapted to the changes to Articles 13(1)(e) and 14(1)(f).

> "(c) the recipients *as far as they can be determined* or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;"

The addition ensures that the controller must communicate all recipients known to him including their names and contact details. To ensure that the controller is generally aware of the transfers and the recipients, the new sentence 2 of Article 24(1) establishes an obligation to record the transfers and the recipients.

## 17. Information regarding automated decision-making II

*Obligation of the controller to separately inform the data subject of any profiling, its extent, contents, goals and purposes.*

*Clarification that information on the "logic involved" entails the criteria for the decision and their balancing.*

To settle the dispute about the scope of the information that a controller has to provide about the existence of automated decision-making, the text in Article 15(1)(h) should be clarified in accordance with the proposed additions to the information obligations in Article 13(2)(f) and 14(2)(g):

> "h) the existence of automated decision-making~~, including profiling, referred to in Article 22(1) and (4)~~ and~~, at least in those cases,~~ meaningful information about the logic involved *including the criteria for the decision and their weighting*, as well as the significance and the envisaged *and possible legal and factual* consequences of such processing for the data subject."

The addition extends the proposed changes to the controller's information obligations to the right of access. This creates consistency in the structure of the rights of data subjects and closes gaps in protection that would arise if the extension was not be made. A separate provision is proposed below for profiling. The phrase "referred to in Article 22(1) and (4)" is again deleted because this wording can lead to the confusion that the obligation to provide information only applies if the data processing is based on paragraphs 1 and 4, but not if the data processing is based on is regulated in paragraphs 2 and 3.

## 18. Information regarding profiling II

*Addition of an obligation to provide information for every profiling, even if it is not directly linked to an automated individual decision but is instead used for other assessment purposes.*

To give the data subject a right of access adequate to the additional risk that results whenever data is processed that is used for profiling, Article 15(1) should be supplemented with a new point (i) – comparable to the information obligation under Articles 13(2) and 14(2).

> *"(i) the use of the data for profiling as well as its extent, contents, goals and purposes."*

The addition creates a complement to the proposed provisions in Articles 13(2) and 14(2) in the right of access. Here too, the aim is to create consistency and avoid the creation of gaps in protection.

## 19. Right to obtain a copy

*Specification of the right to obtain a copy; addition of an obligation to communicate all processed data wherever no copy can be provided.*

To settle most of the disputes regarding the right to obtain a copy under Article 15(3), the prvosion should be rephrased:

> "The controller shall *on application of the data subject* provide a copy of the personal data *that are* undergoing processing *and that are or can be combined in a data set*. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form."

The amendments create legal clarity regarding the right to obtain a copy. This makes the right manageable in practice. The addition "on application of the data subject" on the one hand allows the data subject to scale better when exercising the right of access, and on the other hand it makes it easier for the controller to fulfill his or her obligations by clearly signaling to him or her what the data subject expects. The addition "and that are or can be combined in a data set" concentrates the claim on the objects of data processing that specifically deal with the data subject or can be the basis therefore.

## 20. Right to data portability

*Rephrasing the title of the norm in a way that not only describes a possibility, but the action that the consumer may demand, and that the controller is obligated to perform: "right to data transmission".*

*Expansion of the right to data transfer to the data caused by the data subject.*

*Stipulation of the transfer of data in an interoperable format and in the language of the respective member state or in English.*

Article 20(1) should be made more precise in several places or supplemented with important provisions to enable its implementation in practice. Its scope should be expanded to include all data caused or induced by the data subject. Regarding the format in which the data is to be transferred, it should be made clear that it must be interoperable. The European Data Protection Board should determine the requirements for interoperability. In addition, the controller should be required to provide the data in the national language(s) of the Member State or in English. The right to data portability should apply even if the consent or contract no longer exists, but the data was collected by the controller while the consent or contract existed. To implement these changes, Article 20(1) GDPR should be adapted and supplemented with a new sentence 2.

Article 20

Right to data ~~portability~~ transmission

> "1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has ~~provided to~~ *caused or induced at* a controller, in ~~a structured, commonly used and machine-readable~~ *an interoperable* format *and in the official language or languages of the Member State of the data subject or in English*, and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where

(a) the processing is *or was* based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

*The conditions for the interoperability of formats shall be determined by the Commission."*

The name of the right to "portability" suggests a right to potentiality: the ending "ability" only denotes possibility. However, a right to the possibility of transfer does not help the data subject if he or she wants to enforce an actual transfer in addition to the possibility. Therefore, the heading should be corrected. The aim of expanding the scope of the right to data transfer is achieved by replacing the term "provided" with "caused of induced".

The dispute over the vague legal terms "structured, commonly used and machine-readable format" and "technically feasible" will be resolved by deleting these terms from the standard. They are reflected in the demand for an interoperable format. The clarification of the conditions for interoperability will be imposed on the European Data Protection Board. On the one hand, this ensures that a (necessary) specification actually occurs, and on the other hand, a level of detail can be achieved during the specification that is not possible in the Articles or in the Recitals.

## 21. Protection of children in the context of the right to object

*Special consideration of the fact that personal data has been obtained during childhood in the right to object.*

In order to take due account of the fact that the personal data of a child is involved when examining an objection in accordance with Article 21(1), this provision should be supplemented accordingly.

"1. The data subject shall have the right to object, on grounds relating to his or her particular situation, *in particular where the personal data of a child is concerned*, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims."

The amendment strengthens children in the processing of personal data in accordance with Recital 38(1) by clarifying the term "his or her particular situation" directly in the Article.

## 22. Automated individual decision-making, including profiling

*Deletion of the limitation "solely" in the scope of the applicability of the provision.*

*Addition of a prohibition to be subjected to automatically prepared decisions that the human decider adopts without review and without giving the data subject the opportunity to present his or her point of view prior to the decision.*

*Deletion of the limitation that the decision must produce legal effects concerning the data subject or "similarly significantly affects him or her"; a significant detrimental effect shall be sufficient.*

*Deletion of Art. 22(2)(a) GDPR. Processing on the basis of consent of the data subject according to Art. 22(2)(c) is sufficient.*

*Inadmissibility of the consent of a child to the processing of personal data for automated individual decision-making.*

*Addition of qualitative requirements for a decision that is based on an automatically prepared decision in the image of § 31 of the German Federal Data Protection Act.*

*Amendment of Art. 22(3) GDPR with the phrase "and to an explanation of the reasons for the decision".*

*Separate provisions on lawfulness regarding profiling, which shall be unlawful by default and only possible in pre-defined exceptions.*

The right not to be subject to a decision based solely on automated processing, including profiling, enshrined in Article 22 requires several adjustments to the text. On the one hand, the ban on automated individual decisions needs to be broader in scope. On the other hand, the controller or a third party should not be able to justify that the automated decision is necessary in individual cases. It is sufficient if the person responsible can ask the data subject for his or her consent in accordance with paragraph 2(c). Thirdly, in addition to the obligation to provide information, it should be stipulated that the reasons for the decision are explained to the data subject. Furthermore, in paragraph 2(c), the consent of a child should be excluded to protect children. Finally, qualitative requirements for a decision based on automated processing should be included. These adjustments to Article 22 could be made in the following way:

> "1. The data subject shall have the right not to be subject to a decision based ~~solely~~ on automated processing, including profiling, ~~which produces legal effects concerning him or her or similarly~~ significantly affects him or her.
>
> 2. Paragraph 1 shall not apply if the decision:
>
> ~~(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;~~
>
> (~~a~~*b*) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
>
> (~~b~~*c*) is based on the *adult* data subject's explicit consent.
>
> 3. In the cases referred to in ~~points (a) and (c) of~~ paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view, and to contest the decision *and to an explanation of the reasons for the decision*.
>
> *4. The creation of a probability value about a specific future behavior of a natural person for the purpose of a decision based on automated processing, including profiling, is only permitted if the data used to calculate the probability value is verifiably significant for the calculation of the probability of the particular behavior on the basis of a scientifically recognized mathematical-statistical procedure."*

Paragraph 4 becomes paragraph 5. The adjustments in paragraph 1 remove the double restriction of the right from Article 22(1). The expansion (deletion of "solely") and the lowering of the threshold (significant impairment instead of legal effect or similar) mean that numerous previously unrecognized impairments of consumers' fundamental rights are included. This improves their position in data protection law and allows the Union legislature to fulfill its fundamental rights protection obligations. Decision merely prepared by automated processing are now also encompassed. This means that the person concerned is no longer at the mercy of an automatically prepared decision, which the human decision-maker usually adopts without consideration, without the data subject having the opportunity to present their point of view before the decision is made.

The deletion in paragraph 2 ultimately reduces power asymmetries between providers and consumers and closes protection gaps in the Regulation. If paragraph 2(a) is deleted, it is no longer

possible for the controller or a third party to unilaterally declare the necessity of an automated decision in the context of a contract.

"adult": This addition to paragraph 2(b) means that no one can rely on a child's personal consent for a particularly risky automated decision. The consent of the legal guardian remains possible. The addition is to be seen in connection with the proposed addition to Article 9(2)(a) and takes up the assessment of Recital 71(5).

The additions in paragraph 3 mean that in the event of a complaint, the controller has additional transparency obligations. He or she must explain to the data subject the main reasons for the automated decision and its effects.

The amendment of the new paragraph 4 means that qualitative requirements for automated decision-making are set. The new paragraph 4 takes up the considerations from Recital 71 and is based on Section 31(1) of the German Federal Data Protection Act[4] in its wording and standard purpose but is not limited to scoring and credit information.

## 23. Record of data transmission and recipients

*Establishment of an obligation of the controller to record any data transmission as well as the recipients of transmitted data.*

To be able to give data subjects access to information about the recipients of their personal data, the controller should be required to maintain a record of any recipients and the personal data transmitted to them. To create such an obligation, Article 24(1) must be supplemented with a new sentence 2:

> "1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. *The controller shall record any transmission to a third party and the recipient.* Those measures shall be reviewed and updated where necessary. "

The previous sentence 2 becomes the new sentence 3. By adding the new sentence 2, the documentation obligations of the controller are expanded to include a factor that is extremely relevant to creating transparency. Effective enforcement of the rights of the data subject vis-à-vis the recipients is only possible on the basis of logging transfers of personal data.

## 24. Non-waiverability of the rights of the data subject

*Establishing safeguards from the abandonment of the rights of the data subjects in the context of legal transactions.*

In order to protect the rights of the data subject against legal restrictions or exclusion, their non-waiverability should be expressly stated. Such a provision can be based on Section 6 (1) of the

[4] § 31 Bundesdatenschutzgesetz (BDSG): "(1) For the purpose of deciding on the creation, execution or termination of a contractual relationship with a natural person, the use of a probability value for certain future action by this person (scoring) shall be permitted only if 1. the provisions of data protection law have been followed; 2. the data used to calculate the probability value are demonstrably essential for calculating the probability of the action on the basis of a scientifically recognized mathematic-statistical procedure; 3. other data in addition to address data are used to calculate the probability value; and 4. if address data are used, the data subject was notified ahead of time of the planned use of these data; this notification shall be documented."

German Federal Data Protection Act in the version applicable before 25 May 2018.[5] It should be included as a new paragraph 3 in Article 23:

> *"3. The rights of the data subject of access (Article 15), to rectification (Article 16), to erasure (Article 17), to restriction of processing (Article 18), to data transmission (Article 20) or to object (Article 21) cannot be excluded or limited through legal transaction."*

The addition of the new paragraph 3 prevents controllers from abusing their economic power to restrict or exclude the rights of the data subject in favour of their data processing. This accentuates the task of the GDPR to protect the fundamental rights and freedoms of the data subject.

## 25. Duties of manufacturers

*Addition of duties of manufacturers, including liability for manufacturers to support the controller.*

Since controllers cannot in many cases comply with their data protection obligations according to Articles 24 et seqq. without the manufacturers of IT products and programs supporting them, it is necessary to establish independent data protection obligations for them and to match these with the obligations of the controller. To this end, the German Data Protection Conference proposes to define the term manufacturer within the framework of Article 4 in a new No. 27 in accordance with the product liability law of the European Union and to establish specific data protection obligations for the manufacturer in Article 24.[6] This suggestion is adopted below.

> *"(27) 'manufacturer' means the producer according to Article 3 of Directive 85/374/EEC of the Council 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 applies accordingly. To the extent that he or she determines the purposes and means the processing of personal data, the manufacturer is also controller within the meaning of No. 7."*

For Chapter IV GDPR the heading should be:

> "Controller and processor, *manufacturer*"

For Article 24 the heading should be:

> "Responsibility of the controller *and of the manufacturer*".

In addition, Article 24 should be supplemented with a new paragraph 4:

> *"4. The manufacturer develops and designs his or her products, services and applications taking into account the right to data protection and the state of the art in such a way that it ensures that controllers and processors are able to fulfill their data protection obligations without having to make unreasonable changes to these products, services and applications. He or she supports them in drawing up the records of processing activities (Article 30), in reporting a personal data breach (Article 33) and in communicating the personal data breach to the data subject (Article 34) by providing all necessary information upon request."*

The reference in the new No. 27 in Article 4 ensures that the term "manufacturer" used in data protection law corresponds with the term "producer" in the Product Liability Directive. This means

[5] "The rights of the person concerned to information [...] and to correction, deletion or blocking [...] cannot be excluded or limited by a legal transaction."

[6] Datenschutzkonferenz, Erfahrungsbericht, 2019, pp. 16 et seq.

that case law and literature in product liability law can also be referred to and a clear distinction is made regarding the addressees of the manufacturer's obligations in data protection law.

The new paragraph in Article 24 makes it clear that the obligations of the controller who uses the manufacturer's information technology give rise to original support obligations of the manufacturer. This makes the implementation of the duties of the controller and the enforcement of the fundamental right to data protection in accordance with Article 8 GRCh possible in practice. The many users of information technology are also relieved of their role as controllers and the burden is caused where the design competence and thus also the fulfillment responsibility exists.

For the event that it is not fulfilled, the German Data Protection Conference takes up this obligation of the manufacturer in proposed changes to the right to an effective judicial remedy in Article 79 GDPR and in the provision on compensation in Article 82 GDPR.[7]

The new paragraph 4 refers to the fulfillment of all data protection obligations of the controller and the processor, which must be made possible by the manufacturer. This applies to all obligations, including the obligation to implement all rights of the data subject and in particular to the technology-related obligations of data protection through system design and through default settings in accordance with Article 25 GDPR and the guarantee of sufficient security measures in accordance with Article 32 GDPR.

## 26. Data protection by design

*Addition of an obligation to award special protection to the fundamental rights and interests of children.*

*Technologically-specific or sector-specific designation of the obligation of data protection by design by the Board.*

*Expansion of the obligation to producers/manufacturers of systems that process personal data.*

*Special consideration of the fundamental rights and interests of children in the context of data protection by design and by default according to Article 25 GDPR.*

Even if Article 24(4) as amended would implicitly include manufacturers as the addressees of the obligation to design a system in accordance with data protection provisions, a regulatory need could arise to explicitly include manufacturers in the text of Article 25(1) as addressees. For this purpose and also in the event that the proposed addition of paragraph 4 to Article 24 is not implemented, an addition to Article 25(1) is proposed below. In order to take due account of the special risks for children when designing the system in accordance with data protection law, Article 25(1) should be supplemented accordingly:

> "1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller *and the manufacturer of data processing systems* shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects, *in particular of children*."

[7] Datenschutzkonferenz, Erfahrungsbericht, 2019, pp. 16 et seq.

The amendments mean that the rights and freedoms of children are guaranteed special attention in the context of system design. The supplement essentially has a clarifying function, but this is necessary because of the insufficient consideration of children in system design in the past.

Further risk- and application-specific details of the provision are necessary and should be discussed in the context of a risk-oriented revision of the regulation.

## 27. Data protection by default

*Limitation of the purpose to the functionality of the respective service.*

*Amendment of the principle of data avoidance.*

*Addition of an obligation to award special protection to the fundamental rights and interests of children.*

In order to increase the effectiveness of the obligation to provide data protection-friendly default settings in accordance with Article 25(2) and to limit the data protection-unfriendly design options available to controllers, instead of aligning the default setting with a freely definable purpose, it should be required that the default setting depends on which form of the technical function is necessary to provide the main service for the data subject. For this purpose, a new sentence 2 must be inserted into the text. The previous sentences 2 and 3 become sentences 3 and 4. In order to take due account of the special risks for children when setting the data protection-friendly default, Article 25(2) should also be supplemented in a new sentence 5 to take this circumstance into account:

> "2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. *The processing purpose must be taken into account in a way that as few personal data as possible are processed.* That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. *The default settings particularly take into account the need for protection of children.*"

The new sentence 2 means that, in addition to the principle of data minimization (sentence 1), the principle of data avoidance is also made an essential factor in the design and selection of default settings. The starting point is the functional necessity of a certain default setting, for example to fulfill a contractually agreed service. In addition to the subjective necessity for the purpose ultimately dictated by the controller, the objective necessity also becomes relevant.

The addition of a new sentence 5, like the addition of Article 25(1), strengthens the rights and freedoms of children by explicitly mentioning the need for protection of children in the Article and also has a clarifying effect.

## 28. Information obligations of joint controllers

*Clarification that a division of labour or cooperation in the context of automated individual decision-making must not lead to an omission or limitation of information to be provided to the data subject; obligation to inform about divided / cooperative automated decision processes that has to be met by every cooperating partner concerning their contribution to the process including the interfaces to all other contributions.*

In order to ensure that, in the case of joint responsibility for data processing, the information that those who are jointly responsible must provide to the data subject is actually provided in full, the

text of Article 26(1)(2) should expressly state that controllers are obliged to coordinate their information in such a way that complete information for the data subject is guaranteed:

> "1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them *to ensure complete information for the person concerned* unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects."

The addition specifies the level of coordination between joint controllers: They must cooperate in such a way that their respective efforts to inform the data subject do not create any information gaps for the data subject. It also ensures that the joint controllers are liable for the fulfillment of this requirement in accordance with Article 83(5)(b). They can be effectively sanctioned if the information is incomplete or not provided.

## 29. Personal data of children IV

*Incorporation of an obligation to special consideration of the fundamental rights and interests of children in the context of risk analysis and when determining measures for protection during a data protection impact assessment.*

In order to take due account in every data protection impact assessment of the fact that personal data of children are being processed, Article 35(1) and (7) should be supplemented to take this into account:

> "1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, *in particular as a result of processing of personal data of a child*, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. …
>
> 7. The assessment shall contain at least:
>
> (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
>
> (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
>
> (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1 *which particularly takes into special consideration if personal data of children is concerned*; and
>
> (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned, *in particular of children*."

The amendments consistently continue the proposals to amend Articles 21, 25 and 34 and also extend them to data protection impact assessment. The aim here is also to strengthen the rights

and freedoms of children by ensuring that these are actually taken into account by controllers by explicitly addressing children in the text. However, the additions to Article 35 go beyond mere clarifications and establish concrete obligations when carrying out a data protection impact assessment to give special consideration to children, which extend to both the risk analysis and the definition of protective measures.

## 30. Powers of the supervisory authorities

*Amendment of the powers of the supervisory authorities in Article 58(1) and (2) GDPR with the power to instruct manufacturers.*

To be able to enforce compliance of manufacturers, the supervisory authorities need powers to be able to order effective measures against them. Such a provision cannot be found in the proposal of the German Data Protection Conference. Therefore, the intention of the Data Protection Conference is completed below and a wording that complements its proposal is recommended. For this purpose, it should be sufficient to include manufacturers in the authorisation provision in Article 58(1)(a) and (d) and 58(2)(a), (b) and (d) and to supplement these provision as follows:

> "1. Each supervisory authority shall have all of the following investigative powers:
>
> (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative, *and the manufacturer* to provide any information it requires for the performance of its tasks; …
>
> (d) to notify the controller, ~~or~~ the processor *or the manufacturer* of an alleged infringement of this Regulation; …
>
> 2. Each supervisory authority shall have all of the following corrective powers:
>
> (a) to issue warnings to a controller, ~~or~~ processor *or a manufacturer* that intended processing operations are likely to infringe provisions of this Regulation;
>
> (b) to issue reprimands to a controller, ~~or~~ processor *or a manufacturer* where processing operations have infringed provisions of this Regulation; …
>
> (d) to order the controller, ~~or~~ processor *or a manufacturer* to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; …"

These amendments are necessary for effective enforcement of the manufacturer's obligations under the proposed new Articles 24 and 25. They are the necessary consequence of a serious commitment by manufacturers to fulfill their own data protection obligations. Then again, the five powers mentioned should also be sufficient to provide sufficient incentives for manufacturers to fulfill their obligations – together with the possibility of sanctions and the options for action of the data subject.

## 31. Tasks of the European Data Protection Board

*Incorporation of additional tasks of the European Data Protection Board in Art. 70(1) GDPR: Specification of the obligation to data protection by design according to Art. 25(1) GDPR and data protection by default according to Art. 25(2) GDPR as well as specification of interoperable formats for a transmission of data following Art. 20(1) and (2) GDPR.*

The proposed changes to the GDPR establish three additional tasks for the European Data Protection Board. These should be included in the list of tasks of the Board in Article 70(1). Here, the tasks for specifying the obligation to design a system aligned with data protection requirements in accordance with Article 25(1) and the obligation to set data protection-friendly defaults in ac-

cordance with Article 25(2) can be combined into one task. In the text, additions of a point ea and a point fa are recommended:

> *"(ea) provide guidelines, recommendations and best practices in accordance with point (e) of this paragraph to further define the interoperable formats for transferring data in accordance with Article 20(1) and (2); …*
>
> *(fa) provide guidelines, recommendations and best practices in accordance with point (e) of this paragraph to further define the data protection obligation on a technical and sector-specific basis through system design in accordance with Article 25(1) and by default in accordance with Article 25(2)."*

These additions ensure coherence within the Regulation and ensure that the Board also provides additional clarifications with regard to the proposed changes and makes recommendations on the specific design

## 32. Remedies and penalties with regard to manufacturers

*Extension of the right to an effective judicial remedy and the right to receive compensation to manufacturers.*

To complete the integration of manufacturers into the data protection obligations of the controller and the processor and to make it effective in practice, the German Data Protection Conference proposes to extend the right to an effective judicial remedy in Article 79 to the manufacturer and his obligations under the proposed Articles 24 and 25.[8] This suggestion is adopted below.

For this purpose, Article 79(2) should be supplemented by the inclusion of the manufacturer as a possible opponent of the legal remedy:

> "2. Proceedings against a controller, ~~or~~ a processor *or a manufacturer* shall be brought before the courts of the Member State where the controller, ~~or~~ processor *or manufacturer* 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, ~~or~~ processor *or manufacturer* is a public authority of a Member State acting in the exercise of its public powers."

These additions to Article 79(2) mean that the data subject can also legally demand that the manufacturer fulfills his or her data protection obligations. As a rule, he or she will first contact controller or the processor. If they do not see themselves in a position to fulfill the legitimate request of the data subject because this is technically impossible for them, the data subject can request the data protection-compliant system design in accordance with the proposed Article 25(1) or another support service in accordance with the proposed Article 24(4) from the manufacturer in court. This possibility will significantly support the effective enforcement of data protection law.

The German Data Protection Conference also proposes to extend the provisions on liability and compensation in Article 82 to the manufacturer and his obligations under the proposed Articles 24 and 25.[9] The aim is to ensure that the integration of manufacturers into the data protection obligations of the controller and the processor is successful and can be effectively implemented in practice. This suggestion is adopted below.

For this purpose, Article 82 should be supplemented with an additional paragraph 7:

[8] Datenschutzkonferenz, Erfahrungsbericht, 2019, pp. 16 et seq.

[9] Datenschutzkonferenz, Erfahrungsbericht, 2019, pp. 16 et seq.

> *"7. If the damage is due in whole or in part to the actions or omissions of the manufacturer, the manufacturer is liable to the data subject in addition to the controller or the processor. He or she is also liable to the controller and the processor."*

This additional paragraph means that a data subject who has suffered damage as a result of a violation of the manufacturer's data protection obligations in accordance with the proposed Articles 24(4) and 25(1) can also assert this against the manufacturer. This not only ensures a fair balance between causing damage and compensating for damage, but also helps ensure that manufacturers actually fulfill their data protection obligations. The liability creates an additional incentive for manufacturers to fulfill their data protection obligations. The additional paragraph also brings about harmony between data protection and product liability law.

## 33. Imposing administrative fines

*Specification of the provisions on administrative fines through guidelines issued by the Board in accordance with Art. 70(1)(2)(k) GDPR; specification through non-binding catalogues on fines by the data protection authorities of the member states.*

*Amendment of Art. 83(4)(a) GDPR with a cross reference to the responsibilities of the manufacturer.*

*Obligation of the data protection authorities to publish an annual statistic on the issuing of fines.*

To be able to impose sanctions on manufacturers who disregard their newly proposed data protection obligations, additional provisions are required. Such provisions are missing from the proposal of the German Data Protection Conference. Therefore, the intention of the Data Protection Conference is completed below and a wording that complements its proposal is recommended in order to be able to impose sanctions on manufacturers as well. For this purpose, Article 83(2) should be supplemented in points (c), (d), (e) and (h) as follows:

> "(c) any action taken by the controller, ~~or~~ processor *or manufacturer* to mitigate the damage suffered by data subjects;
>
> d) the degree of responsibility of the controller, ~~or~~ processor *or manufacturer* taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
>
> e) any relevant previous infringements by the controller, ~~or~~ processor *or manufacturer*; …
>
> h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller, ~~or~~ processor *or manufacturer* notified the infringement; …"

For the same reason, paragraph 3 of Article 83 should be supplemented as follows:

> "3. If a controller, ~~or~~ processor *or manufacturere* intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement."

Finally, the actual threat of sanctions must be included in Article 83(4)(a). This provision should also contain a reference to the specific manufacturer obligation in the proposed Article 24(4).

> "(a) the obligations of the controller, ~~and~~ the processor *and the manufacturer* pursuant to Articles 8, 11, *24(4)*, 25 to 39 and 42 and 43;"

These additions mean that the supervisory authorities can effectively enforce the specific data protection obligations of the manufacturers in accordance with the proposed Articles 24 and 25. Only the threat of sanctions in Article 83 contains the necessary incentives for those addressed to comply with their obligations, even in the face of economic incentives not to do so. In particular,

Article 83(6) enables the supervisory authorities to give the necessary emphasis to their new powers in accordance with Article 58, including towards manufacturers.

In order to support the enforcement of the GDPR, to create transparency about the actions of authorities and to contribute to a harmonized practice of imposing fines, the supervisory authorities should publish semi-annual statistics on these procedures. For this purpose, Article 83 should be supplemented with an additional paragraph 10:

> *"10. Each supervisory authority shall publish statistics on the procedures carried out in accordance with this Article one month after the end of each six-month period."*

This additional paragraph brings about a significant increase in transparency. On the one hand, the consumer can convince himself of the effective enforcement of data protection law, and on the other hand, a controller can better anticipate how the extremely broad fine framework of the GDPR will be applied in practice.

SPONSORED BY THE

Federal Ministry
of Education
and Research

Plattform
Privatheit

PUBLISHER

Fraunhofer

Natur
Technik
Kultur
Gesellschaft
UNIKASSEL
VERSITÄT