provet

Projektgruppe verfassungsverträgliche Technikgestaltung

Evaluation of the General Data Protection Regulation from a consumer perspective

- English excerpts -

Expert report commissioned by Verbraucherzentrale Bundesverbands e.V. (vzbv)

Responsible person:

Univ.-Prof. Dr. jur. Alexander Roßnagel

Carried out by:

Univ.-Prof. Dr. jur. Alexander Roßnagel

Dr. jur. Christian Geminn

Kassel, 26. November 2019

Remark

This text is an English excerpt from the German-language expert report "Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht" carried out by Prof. Dr. Alexander Roßnagel and Dr. Christian Geminn on behalf of the Federation of German Consumer Associations (vzbv) in November 2019. All chapter numbers, references and footnotes in the text refer to the German report, which is available online at https://www.vzbv.de/sites/default/files/downloads/2019/12/04/19-11-26_gutachten_evaluation_dsgvo.pdf

Executive Summary

The GDPR has improved the standing of consumers regarding the processing of personal data in many places. Examples are the residence principle, the right to data portability, data protection by design, the right to lodge a complaint and the sanctioning of violations.

Yet, it does not realise its full potential. On the one hand, the GDPR has created significant 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 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 scoring. Both hinder the innovations that the GDPR aimed to introduce 2018 into the European data protection practice. They are unable to unfold their potentials when it comes to protecting consumers.

This report shows that issues exist on two levels. First, there are issues that result from deficits in the text of the regulation. Here, the report suggests 28 alterations of the text in order to improve it – from the point of view of consumers. Beyond that, there are conceptional issues that cannot be resolved with smaller alterations of the text of the norm. The report formulates approaches to these issues whose implementation is directed more towards the future.

The evaluation of the GDPR that is scheduled for the year 2020 presents the ideal opportunity to point out these issues to union lawmakers and to present proposals that constructively evolve the GDPR. The goal must be to reduce the power gradient between providers and consumers. This goal is achieved by better bringing to bear the innovations that are laid out already in the GDPR.

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. Where this is not the case, instead of the union lawmakers, the lawmakers of the member states, the European Data Protection Board and the national data protection authorities need to enact laws or guidelines. The report contains proposals regarding this as well.

In particular, the report proposes the following revisions of the GDPR:

Processing in the course of a purely personal or household activity:

- Retraction of the complete exemption of invasive data processing from the material scope of the GDPR in Art. 2(2)(c); instead risk-adequate differentiation also in the context of personal or household activity; complete exemption from the material scope only for low-risk processing; for heightened risks application of select provisions of the GDPR.

Residence principle:

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

Principles relating to processing of personal data:

- Adjustment of the German language version of the GDPR: Replacing the term "Treu und Glauben" in Art. 5(1)(a) with "Fairness".
- Amendment of the GDPR with an obligation to data avoidance in Art. 5(1)(c).
- Modernising and risk-adequate evolution of the principles.

Relations between consent and other grounds for lawful processing:

- Clarification in Art. 6(1)(1) GDPR that a controller in addition to consent cannot rely on another ground for lawful processing.

Profiling:

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

Processing of data of children:

- 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.
- Transfer of recital 38(2) GDPR to the articles, prohibiting the use of personal data of children for the purposes of marketing or profiling.
- Exclusion of the consent of a child from the processing of special categories of personal data according to Art. 9(2)(a) GDPR.
- Special consideration of the fact that personal data has been obtained during childhood in the right to object.
- Exclusion of the consent of a child to the processing of personal data for automated individual decision-making.

- 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.

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.

Presenting information:

- Addition of sector specific or technology specific provisions regarding the presentation of information in the context of specific fields of processing and technologies.
- Presentation of information that is adequate to the situation, the interests and the decisions involved.
- Limitation of information to the actual circumstances of the respective processing that is about to occur.

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.
- 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 his or her contribution to the process including the interfaces to all other contributions.
- 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.

Right of access by the data subject:

- Obligation of the controller to log all recipients of personal data; obligation to present the log to the data subject.
- Obligation of the controller to separately inform the data subject of any profiling, its extent, contents, goals and purposes.
- Specification of the right to be provided with a copy; addition of an obligation to communicate all processed data wherever no copy can be provided.

Right to data portability:

- Rephrasing the title of the norm in a way that not only presents a possibility, but the action that the consumer may demand and that the controller is obligated to perform: “Recht auf Datenübertragung” / “right to data transfer”.
- 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 German (or the respective language of the member state) or in English.

Automated individual decision-making:

- Deletion of the limitation “solely”.
- 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 detrimental effect shall be sufficient.
- Deletion of Art. 22(2)(a) GDPR. The consent of the data subject according to Art. 22(2)(c) shall be sufficient.
- 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 “to clarification of the reasons for the decision”.

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 specification of the obligation of data protection by design by the Board.
- Expansion of the obligation to producers/manufacturers of systems that process personal data.

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.

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

Data protection law governs a field of law that is challenged constantly and profoundly by emerging business models and the dynamic evolution of information technology. Therefore, the GDPR cannot be the final act in the discussion on the structural foundation and implementation of data protection law. Rather, developments are on the horizon that simply overstrain the current data protection law. The reason for this is on the one hand that the GDPR in essence maintains the fundamental concepts of data protection law that were developed in the 1970s. On the other hand, it results from the refusal of the union lawmakers to enact technologically specific basic rules that do justice to the biggest threats to fundamental rights caused by modern information technology. The report offers food for thought regarding these fundamental questions and outlines approaches that prevent disadvantages for consumers in the context of the risks that emerge from these challenges.

[…]

2.3 Proposed provisions

This section of the report sets out suggestions for how the amendments to individual provisions of the General Data Protection Regulation proposed in this report could be worded, and is intended as a basis for discussion on how these provisions could be improved.

2.3.1 Residence principle

To extend the territorial scope of the General Data Protection Regulation to any form of processing of personal data of data subjects residing in the European Union, thereby ensuring the consistent application of the residence principle, the following amendment to Art. 3 (2) (a) GDPR 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 offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union~~ *contacting such data subjects in the Union, irrespective of whether a payment by the data subject is required*;"

Removing the "offering of goods or services" requirement means this proposition no longer has to be differentiated from other activities. This extends the group of controllers or processors

affected because it means that every contact with a person within the Union is covered by the Regulation. However, the Regulation does not apply if the initiative for the ultimate processing of personal data comes from the data subject themselves rather than from the controller or processor.

2.3.2 Data protection principles

In order to describe the second principle of Art. 5 (1) (a) GDPR in terms that are appropriate to its purpose, and to avoid confusion based on a German civil-law understanding of the term "good faith", the following change is recommended to the German version of Art. 5 (1) (a) GDPR:

> "(1) Personal data shall be
>
> a) processed lawfully, *fairly* ~~in good faith~~ and in a transparent manner in relation to the data subject ('lawfulness, *fairness* ~~processing in good faith~~ and transparency');"

The following amendment to Art. 5 (1) (c) GDPR is recommended in order to extend the principle of data minimisation to include the principle of data reduction:

> "(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 selected and designed with the objective of processing as little personal data as possible (data reduction)*;"

Use of the formulation "processing as little personal data as possible" brings the proportionality principle to the fore. It is important that data minimisation is not merely applied for a specific purpose chosen by the controller, but that the processing of personal data is reduced by designing the system with the purpose in mind.

2.3.3 Priority of consent

To make it clear that a processor cannot, in addition to consent, claim another legal ground for the processing of personal data, the following amendment to the first subparagraph of Art. 6 (1) GDPR is proposed:

> "(1) Processing shall be lawful only if and to the extent that ~~at least one of the following applies~~ ~~a) The~~ *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 changes make it clear that consent and the other lawful grounds can only be used as alternatives. By adding an "either – or" and thereby separating consent from the lawful grounds provided by statute, and deleting the "at least", the option to equate consent with the lawful grounds provided by statute and to combine it with these is removed. After the amendment,

there will only be two – mutually exclusive – ways to justify the data processing. This will prevent a controller, having obtained consent, from relying on a different lawful ground for processing the data. If consent is obtained, the controller must allow its activities to be subject to the provisions governing consent.

2.3.4 Determining the purpose of the contract

In order to define the lawful ground of the current point (b) of the first subparagraph of Art. 6 (1) GDPR more precisely and make it more objective, the following amendment 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 including a reference to the objective necessity of processing of personal data for the performance of the contract, the lawfulness is tied to the functional necessity of the agreed activity. It is no longer possible to formulate contracts in such a way as to justify more far-reaching data processing – such as providing information from associated companies or keeping the customer informed about other products – that is not necessary to fulfil the primary obligations of the contract. Such data processing activities are only possible if they are justified by overriding legitimate interests or if the data subject has given consent.

2.3.5 Checking that the processing purposes are compatible

In order to take due account of the fact that the personal data of a child are involved when assessing the compatibility of an old purpose with a new one, point (d) of the first subparagraph of Art. 6 (4) GDPR should be amended as follows:

> "d) the possible consequences of the intended further processing for data subjects, *particularly where the personal data relate to a child*;"

This addition requires the controller to pay particular attention to the consequences of further processing for children, where changes to the processing purpose are planned. This duty is at most implied in the current text (via recital 38 sentence 1 GDPR) and should be explicitly included in the normative text to strengthen the position of children in terms of data protection.

2.3.6 Exclusion of the consent of a child to marketing and profiling

In order to incorporate the premise of recital 38 sentence 2 GDPR into the wording of Art. 8 (1) GDPR,[1] the following new sentence 2 is proposed:

> "This does not apply to the processing of personal data of a child for the purposes of marketing or creating personality or user profiles."

The current sentence 2 becomes sentence 3. The addition changes recital 38 sentence 2 GDPR from interpretation guidance into directly applicable law and thereby strengthens legal certainty.

[1] See section 2.1.6.

2.3.7 Exclusion of the consent of a child to processing of special categories of personal data

In order to ensure that they are adequately protected against particular risks, children should not be able to consent to the processing of special categories of personal data in accordance with Art. 9 (2) (a) GDPR.[2] The inclusion of an additional word is proposed:

> "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;"

The effect of this addition is that no one can rely on the personal consent of a child to the particularly risky processing of special categories of personal data. Consent can still be given by the parent or guardian.

2.3.8 Provision of information must relate only to data processing intended to be performed in the near future

In order to comply with the duty to provide information to the data subject about the processing of his or her data, all information about data processing must always be comprehensive and precise and include all the necessary details.[3] The following amendment to the text in Art. 12 (1) GDPR 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 addition of the word "current" makes it clear that the information must relate to the data processing being planned at the present time, for which the scope, purpose and method of processing have been established and are known in full. This prevents controllers from fulfilling this duty to provide information through reference to a privacy policy that covers all conceivable future forms of data processing with vague references to future possibilities. Future changes to data processing activities that have not yet been determined and therefore cannot be precisely described must lead to new information being provided at the relevant time.

The amendment should be accompanied by a clarification in recital 60 GDPR to the effect that highly complex data processing is no excuse for deficient information.

---

2 See section 2.1.6.
3 See section 2.1.7.1.

2.3.9 Balance between duty to provide information and protection of secrecy

In order to provide the maximum possible level of information on data processing while protecting legally recognised secrets and intellectual property rights, the controller should be obliged to seek ways of providing the most comprehensive and accurate information possible without breaching secrecy.[4] A new paragraph 7 should be added to Art. 12 GDPR containing a general rule on to resolve the conflict between information and secrecy (practical concordance principle):

> "*(7) If the information to be provided to the data subject compromises the rights and freedoms of other persons, such as commercial secrecy or intellectual property rights, the controller shall ensure the maximum possible level of information while respecting those rights and freedoms.*"

The current paragraphs 7 and 8 become paragraphs 8 and 9. The addition of a new rule to resolve the conflict between the right to information and the protection of secrecy applies to all information to be provided by the controller to the data subject about the data processing. This will, in particular, improve the level of information in cases of automated decision-making processes.

In accordance with the text of the new paragraph 7 of Art. 12 GDPR, the considerations in recital 63 sentences 5 and 6 GDPR[5] will need to be adapted to the new rule. References to appropriate procedures to protect commercial secrecy or intellectual property rights (e.g. 'noise addition') could be provided here. Moving this into recital 58 or 60 GDPR would also be a possibility.

2.3.10 Up-to-date and relevant information about data collection

In order to ensure that the controller provides the data subject with the relevant information "at the time when personal data are obtained",[6] the introductory sentences to Art. 13 (1) and (2) GDPR should be amended as follows:

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

These additions ensure that the information is provided at the right time (and is thus appropriate to the situation), namely at the time the data are collected and before the data subject is required

---

4 See section 2.1.8.2.
5 See section 2.1.8.2.
6 See section 2.1.7.3.

to make or has the option to make a decision. This strengthens the data subject's right of self-determination and, in particular, increases the transparency of complex processing activities.

2.3.11 Information about recipients

In order to provide adequate information about the recipients of personal data and thereby enable a data subject to pursue their legal rights, or at least make it considerably easier for them to do so,[7] the wording of Art. 13 (1) (e) GDPR should be amended slightly:

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

The same change should be made to the identically worded Art. 14 (1) (e) GDPR.

The addition requires the controller to disclose all recipients of personal data known to it. If it is possible for the controller to name a recipient specifically, it cannot resort to simply naming categories of recipient. Naming categories of recipient is however permitted if a specific recipient cannot (yet) be named at the time the information is provided.

2.3.12 Information on automated decision-making processes

To avoid disputes about the scope of the information that a controller is required to provide about the existence of an automated decision-making process, the text of Art. 13 (2) (f) and 14 (2) (g) GDPR should be made more precise.

> "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 decision-making criteria and their weighting* as well as the significance and the envisaged *and possible legal and actual* consequences of such processing for the data subject."

The addition better protects the interests of the consumer who, in future, will receive a significantly clearer insight into automated decision-making processes as a result of the information to be provided. In particular, consumers will be able to see which criteria influence the decision and how they influence it. They will also find out what impact the data processing has on them. A separate provision is proposed for profiling below. The words "referred to in Article 22 (1) and (4)" are deleted because this formulation could be misleading and suggest that the obligation to provide information applies only when data processing is based on paragraphs 1 and 4, but not when the data processing is governed by paragraphs 2 and 3.

Also, a division of labour in the context of automated decisions in an individual case must not result in information about this procedure not being supplied, or not being supplied in full. Where the activities involved in an automated decision-making process are split between different providers, the controllers should be required to coordinate their information so that every party involved provides information about its part of the process and about the interfaces with all other parts.[8]

---

7 See section 2.1.8.

8 See also section 2.3.24 with regard to this proposal.

2.3.13 Information about profiling

To ensure that the data subjects are adequately informed about the additional processing risk when data are collected that are also intended to be used for profiling, Art. 13 (2) GDPR should be amended to include a new point (g) and Art. 14 (2) GDPR should be amended to include an identical new point (h).

> "*g/h) the use of the data for profiling and the scope, content, objectives and intended purpose of such profiling.*"

These additions will increase the transparency of the processing. In particular, it should be clear to the data subject what possible further consequences could arise from the profiling. This would make it easier for consumers to decide whether they wish the profiling to take place or will tolerate it, and to select a service on the basis of this decision.

2.3.14 Right to access information about recipients

In order to ensure that data subjects are able to access adequate information about the recipients of personal data and thereby pursue their legal rights, or at least make it easier for them to do so[9], a new sentence 2 should be added to Art. 24 (1) GDPR containing an obligation to keep records of the transfer and the recipients, and the wording of Art. 15 (1) (c) GDPR should be amended slightly in line with the new version of 13 (1) (e) GDPR and Art. 14 (1) (f) GDPR:

> "c) the recipients*, when 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;"

This addition will ensure that the controller must notify the data subject of all recipients known to it, with names and contact details. In order to ensure that the controller is generally aware of the transfers and the recipients, the new sentence 2 in Art. 24 (1) GDPR includes a requirement to document the transfers and the recipients.[10]

2.3.15 Right to access information about automated decision-making processes

To avoid disputes about the scope of access to information that a controller is required to provide about the existence of an automated decision-making process, the text of Art. 15 (1) (h) GDPR should be made more precise – in accordance with the proposed amendments to the duties to provide information in Art. 13 (2) (f) and 14 (2) (g) GDPR.

> "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 decision-making criteria and their weighting* as well as the significance and the envisaged *and possible legal and actual* consequences of such processing for the data subject."

This addition will extend the proposed changes to the controller's information-providing duties[11] to the data subject's right of access. This creates consistency across the data subject's

---

9 See section 2.1.9.
10 See section 2.3.21.
11 See section 2.3.12.

various rights and closes gaps in protection that would arise if this change were not made. A separate provision is proposed for profiling below. The words "referred to in Article 22 (1) and (4)" are deleted here too, because this formulation could be misleading and suggest that the obligation to provide information applies only when data processing is based on paragraphs 1 and 4, but not when the data processing is governed by paragraphs 2 and 3.

2.3.16 Right to access information about profiling

To give data subjects an adequate right to access information about the additional processing risk when data are processed for profiling purposes, a point (i) should be added to Art. 15 (1) GDPR – similar to the obligation to provide information under Art. 13 (2) and Art. 14 (2) GDPR.

> "i*) the use of the data for profiling and* ***the scope, content, objectives and intended purpose of such profiling****.*"

This addition will create a right to access information that mirrors the proposed provisions in Art. 13 (2) and Art. 14 (2) GDPR[12]. The purpose here, too, is to create consistency and to prevent gaps in protection from arising.

2.3.17 Right to a copy

To avoid most disputes about the right to obtain a copy under Art. 15 (3) GDPR, the provision should be reworded:

> "The controller shall provide *upon request from the data subject* a copy of the personal data undergoing processing *that are or may be grouped together in a single data record*. 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 addition creates legal clarity with regard to the right to obtain a copy. It makes the right to obtain a copy more workable. The addition of "upon request from the data subject" allows the data subject to scale the request better when exercising the right to access information, while at the same time it makes it easier for the controller to comply with its obligations because the data subject clearly signals to the controller what he or she expects from it. The addition of "that are or may be grouped together in a single data record" narrows down the request to the objects of the data processing that are or could be specifically concerned with the data subject.

2.3.18 Right to data porting

In order for Art. 20 (1) GDPR to be implemented in practice, there are various points that need to be reformulated more precisely or have important clarifications added. The scope of the provision should be extended to include all data that the data subject has caused to be collected. It should be made clear that the format in which the data are to be provided must be interoperable. The requirements for interoperability should be specified by the European Data Protection Board. Furthermore, the controller should be required to provide the data in the language of the Member State concerned or in English. The right to data porting should also apply if the consent

[12] See section 2.3.13.

is no longer valid or the contract is no longer in force but the data were collected by the controller when consent existed or a contract was in force.[13] In order to implement these changes, Art. 20 (1) GDPR should be amended and a new sentence 2 added.

Article 20

Right to data port~~ability~~*ing*

"(1) The data subject shall have the right to receive the personal data concerning him or her, which he or she has ~~provided to a controller~~ *caused to be collected by a controller*, in a*n* ~~structured, commonly used and machine-readable~~ *interoperable* format *and in the language 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 based *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 requirements for interoperability of the formats shall be defined by the European Data Protection Board."

The way in which the right is currently couched as a right to "portability" with its "-ability" ending suggests that it is merely a possibility. However, the right to the possibility of porting does not help the data subject who wishes to enforce actual porting, not merely the possibility of such. The heading should therefore be amended. The aim of extending the scope of the right to data porting is achieved by replacing the word "provided" with the word "caused". Any dispute about the undefined legal terms "structured, commonly used and machine-readable format" and "technically feasible" is resolved by deleting these terms from the normative text. The requirement becomes "an interoperable format" instead. The European Data Protection Board is charged with defining the requirements for interoperability. This ensures firstly that the necessary clarification of the wording is actually implemented, while at the same time a degree of detail can be achieved in the clarification that is not possible in the normative text or in the recitals.

2.3.19 Protection of children in connection with objections

In order to take due account of the fact that personal data of a child are involved when examining an objection under Art. 21 (1) GDPR, this provision should be amended accordingly.

"(1) The data subject shall have the right to object, on grounds relating to his or her particular situation, *particularly if the personal data relate to a child,* 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

[13] See section 2.1.10.

and freedoms of the data subject or for the establishment, exercise or defence of legal claims."

The amendment strengthens the protection of children when their personal data is being processed, in accordance with recital 38 sentence 1 GDPR, by clarifying the phrase "his or her particular situation" in the normative text.

2.3.20 Automated individual decision-making

The right to not to be subject to a decision based solely on automated processing – including profiling – provided for in Art. 22 GDPR requires several adjustments.[14] Firstly, the prohibition on automated individual decision-making should be framed more widely.[15] Secondly, the controller or a third party should not be able to claim as justification that the automated individual decision-making is necessary. It is sufficient if the controller can ask the data subject for their consent in accordance with paragraph 2 (c). Thirdly, in addition to the obligation to provide the data subject with access to information, there should be a requirement to explain the grounds for the decision to the data subject. And to protect children, the consent of a child should be excluded under paragraph 2 (c). Finally, qualitative requirements for a decision based on automated processing should be included. These amendments to Art. 22 GDPR could take the following form:

"(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 have the grounds for the decision explained*.

(4) The use of a probability value for certain future action of a natural person for the purpose of a decision based on automated processing, including profiling, shall

---

14 See sections 2.1.11 and 2.2.3.

15 With regard to profiling carried out in preparation for automated decision-making, see sections 2.1.12 and 2.2.3.

be permitted only if the data used to calculate the probability value are demonstrably relevant for calculating the probability of the action on the basis of a scientifically recognised mathematical or statistical procedure."

Paragraph 4 becomes paragraph 5. The amendments in paragraph 1 remove the double restriction on the right arising from Art. 22 (1) GDPR. The effect of the extension (deletion of "exclusively") and the lowering of the threshold (significant effect instead of legal effects or similar) is to include numerous constraints on consumers' basic rights that were not previously covered. This improves the position of consumers under data protection law and enables the EU legislators to fulfil their obligation to protect fundamental rights. Decisions for which the preparatory work is done by automated processing are now also included. This means that the data subject is no longer at the mercy of decisions based on automated processing, which are generally accepted at face value by the human decision-maker without the data subject having an opportunity to express his or her point of view before the decision is taken.

The effect of the deletion in paragraph 2 is to remove the power imbalance between provider and consumer and close gaps in protection in the Regulation. If paragraph 2 (a) is removed, it is no longer possible for the controller or a third party unilaterally to declare that an automated decision is necessary in the context of a contract.

The effect of the addition to paragraph 2 (b) ("adult") is that no one can rely on the personal consent of a child to the particularly risky automated decision-making process. Consent can still be given by the parent or guardian. The addition is to be seen in the context of the proposed amendment to Art. 9 (2) (a) GDPR and picks up on the premise of recital 71 sentence 5 GDPR.

The effect of the amendment to paragraph 3 is that in the event of a complaint, the controller has additional obligations with regard to transparency. The controller is obliged to explain to the data subject the relevant grounds for the decision made by means of automated processing, and its consequences.

The effect of the insertion of the new paragraph 4 is to specify qualitative requirements for automated decision-making. The new paragraph 4 picks up on the considerations outlined in recital 71 GDPR and, in terms of its wording and normative purpose, is based on section 31 (1) of the German Data Protection Act (BDSG), although is not limited to (credit)scoring as that provision is.

2.3.21 Documentation of data transfers and the recipients

In order to be able to give the data subject information about who has received their personal data in the event of a request for access to such information, the controller is required to keep records of the recipients and the data transferred. Establishing this requirement necessitates the addition of a new sentence 2 to Art. 24 (1) GDPR:

"(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 keep records of the transfers of personal data to third parties and the recipients of such data.* Those measures shall be reviewed and updated where necessary."

The current sentence 2 becomes the new sentence 3. The addition of the new sentence 2 extends the record-keeping obligations of the controller to include a factor that is extremely relevant in terms of creating transparency. Data subjects can only effectively enforce their rights against the recipients if there are records documenting the transfers of personal data.

2.3.22 Data protection by design

The wording of Art. 25 (1) GDPR should specifically mention the system manufacturers[16] and should also be amended to ensure that due account of the special risks to children is taken when designing systems in accordance with data protection requirements:[17]

> "(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, *especially children*, 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."

The purpose of this addition is to ensure that particular attention is paid to the rights and freedoms of children when systems are designed. The purpose of the addition is thus primarily clarification – which is necessary because children's rights and freedoms have not been given sufficient consideration in system design in the past.

Further steps towards making the legislation more specific with regard to risk and application are necessary and will be discussed in connection with a risk-focused update of the Regulation.[18]

2.3.23 Data protection by default

Maximum force needs to be given to the obligation to ensure data protection by default set out in Art. 25 (2) GDPR and to limit the scope for a controller to set up systems in a way that is not conducive to data protection. Rather than the default settings being set in such a way that the purpose can be freely determined, they should be set in a manner to produce the configuration of the technical functionality that is required in order to provide the main service to the data subject.[19] To this end, a new sentence 2 should be added to the normative text. The current sentences 2 and 3 become sentences 3 and 4. In order to ensure that the special risks to children

---

16 See sections 2.1.13.2 and 2.2.4.
17 See section 2.1.6.
18 See section 3.3.1.
19 See section 2.1.14.

are taken into account in the context of data protection by default,[20] Art. 25 (2) GDPR should have a new sentence 5:

> "(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. *Consideration must be given to formulating the processing purpose in such a way that as little personal data as possible is 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 must take particular account of the need to protect children.*"

The effect of the new sentence 2 is that, in addition to the principle of data minimisation (sentence 1), the principle of data reduction is also elevated to a key factor in the design and selection of default settings. The starting point is the functional need for a certain default setting – for example to provide a contractually agreed service. In addition to the subjective necessity for the purpose, which ultimately is dictated by the controller, the objective necessity now also becomes relevant.

Like the amendment to Art. 25 (1) GDPR, the addition of a new sentence 5 which explicitly incorporates the need to protect children into the normative text has the effect of strengthening the rights and freedoms of children and also serves to provide further clarification.

2.3.24 Obligations to provide information where there are joint controllers

To ensure that all the information required to be provided to the data subject by the joint controllers in cases where responsibility for data processing is shared is indeed provided, the wording of Art. 26 (1) sentence 2 GDPR should explicitly state that the controllers are obliged to coordinate their information in such a way as to ensure that the data subject is fully informed.

> "(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, *in order to ensure that the data subject is fully informed*, by means of an arrangement between them 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 clarifies the degree of coordination required between the joint controllers. They have to work together to ensure that the data subject does not miss out on any information as a result of the information each controller provides. It also ensures that all joint controllers within

[20] See section 2.1.6.

the meaning of Art. 83 (5) (b) GDPR are liable for compliance with this requirement. They are liable to sanctions if incomplete information is provided or information is not provided at all.

2.3.25 Taking the risks to children into account in the data protection impact assessment

In order to take account in every data protection impact assessment of the fact that personal data of children is being processed, Art. 35 (1) and (7) GDPR should be amended as follows:

> "(1) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, *in particular the processing of personal data of a child,* is likely to result in a high risk to the rights and freedoms of natural persons, 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 *that pays particular attention to such risks and freedoms if the processing involves personal data of a child*; 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*, particularly of children*."

The addition is a logical extension of the proposed amendments in Art. 21, 25 and 34 GDPR and also encompasses the data protection impact assessment. Here too, the aim is to strengthen the rights and freedoms of children by explicitly referring to children in the normative text and thereby ensuring that controllers respect their specific rights and freedoms. The changes to Art. 35 GDPR go further than mere clarification and establish specific obligations to pay particular attention to children when carrying out a data protection impact assessment. These obligations extend both to the risk analysis and to the specification of safeguards.

2.3.26 New tasks for the European Data Protection Board

The proposed changes to the General Data Protection Regulation confer three additional responsibilities upon the European Data Protection Board.[21] These should be included in the list of the Board's tasks in Art. 70 (1) GDPR. The tasks of defining more precisely the duty to ensure data protection by design in accordance with Art. 25 (1) GDPR and the duty to provide

[21] See section 2.2.5.

data protection by default in accordance with Art. 25 (2) GDPR can be combined into one task. The provision should be amended to include a point (ea) and a point (fa):

> "*(ea) provide guidance, recommendations and* best practices *in accordance with point (e) of this paragraph to define in more detail the interoperable formats for a transfer of data in accordance with Article 20 (1) and (2);"*
>
> *"(fa) provide guidance, recommendations and* best practices *in accordance with point (e) of this paragraph to provide a more detailed technical and area-specific definition of the duty of data protection by design in accordance with Article 25 (1) and through data protection by default in accordance with Article 25 (2);"*

These additions create consistency within the Regulation and ensure that the Board also provides additional clarifications in relation to the proposed changes and provides recommendations on specific design.

2.3.27 Statistics on sanctions

To support the implementation of the General Data Protection Regulation, to create transparency about action taken by the supervisory authorities and to help ensure that administrative fines are imposed consistently, the supervisory authorities should publish statistics on these processes twice a year. An additional paragraph 10 should be added to Art. 83 GDPR for this:

> *"(10) Each supervisory authority shall publish statistics on action taken under this provision twice a year, in each case within one month of the end of each half year."*

This new paragraph will increase transparency significantly. Not only will consumers be able to see that data protection legislation is being implemented effectively, but a controller will be better able to anticipate how the extremely broad provisions for imposing fines set out in the General Data Protection Regulation are applied in practice.

[…]

6. Summary

The innovations of the General Data Protection Regulation 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. This report has made recommendations to this end which can be taken advantage of in the context of the evaluation of the GDPR in 2020 in order to constructively advance the regulation. While drafting these recommendations, the view of the consumer took centre stage. Strengthening the position of the consumer and to reduce asymmetry between controller and data subject is in line with the pronounced goal of the GDPR to have the processing of personal

data serve mankind[22] and to safeguard the fundamental rights and freedoms of data subjects while and contribute to the well-being of natural persons – indeed with respect to the rights of the controllers.[23]

This report has demonstrated that even small changes in the wording of the provisions of the regulation can have a significant effect in strengthening the position of consumers and to prevent aberration. In some places however, extensive specification and clarification through guidelines issued by the European Data Protection Board is irremissible.

The discourse about data protection law must not stop with the evaluation of the GDPR in 2020. The fundamental principles of data protection in Europe have remained essentially unchanged since the 1970s. The technological innovations that have taken place since then as well as the foreseeable technological evaluation necessitate that we question these fundamental principles and that we evolve them.

22 Recital 4(1) GDPR.
23 Recitals 2 and 4 GDPR.