



Attorneys at Law
External Data Protection Officers

Bonn, November 20th 2024

Position Paper

Public consultation on Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0

We welcome the initiative of the EDPB to provide controllers with guidelines on the processing of personal data based on Article 6(1)(f) GDPR, in order to assist them in their application of this provision. We believe that the guidelines can help controllers to assess and implement the criteria set out in Article 6(1)(f) GDPR that they must meet in order to lawfully process personal data on the basis of a legitimate interest. In our view, the current version of the guidelines summarizes some important topics well and addresses important legal issues that arise for controllers when processing personal data on the basis of Article 6(1)(f) GDPR. Nevertheless, we think that the guidelines could be more precise at some points. We therefore appreciate the opportunity to comment on them.

In our statement, we focus on data processing by non-public bodies within the scope of the GDPR and on some – in our view – practice-relevant aspects to be highlighted. Our comments are structured in line with the guidelines, paired with the corresponding paragraph.

We consent to the publication of our statement.

Scheja & Partners GmbH & Co. KG

Adenauerallee 136
53113 Bonn, Germany
T +49 228 227226-0
F +49 228 227226-26
www.scheja-partners.de

Head office: Bonn; Registration court: Amtsgericht (local court) Bonn; Commercial register no.: HRA 10220; VAT ID no.: DE286820627

Personally liable partner:

Scheja & Partners Management GmbH; Head office: Bonn; Registration court: Amtsgericht (local court) Bonn; Commercial register no.: HRB 28299; Managing directors (each with the sole power of representation): RA Jens-Martin-Heidemann, LL.M., RA Boris Reibach, LL.M., RA Florian Reichert, RA Dr. Gregor Scheja

Jenny Strauß, LL.M. (Information Technology Law)

jenny.strauss@scheja-partners.de
Attorney at Law

Kristina Radtke, LL.M. (Information Technology Law)

kristina.radtke@scheja-partners.de
Attorney at Law

Certified Specialist Lawyer (Information Technology Law)

Markus Alexandru

markus.alexandru@scheja-partners.de
Attorney at Law

Table of contents

| | |
|--|---|
| A. Elements to be taken into account when assessing the applicability of the Article 6(1)(f) GDPR as a legal basis, paragraph 12 | 3 |
| B. Elements to be taken into account when assessing the applicability of Article 6(1)(f) GDPR as a legal basis, paragraph 13 | 3 |
| C. "Legitimate" nature of the interest pursued by the controller or by a third party, paragraph 17.. | 4 |
| D. Further consequences of the processing, paragraph 45..... | 5 |
| E. Further consequences of the processing, paragraph 46..... | 5 |
| F. Further consequences of the processing, paragraph 47 and Reasonable expectations of the data subject, paragraph 52..... | 6 |
| G. Reasonable expectations of the data subject, paragraph 54..... | 6 |
| H. Transparency and information to be provided to data subjects, paragraph 67 and 68 and Right of access, paragraph 70 | 6 |

A. Elements to be taken into account when assessing the applicability of the Article 6(1)(f) GDPR as a legal basis, paragraph 12

If a controller has appointed a data protection officer, it should ensure that the data protection officer is involved at an early stage, in his or her function as an advisor, when assessing whether Article 6(1)(f) GDPR can be used as a legal basis for the intended processing of personal data. The guidelines refer here to Article 38(1) GDPR.

Legal Assessment:

Even though the identification of interests and, in particular, the balancing test itself is regularly a challenging task, data protection officers are typically not involved in practice. This may be due to the wording of Article 38(1) GDPR that speaks only generally of an early involvement of the data protection officer in all issues which relate to the protection of personal data. Also the tasks of the data protection officer in Article 39(1) GDPR and Recital 97 GDPR are described in general terms only.

We welcome that the guidelines explicitly call for the involvement of a designated data protection officer. The involvement of the data protection officer ensures that the data processing actually fulfills the requirements of Article 6(1)(f) GDPR. Specifically, it will improve the quality and validity of any balancing test. The early involvement of the data protection officer should therefore be emphasized with regards to its great practical relevance.

B. Elements to be taken into account when assessing the applicability of Article 6(1)(f) GDPR as a legal basis, paragraph 13

Recourse to Article 6(1)(f) GDPR should only be possible if the intended processing of personal data is strictly necessary for pursuing a legitimate interest. In this context, the guidelines refer to the recent SCHUFA judgment of the European Court of Justice (hereinafter: CJEU) (CJEU, judgment of 7 December 2023, Joined Cases C-26/22 and C-64/22, SCHUFA Holding (Libération de reliquat de dette) (ECLI:EU:C:2023:958)).

Legal Assessment:

The wording "strictly" goes beyond the wording of Article 6(1)(f) GDPR, which only speaks of "necessary" processing. According to Recital 47(6) and Recital 49(1) GDPR, on the other hand, the processing of personal data can be based on a legitimate interest if it is "strictly necessary" for the purposes of preventing fraud or for the purposes of ensuring network and information security. Likewise, the SCHUFA decision of December 7, 2023, paragraph 88, indicates that the CJEU understands the provision in the way that the processing must be "strictly necessary" for the purposes pursued.

It remains vague what is meant by the restriction to "strictly" necessary processing; should a "necessary" processing no longer be sufficient when evaluating the purposes of the processing, i.e. are there increased requirements for the necessity of the processing? It also remains unclear how a "necessary" processing would differ from a "strictly necessary" processing. This applies all the more since the

guidelines refer to the SCHUFA decision of the CJEU, although it is not clear to what extent it adopts the CJEU's interpretation: Does every processing based on Article 6(1)(f) GDPR have to be "strictly necessary" or does it only refer to processings that pursue the purposes of preventing fraud or ensuring network and information security? If the intention is to impose additional requirements on a processing to be "necessary", the scope of Article 6(1)(f) GDPR would, at least with respect to its wording, be too narrowly restricted. A clarifying explanation should be included in the guidelines.

C. "Legitimate" nature of the interest pursued by the controller or by a third party, paragraph 17

According to the guidelines, several cumulative criteria should be taken into account when determining whether an interest is legitimate. An interest also ought to be "real and present, and not speculative". The CJEU has stated in this regard that an interest "must be present and effective as at the date of the data processing and must not be hypothetical at that date." (CJEU, judgment of 11 December 2019, Case C-708/18, Asociația de Proprietari bloc M5A-ScaraA (ECLI:EU:C:2019:1064), paragraph 44).

Legal Assessment:

However, in our opinion, this falls short. Firstly, it is not explained when an interest is to be categorized as hypothetical at all. Interests that do not appear fully unreasonable are not speculative or hypothetical, but may lie in the future and thus not be "present" in the narrow sense. When a website is accessed, for example, the visitor's IP address is stored for a short period of time so that any cyberattacks can be investigated if necessary. The interest in investigating a cyberattack is not present the moment the website is accessed, but it does become present in the event of an actual attack. In our view, this cannot mean this interest is not present, so that the IP address could not be stored initially on grounds of Article 6(1)(f) GDPR. In addition, and for clarification, it should be mentioned in the guidelines that the purpose of preventing fraud is always "real and present, and not speculative" and therefore qualifies as a legitimate interest under Article 6(1)(f) GDPR.

Another example: A controller collects customers' data in the context of concluding contracts so that it can later send advertising to customers.. At this point, he or she has not yet decided on what specific advertising to send to the customers. All that is certain at this point is that he or she wants to advertise products at a later date. Strictly speaking, there is no "present" interest in the data processing upon conclusion of a contract if the controller is planning to roll out the advertising only later, for example, after designing a specific campaign and selecting suitable customers for it. Here, too, the interest is not "speculative", but already specifically outlined, even though lying in the future.

For practice, it would be helpful to have an explanation of what degree of certainty is required for a purpose in the future to be included in the balancing test.

D. Further consequences of the processing, paragraph 45

Paragraph 32 lists "Further consequences of the processing" that should be identified and taken into account in the balancing test when assessing the possible impact of an intended processing of personal data on data subjects. According to paragraph 45, this may also include "Potential future decisions or actions by third parties that may be based on the personal data to be processed by the controller".

Legal Assessment:

This example should be restricted. It is very far-reaching to demand from controllers, when examining a balancing test, to assess and include all possible actions of any third party. This requirement is impractical and urgently needs to be restricted, if not removed. Any third party is responsible for its own data processing and thus must be able to provide a legal basis. This is clearly stated in the definition of a "third party" in Article 4 No. 10 GDPR. The obligation to anticipate any possible actions of third parties must not be part of the responsibility of the first controller and should therefore not be examined here. On the other hand, if the example intends to refer to cases in which those responsible can already foresee that the personal data they process will be used by other recipients for their own processing (see, for example, credit reference agencies) and who they are, this should be pointed out in the guidelines.

E. Further consequences of the processing, paragraph 46

When assessing the impact of an intended processing of personal data, controllers should consider any potential emotional impact for data subjects, in addition to specific consequences that can be foreseen. According to the guidelines, this should be required because continuous monitoring of their online activities could make data subjects feel as if an essential part of their private lives was constantly being monitored.

Legal Assessment:

Emotional effects are always a subjective matter and thus difficult for controllers to assess. At least based on the wording, emotional aspects are not taken into account in any other data processing requirement of the GDPR.

The monitoring of online activities is a phenomenon that data subjects expect as a side effect of using online services. Furthermore, the disclosure of information for the best possible online experience is also generally accepted. Proof of these points can also be seen in the phenomenon of consent fatigue. It therefore seems rather unlikely for online users to assume that online monitoring per se will lead to continuous surveillance of the private lives of data subjects.

This should be seen in the context of paragraph 54. In terms of when data subjects' expectations are reasonable in a balancing test and contrary to the above, it is explained that a person who has "only signed up for a newsletter" on a website has different reasonable expectations than, for example, a person who is already in a business relationship with the operator of the website or the controller. Based on their previous experience using online services, it can be assumed data subjects are aware of the fact

that data controllers usually offer newsletter registrations for obtaining personal data that is highly valuable to them, especially for advertising purposes.

F. Further consequences of the processing, paragraph 47 and Reasonable expectations of the data subject, paragraph 52

The possible impact of the processing of personal data on the rights, freedoms and interests of data subjects should be determined on the basis of an objectified standard. In particular, data subjects should not be "unduly surprised" by the actual processing of their personal data or its consequences.

Legal Assessment:

Certain subjective criteria (reasonable expectations) should thus be considered from an objective point of view. This should be clarified, preferably along with additional use cases, as to how this could be done in practice. It should also be explained when a data subject can be considered "unduly surprised".

G. Reasonable expectations of the data subject, paragraph 54

Paragraph 54 contains a list of factors that can, according to the guidelines, be used to assess what the reasonable expectations are in a given context. These factors include "characteristics of the relationship with the data subject or of the service" as well as "characteristics of the 'average' data subjects whose personal data is to be processed".

Legal Assessment:

The guidelines, as we think, correctly clarify that a close relationship, of which the data subject is aware, between a controller and other companies in a corporate group may lead to reasonable expectations that personal data will be passed on within the group and that any assessment should be based on the degree of general awareness of the relevant corporate structures. Reference should be made here to Recital 48 GDPR, according to which data processing within company groups can, in principle, constitute a legitimate interest within the meaning of Article 6(1)(f) GDPR.

H. Transparency and information to be provided to data subjects, paragraph 67 and 68 and Right of access, paragraph 70

These sections of the guidelines state, on the one hand, that the specific legitimate interests of a controller should be clearly identified and communicated to the data subject, regarding Article 13(1)(d) and Article 14(2)(b) GDPR (paragraph 67). On the other hand, a controller may provide the data subject with information on the balancing test in advance of any collection of personal data, including in a "layered privacy statement/notice". Information provided to data subjects should always include a note that data subjects could receive information on the balancing test upon request. The mere fulfillment of information obligations under Art. 12 to Art. 14 GDPR should not be sufficient in itself to establish

reasonable expectations. This is a consequence of the accountability principle in Article 5(2) GDPR, according to the guidelines. Furthermore, Article 15(1) GDPR would not explicitly require information on the legal basis for the processing of personal data to be provided.

Legal Assessment:

There is no provision in the GDPR containing an obligation on the controller to provide full information on the specific balancing test, nor a corresponding right of the data subject. The interpretation in paragraph 68 goes too far.

The following aspects should be mentioned to emphasize that the accountability principle does not imply any information obligations on the part of the controller: Article 5(2) GDPR mentions the ability to demonstrate compliance with the principles of Article 5(1) GDPR – including the principle of lawfulness. It does not mention any further information requirements. Consequently, the controller must be able to demonstrate the lawfulness of the data processing. However, this does not include the obligation to provide evidence to data subjects. Rather, accountability refers to the obligation to provide evidence to courts or supervisory authorities, if necessary.

The principle of transparency in Article 5(1)(a) GDPR is specified by information obligations in Articles 12, 13(1)(d) and 14(2)(b) GDPR. Based on their wording, these provisions do not establish a right of the data subject to receive full information on the balancing test. Instead, the information to be provided to the data subject is limited to communicating the interests pursued by the controller. The wording is very clear here. This is an argument against an unintended legislative loophole, which would have to exist for an analogous application of Article 5(2) GDPR.

The justification that the data subject needs this information on the balancing test in order to be able to assess its legality and, if necessary, to assert further rights, also leaves out the data subject's right to object under Art. 21 GDPR. This right to object specifically allows the data subject to present special personal reasons that the controller could not normally be aware of. This should then initiate a new balancing test. It is not necessary for the data subject to be informed about the details taken into consideration by the controller in order to assert the right to object.

It also cannot be inferred from Article 15 GDPR either that the data subject must be provided with information on the balancing test. In addition, in many cases, trade and business secrets may also become relevant in the balancing test (e.g. information on risk-mitigating measures such as special pseudonymization procedures). Article 15 GDPR must be brought into line with the rights of the controller and Art. 16 of the Charter of Fundamental Rights ("Freedom to conduct a business"). This stands in the way of a (general) obligation for a controller to provide information on the balancing test, because confidential internal information may be included there and could therefore be released to groups of people who should not have this knowledge.

An obligation for the controller to disclose full information on the balancing test to data subjects is too far-reaching as there is no legal basis for having to do so. We therefore suggest leaving it only as a recommendation that controllers may voluntarily disclose such information upon request. Disclosure of information on the balancing test should neither be presented as a right of the data subject nor as an obligation of the controller.

Scheja & Partners GmbH & Co. KG

Adenauerallee 136
53113 Bonn, Germany
T +49 228 227226-0
F +49 228 227226-26
www.scheja-partners.de

Head office: Bonn; Registration court: Amtsgericht (local court) Bonn; Commercial register no.: HRA 10220; VAT ID no.: DE286820627

Personally liable partner:

Scheja & Partners Management GmbH; Head office: Bonn; Registration court: Amtsgericht (local court) Bonn; Commercial register no.: HRB 28299; Managing directors (each with the sole power of representation): RA Jens-Martin-Heidemann, LL.M., RA Boris Reibach, LL.M., RA Florian Reichert, RA Dr. Gregor Scheja

Jenny Strauß, LL.M. (Information Technology Law)

jenny.strauss@scheja-partners.de
Attorney at Law

Kristina Radtke, LL.M. (Information Technology Law)

kristina.radtke@scheja-partners.de
Attorney at Law
Certified Specialist Lawyer (Information Technology Law)

Markus Alexandru

markus.alexandru@scheja-partners.de
Attorney at Law