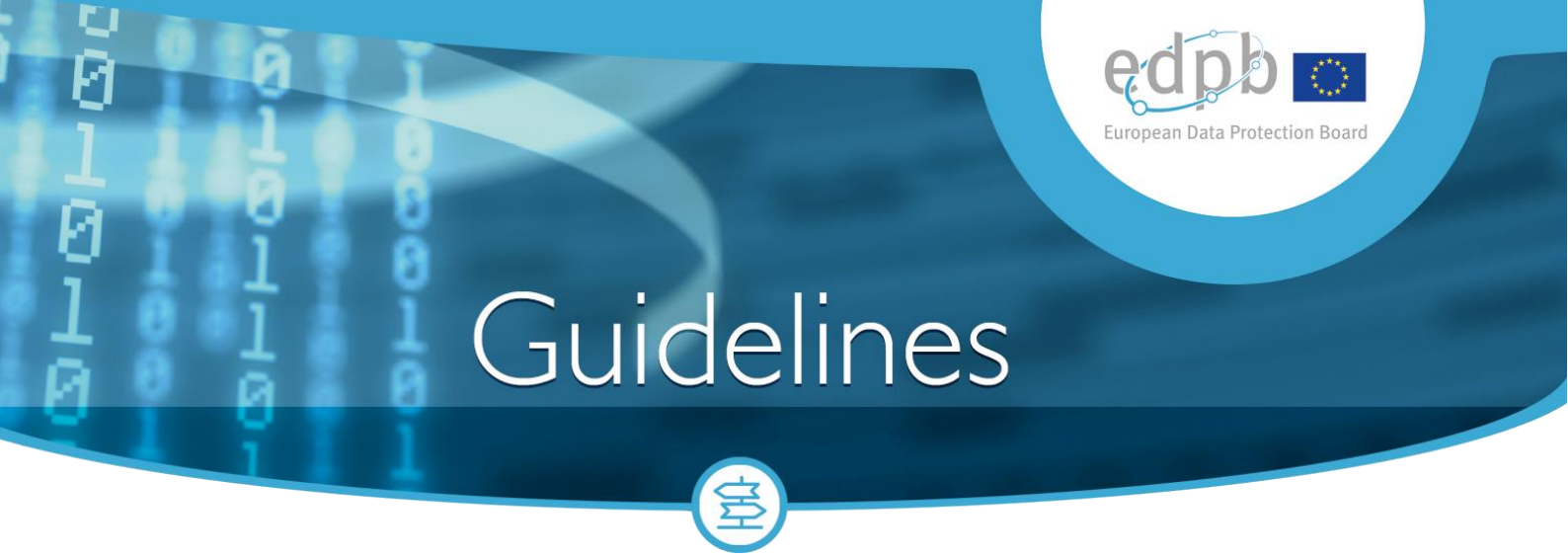

Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR

Version 1.0

Adopted on 8 October 2024

EXECUTIVE SUMMARY

These guidelines analyse the criteria set down in Article 6(1)(f) GDPR that controllers must meet to lawfully engage in the processing of personal data that is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party".

Article 6(1)(f) GDPR is one of the six legal bases for the lawful processing of personal data envisaged by the GDPR. Article 6(1)(f) GDPR should neither be treated as a "last resort" for rare or unexpected situations where other legal bases are deemed not to apply nor should it be automatically chosen or its use unduly extended on the basis of a perception that Article 6(1)(f) GDPR is less constraining than other legal bases.

For processing to be based on Article 6(1)(f) GDPR, three cumulative conditions must be fulfilled:

- First, the pursuit of a legitimate interest by the controller or by a third party;
- Second, the need to process personal data for the purposes of the legitimate interest(s) pursued; and
- Third, the interests or fundamental freedoms and rights of the concerned data subjects do not take precedence over the legitimate interest(s) of the controller or of a third party.

In order to determine whether a given processing of personal data may be based on Article 6(1)(f) GDPR, controllers should carefully assess and document whether these three cumulative conditions are met. This assessment should be done before carrying out the relevant processing operations.

With regard to the condition relating to the pursuit of a legitimate interest, not all interests of the controller or a third party may be deemed legitimate; only those interests that are lawful, precisely articulated and present may be validly invoked to rely on Article 6(1)(f) GDPR as a legal basis. It is also the responsibility of the controller to inform the data subject of the legitimate interests pursued where that processing is based on Article 6(1)(f) GDPR.

With regard to the condition that the processing of personal data be necessary for the purposes of the legitimate interests pursued, it should be ascertained whether the legitimate interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects, also taking into account the principles enshrined in Article 5(1) GDPR. If such other means exist, the processing may not be based on Article 6(1)(f) GDPR.

With regard to the condition that the interests or fundamental rights and freedoms of the person concerned by the data processing do not take precedence over the legitimate interests of the controller or of a third party, that condition entails a balancing of the opposing rights and interests at issue which depends in principle on the specific circumstances of the relevant processing. The processing may take place only if the outcome of this balancing exercise is that the legitimate interests being pursued are not overridden by the data subjects' interests, rights and freedoms.

A proper Article 6(1)(f) GDPR assessment is not a straightforward exercise. Rather, the assessment — and in particular the balancing of opposing interests and rights — requires full consideration of a number of factors, such as the nature and source of the relevant legitimate interest(s), the impact of the processing on the data subject and their reasonable expectations about the processing, and the existence of additional safeguards which could limit undue impact on the data subject. The present guidelines provide guidance on how such an assessment should be carried out in practice, including in a number of specific contexts (e.g., fraud prevention, direct marketing, information security, etc.) where this legal basis may be considered.

The guidelines also explain the relationship that exists between Article 6(1)(f) GDPR and a number of data subject rights under the GDPR.

Contents

The European Data Protection Board

Having regard to Article 70(1)(e) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES:

I. INTRODUCTION

1. Pursuant to Article 8 of the Charter of Fundamental Rights of the European Union (hereinafter "Charter"), personal data must be processed fairly for specified purposes and on the basis of a legitimate basis laid down by law. Article 6(1) GDPR provides that processing shall be lawful only if and to the extent that at least one of the six legal bases set out in Article 6(1)(a) to (f) GDPR applies. Consequently, before a controller starts processing personal data, it must identify the applicable legal basis and ensure that the requirements of at least one of the legal bases in Article 6(1) GDPR are fulfilled. In this regard, it should be recalled that the GDPR does not establish any hierarchy between the different legal bases laid down in Article 6(1).[2]

2. Article 6(1)(f) GDPR provides a legal basis for the processing of personal data to the extent that "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".

3. In line with the accountability principle and except where provided for by law, the determination of the legal basis for a specific processing of personal data falls within the responsibility of the controller. The main purpose of these guidelines is therefore to assist controllers in assessing whether Article 6(1)(f) GDPR may be invoked as a valid legal basis for their processing of personal data.

4. Moreover, the European Data Protection Board (hereafter "EDPB") recalls that the legal basis for a given personal data processing needs to be considered in the context of the GDPR as a whole, the objectives set out in Article 1 GDPR, and alongside the controllers' duty to process personal data in compliance with the data protection principles enshrined in Article 5 GDPR, such as the "data minimisation" principle.[3] In this respect, it should also be noted that, "in accordance with Article 5 GDPR, the controller bears the burden of proving that data are collected, inter alia, for specified, explicit and legitimate purposes and that they are processed lawfully, fairly and in a transparent manner in relation to the data subject".[4]

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".
[2] See e.g. Opinion of Advocate General Szpunar in Case C-394/23, *Mousse* (ECLI:EU:C:2024:610), paras. 28-29.
[3] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 109.
[4] Ibid., para. 95. See further EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects (version 2.0, 8 October 2019), paras. 11-12.

5. Article 7(f) of Directive 95/46/EC included a legal basis analogous to that in Article 6(1)(f) GDPR, as it provided that personal data processing may be considered lawful if necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. In that sense, this legal basis is not a novelty introduced by the GDPR. Therefore, the present guidelines build upon and update Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC of the Article 29 Data Protection Working Party (hereinafter "WP29").[5] However, it is important to stress that with the adoption of the GDPR, the EU data protection legal framework has evolved. In particular, the GDPR has strengthened the position of data subjects, the exercise of data subject rights and the obligations of controllers, including by codifying recommendations and positions expressed by the WP29. Furthermore, it should be noted that Article 6(1)(f) GDPR has been interpreted in several rulings of the Court of Justice of the European Union (hereinafter "CJEU") – which have been issued after the adoption of the above-mentioned WP29 Opinion – which must be taken into account when assessing this legal basis.

6. For processing to be based on the legitimate interest legal basis, three cumulative conditions must be fulfilled:[6]

   - First, the pursuit of a legitimate interest by the controller or by a third party;
   - Second, the need to process personal data for the purposes of the legitimate interest(s) pursued (i.e., the processing of personal data must be "necessary" for those purposes); and
   - Third, the interests or fundamental freedoms and rights of the concerned data subjects do not take precedence over the legitimate interest(s) of the controller or of a third party.

7. With respect to the third condition, the controller must weigh its legitimate interest(s) or those of a third party and the "interests or fundamental rights and freedoms of data subjects". This "balancing exercise" between the fundamental rights, freedoms and interests at stake must be performed for each processing to be based on legitimate interest as a legal basis,[7] and must be done before carrying out the relevant processing operation(s).

8. It should also be highlighted that the second indent of Article 6(1) GDPR provides that the legal basis in Article 6(1)(f) shall not apply to processing carried out by public authorities in the performance of their tasks.

9. Article 6(1)(f) GDPR cannot be considered as a legal basis "by default". On the contrary, before relying on such a legal basis, the controller should perform a careful assessment of the planned processing and follow a specific methodology. The open-ended nature of Article 6(1)(f) GDPR[8] does not necessarily mean that this legal basis should be seen as one that can only be used as a "last resort" in rare and unforeseen situations, or that Article 6(1)(f) should be seen as a last option if no other legal bases apply. Nor should Article 6(1)(f) be seen as a preferred option by controllers and its use should not be unduly extended to circumvent specific legal requirements or because it would be considered as less constraining than the other legal bases in Article 6(1) GDPR. In other words, Article 6(1)(f) should not be considered as an "open door" to legitimise all data processing activities which do not fall under any of the other legal bases in

[5] WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217, Adopted on 9 April 2014).
[6] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 106; CJEU, judgment of 11 December 2019, Case C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), para. 40.
[7] CJEU, judgment of 4 May 2017, Case C-13/16, *Rīgas satiksme* (ECLI:EU:C:2017:336), para. 28.
[8] See Opinion of Advocate General Bobek in Case C-40/17, *Fashion ID* (EU:C:2018:1039), para. 122.

Article 6(1) GDPR. Rather, it should be recalled that Article 6(1)(f), like each of the legal bases set out in Article 6(1) GDPR, must be interpreted restrictively.[9]

10. It should be highlighted that when personal data are processed for different purposes the processing for each of those purposes must fall within one of the cases provided for in Article 6(1) GDPR.[10] The purpose and the legal basis of such processing must be identified from the outset of the processing and must be communicated to the data subject (see Articles 13(1)(c) and 14(1)(c) GDPR). Therefore, processing relying on Article 6(1)(f) GDPR should not encompass several purposes without assessing the validity of the legal basis for each of them.

11. These guidelines are without prejudice to Directive 2002/58/EC ("ePrivacy Directive"), which governs the role of consent as a legal basis in the field of electronic communications.[11]

II. ELEMENTS TO BE TAKEN INTO ACCOUNT WHEN ASSESSING THE APPLICABLITY OF ARTICLE 6(1)(F) GDPR AS A LEGAL BASIS

12. In order to determine whether a given processing of personal data may be based on Article 6(1)(f) GDPR, controllers must carefully assess whether the three cumulative conditions listed above can be met so as to ensure that the processing is lawful. [12] This assessment should follow the three-step process outlined below, although in some circumstances the examinations of the second and third conditions may merge in so far as the assessment of whether the legitimate interests pursued by the processing of personal data cannot reasonably be achieved by less intrusive means requires a balancing of the opposing rights and interests at issue.[13] The assessment should be made at the outset of the processing, with the involvement of the Data Protection Officer (DPO) (if designated),[14] and should be documented by the controller in line with the accountability principle set out in Article 5(2) GDPR.

13. It should be stressed from the outset that the existence and identification of a legitimate interest pursued by the controller or a third party is not in itself sufficient to rely on Article 6(1)(f) GDPR as a legal basis.[15] The controller may rely on this legal basis only if it has also assessed and concluded that the envisaged processing is strictly necessary for pursuing such a legitimate interest and that the interests or

[9] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), paras. 92-93 (stating: "In the absence of such consent, or where that consent is not freely given, specific, informed and unambiguous, within the meaning of Article 4(11) of the GDPR, such processing is nevertheless justified where it meets one of the requirements of necessity mentioned in points (b) to (f) of the first subparagraph of Article 6(1) of that regulation. In that context, the justifications provided for in that latter provision, in so far as they allow the processing of personal data carried out in the absence of the data subject's consent to be made lawful, must be interpreted restrictively (see, to that effect, judgment of 24 February 2022, Valsts ieņēmumu dienests (Processing of personal data for tax purposes), C-175/20, EU:C:2022:124, paragraph 73 and the case-law cited)").

[10] Ibid., para. 90.

[11] See EDPB, Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, paras. 14-15; EDPB, Guidelines 8/2020 on the targeting of social media users, paras. 71-72; EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities.

[12] CJEU, judgment of 11 December 2019, Case C-708/18, *Asociația de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), para. 40; CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 106; 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), para. 75.

[13] 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), para. 92.

[14] See Article 38(1) GDPR.

[15] 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), para. 75.

fundamental rights and freedoms of the person(s) concerned by the data processing do not take precedence over the legitimate interest pursued,[16] as explained in further details below.

A. 1st step: Pursuit of a legitimate interest by the controller or by a third party

1. "Legitimate" nature of the interest pursued by the controller or by a third party

14. The concept of "interest" is closely related to, but distinct from, the concept of "purpose" mentioned, for instance, in Article 5(1)(b) GDPR. A "purpose" is the specific reason why the data are processed: the aim or intention of the data processing. An "interest", on the other hand, is the broader stake or benefit that a controller or third party may have in engaging in a specific processing activity. For example, a controller may have an *interest* in promoting its products, whereas this interest may be advanced by processing personal data for direct marketing *purposes*.

15. Not all interests enable a controller to invoke Article 6(1)(f) GDPR as a legal basis. The CJEU has made clear that the first step to be taken when assessing whether Article 6(1)(f) may be invoked as a valid legal basis is to check whether the interest pursued by the controller may be considered as being "*legitimate*".[17] In other words, the controller needs to conclude that the interest to be pursued is "legitimate" *before* moving on to the second step of the three-step assessment process to be performed under Article 6(1)(f) (i.e., before assessing whether the processing of personal data is necessary for pursuing the legitimate interest in question).

16. There is no exhaustive list of interests that may be considered as being legitimate. In the absence of a definition of that concept in the GDPR, a wide range of interests is, in principle, capable of being regarded as legitimate.[18] Both the GDPR[19] and the CJEU have expressly recognised several interests as being legitimate, such as having access to information online,[20] ensuring the continued functioning of publicly accessible websites,[21] obtaining the personal information of a person who damaged someone's property

[16] Ibid.
[17] Ibid.
[18] 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), para. 76.
[19] The GDPR mentions, by way of illustration, that the processing of personal data for the purposes of preventing fraud or for direct marketing purposes, as well as the processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, may be regarded as carried out for a legitimate interest (see Recitals 47 and 49 GDPR). See further Opinion of Advocate General Rantos, in Case C-252/21, *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)* (ECLI:EU:C:2022:704), para. 84.
[20] CJEU, judgment of 13 May 2014, Case C-131/12, *Google Spain and Google* (EU:C:2014:317), para. 81; CJEU, judgment of 24 September 2019, Case C-136/17, *GC and Others (De-referencing of sensitive data)* (EU:C:2019:773), para. 53.
[21] CJEU, judgment of 19 October 2016, Case C-582/14, *Breyer* (EU:C:2016:779), para. 60.

in order to sue that person for damages,[22] protecting the property, health and life of the co-owners of a building,[23] product improvement,[24] and assessing the creditworthiness of individuals,[25] among others.

17. An interest may be regarded as "legitimate" if the following cumulative criteria are met:[26]

- The interest is lawful, i.e., not contrary to EU or Member State law.[27] While the concept of "legitimate interest" within the meaning of Article 6(1)(f) GDPR is not limited to interests enshrined in and determined by law, it requires that the alleged legitimate interest be lawful.[28]

- The interest is clearly and precisely articulated. The perimeter of the legitimate interest pursued must be clearly identified in order to ensure that it will be properly balanced against the interests or fundamental rights and freedoms of the data subject.

- The interest is real and present, and not speculative. As clarified by the CJEU, the legitimate interest must be present and effective at the date of the data processing and must not be hypothetical at that date.[29]

18. Recital 47 of the GDPR makes clear that a "legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller". However, this is just an example of a possible indicator that an interest may be qualified as "legitimate", and it is without prejudice to the controller's obligation to assess and ensure that all of the three cumulative conditions for relying on Article 6(1)(f) GDPR as a legal basis are met for the envisaged processing operations.

Example 1:

A European company selling electronic cigarettes and refill containers wants to promote its products by sending promotional emails to its customers living in a certain area within the EU. To do so, it needs to collect—and hence process—the personal data (e.g., email address and names) of such individuals. Even though processing of personal data for direct marketing purposes may often be regarded as carried out for a legitimate interest, in these specific circumstances the interest may not be qualified as being "legitimate" because commercial communications in Information Society services with the aim or with the direct or

[22] CJEU, judgment of 4 May 2017, Case C-13/16, *Rīgas satiksme* (EU:C:2017:336), para. 29; CJEU, judgment of 17 June 2021, Case C-597/19, *M.I.C.M.* (EU:C:2021:492), para. 108.

[23] CJEU, judgment of 11 December 2019, Case C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA* (EU:C:2019:1064), para. 42.

[24] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 122 (the Court noted in this regard that "it cannot be ruled out from the outset that the controller's interest in improving the product or service with a view to making it more efficient and thus more attractive can constitute a legitimate interest").

[25] 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), para. 83.

[26] For an analogous set of criteria, see WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217, Adopted on 9 April 2014), pp. 24-25.

[27] CJEU, judgment of 4 October 2024, Case C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), para 49.

[28] Ibid, para. 40. The CJEU held in the same judgment that a commercial interest of the controller could constitute a legitimate interest, within the meaning of Article 6(1)(f) GDPR, provided that it is not contrary to the law. The existence of such an interest and its lawfulness should however be assessed on a case-by-case basis (see para. 49).

[29] CJEU, judgment of 11 December 2019, Case C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), para. 44.

indirect effect of promoting electronic cigarettes and refill containers are generally prohibited under the EU Tobacco Products Directive and the national rules transposing it.[30]

Nb: this example solely aims at illustrating a non-legitimate interest and is without prejudice to the compliance of the processing at stake with other elements of Article 6(1)(f) or any other provision of the GDPR or other relevant laws.

Example 2:

A "neighbourhood watch" organisation has decided that, "for the greater good of society", it wishes to install a video surveillance system in a given neighbourhood to monitor possible criminal activities in the area. While the protection of property, health and life may in some circumstances be characterised as a legitimate interest, the interest as expressed by the controller with reference to the processing which is occurring in the present case is very vague, as it is phrased in general terms and does not refer to any specific safety issues. Thus, it is not sufficiently articulated in order to assess its legitimacy and eventually pursue the rest of the three-step assessment process under Article 6(1)(f) GDPR.

Nb: this example solely aims at illustrating the absence of a sufficiently clear interest and is without prejudice to the compliance of the processing at stake with other elements of Article 6(1)(f) or other provisions of the GDPR or other relevant laws.

Example 3:

A newspaper envisages to create a database consisting of former subscribers who have not renewed their subscription in order to be able to retrieve such contacts in the event of a launch of a new magazine, as part of their client relationship. At the time of the creation of the database, the newspaper has no concrete plan to develop and launch a new magazine.

In the present case, the interest pursued by the controller through the population of its database – a processing falling under the scope of the GDPR – cannot be considered as real and present, as the launch of a new magazine is only hypothetical at this stage. Therefore, the interest pursued by the controller may not be considered "legitimate".

Nb: this example solely aims at illustrating the absence of a real and present interest and is without prejudice to the compliance of the processing at stake with other elements of Article 6(1)(f) or other provisions of the GDPR or other relevant laws.

2. Interest pursued by the controller or a third party

19. Article 6(1)(f) GDPR refers to the legitimate interests pursued "by the controller or by a third party". As a general rule, the interest pursued by the controller should be related to the actual activities of the controller. For example, the CJEU found that, even though the sharing of information with law-enforcement agencies in order to prevent, detect and prosecute criminal offences is a legitimate interest as such, it is not capable, in principle, of constituting a legitimate interest pursued by a controller whose

[30] See Art. 20(5)(a) of Directive 2014/40/EU of the European Parliament and the Council of 3 April 2014 on the approximation of the laws, regulations and administrative provisions of the Member States concerning the manufacture, presentation and sale of tobacco and related products and repealing Directive 2001/37/EC.

activity is essentially economic and commercial in nature, as it is unrelated to its economic and commercial activity.[31]

20. However, the reference to an interest pursued by "a third party" in the wording of Article 6(1)(f) GDPR indicates that the interest(s) of one or more specific third parties may be legitimately pursued within the meaning of Article 6(1)(f),[32] and may thus be balanced against the interests or fundamental rights and freedoms of the data subject.[33] In some cases, the processing of personal data may serve to pursue simultaneously the legitimate interests of the controller and of a third party.[34] The legitimate nature of the interest of a third party must be assessed following the same criteria which apply with respect to the controller's own interests.

Example 4:

A taxi driver had parked his vehicle on the side of the road. As a scooter passed by the taxi, the passenger in the back seat of the taxi opened the door, which scraped and damaged the scooter. Proceedings were initiated and a report was drawn up in which the taxi driver was identified as responsible for the accident. The owner of the scooter then claimed compensation from the insurance company covering the taxi driver's civil liability. However, the insurance company informed the scooter owner that it would not pay him any compensation on the grounds that the accident had occurred because of the behaviour of the taxi passenger, not because of the driver. Therefore, the insurance company informed the scooter owner that he would have to initiate civil proceedings against the passenger.

Following this advice, the scooter owner approached the taxi company asking it to provide information about the identity of the taxi passenger in order to initiate civil proceedings to obtain compensation for his damages.

In the present case, the taxi company is the controller, while the passenger is the data subject. The owner of the scooter is a third party and has a legitimate interest in obtaining the identity of the person who caused the damage in order to be able to claim compensation. In this context, the communication of the data may therefore be considered as being undertaken to pursue the legitimate interests of a third party. Thus, Article 6(1)(f) of the GDPR could be a valid legal basis for sharing the personal data of the taxi passenger to pursue the legitimate interests of the owner of the scooter.

Nb: this example solely aims at illustrating the notion of a legitimate interest pursued by a third party and is without prejudice to the lawfulness of the processing under national law or other methods by which victims of untraced vehicles might obtain compensation

21. Some of the main contexts where personal data may be processed in the interest of a third party are illustrated below.

[31] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 124. See further Chapter IV, Section 7.1, below in these guidelines.

[32] 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), para. 83.

[33] For example, the CJEU found that the following interest of a third party is, in principle, likely to constitute a legitimate interest within the meaning of Article 6(1)(f) GDPR: the interest of a partner with an indirect shareholding in an investment fund established in the form of a limited partnership offering shares for public subscription to obtain personal data relating to the other indirect partners of that partnership with a view to entering into contract with them or negotiating with them the purchase of shares. See CJEU, judgment of 12 September 2024, Joined Cases C-17/22 and C-18/22, *HTB Neunte Immobilien Portfolio* (ECLI:EU:C:2024:738), paras. 56-57. However, the CJEU also noted that the existence of such an interest should be assessed on a case-by-case basis, taking into account the legal framework applicable and all the circumstances of the case.

[34] 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), para. 83.

22. *Establishment, exercise or defence of legal claims*. A third party may have an interest in establishing, exercising or defending a legal claim. For instance, in the *Rīgas satiksme* case, the CJEU found that "there is no doubt that the interest of a third party in obtaining the personal information of a person who damaged their property in order to sue that person for damages can be qualified as a legitimate interest".[35]

23. *Disclosure of data for purposes of transparency and accountability*. One important context where a legitimate interest of a third party may be identified is the case of disclosure of data for purposes of transparency and accountability (e.g., in certain circumstances, the disclosure of the salaries of the top management in a company), where this is not mandated by law or contract. In this context, it can be considered that the disclosure is done primarily not in the interest of the controller who discloses the data, but rather, in the interest of the recipients of this information, such as the employees or the shareholders of the company.

24. *Historical or other kinds of scientific research*. Another important context where processing in the legitimate interests of third parties may be relevant is historical or other kinds of scientific research.[36]

25. *General public interest or third party's interest*. Interests of third parties, as mentioned in Article 6(1)(f) GDPR, are not to be confused with interests of the wider community (general public interests), although in some cases the interests pursued by a specific controller or a specific third party may also serve broader interests.[37] The interests of the wider community are mainly subject to the justifications provided for in Article 6(1)(e) or (c), if controllers are tasked or required by law to preserve or pursue such interests. This is the case, for instance, when private operators are obliged to assist law enforcement authorities in their efforts to combat certain illegal activities. Where a controller carries out further activities which do not fall within such specific legal obligations set out in laws and regulations, it needs to demonstrate, that this is done in pursuit of the controller's own legitimate interests or those of specific third parties.[38] In any event, a legitimate interest may not be invoked with the aim or effect of circumventing legal requirements.

26. In this context it should be recalled that, in case personal data will be processed for a purpose other than that for which the data were initially collected, the controller must check and ensure that the new purpose is compatible with the original purpose under Article 6(4) GDPR[39] (unless the data subject has given consent or the processing is based on EU or Member State law). Therefore, such compatibility assessment should, in general, be done in situations where personal data were initially collected in the legitimate interest of the controller and, then, are further processed in the legitimate interest of a third party.

[35] CJEU, judgment of 4 May 2017, Case C-13/16, *Rīgas satiksme* (EU:C:2017:336), para. 29.

[36] See by analogy Opinion of Advocate General Mancini in Case 234/83, *Gesamthochschule Duisburg v. Hauptzollamt München-Mitte* [1985] on the interpretation of "scientific activities"' in the context of the legislation relating to custom duties (first indent of Article 3(2) of Regulation No 1798/75): "scientific activities must be interpreted as including activities carried on by a public or private establishment engaged in education or research for the purpose of further the acquisition, development, exposition or dissemination of scientific knowledge […]".

[37] 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), para. 83 (stating that the processing at issue in the case may serve to "pursue the legitimate interest of SCHUFA's contractual partners, who intend to conclude credit agreements with individuals, in being able to assess the creditworthiness of those individuals, and thus the interests of the credit sector from a socio-economic point of view").

[38] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 124.

[39] Article 6(4) GDPR provides a non-exhaustive list of circumstances that must be taken into account in order to determine the compatibility of the purposes. Note that Recital 50 also refers to the reasonable expectations of data subjects based on their relationship with the controller as an additional factor to be considered in this context.

27. Nevertheless, it should be emphasised that Article 6(1)(f) GDPR may be invoked as a valid legal basis only if the necessity and balancing tests outlined below (see Section B and C below in this chapter) have also been carried out and the outcome of such tests was favourable to the controller.

B. 2nd step: Analysis of the necessity of the processing to pursue the legitimate interests

28. The condition relating to the "necessity of the processing" is not specific to processing relying on Article 6(1)(f) GDPR as a legal basis.[40] At the outset, it is important to make clear that the concept of what is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party" does not cover simply what is useful to pursue such an interest. The concept of necessity has an independent meaning in EU law, which must be interpreted in a way that fully reflects the objectives of data protection law.[41] Therefore, it also involves consideration of the fundamental rights to privacy and protection of personal data, as well as the requirements stemming from the data protection principles.

29. Assessing what is "necessary" involves ascertaining whether in practice the legitimate data processing interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects.[42] If there are reasonable, just as effective, but less intrusive alternatives, the processing may not be considered to be "necessary".[43] In this context, the CJEU expressly recalled that the condition relating to the need for processing must be examined in conjunction with the "data minimisation" principle enshrined in Article 5(1)(c) GDPR, in accordance with which personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".[44] The Court also emphasised that a processing should be carried out "only in so far as is strictly necessary" for the purposes of the legitimate interest identified.[45] This requirement of strict necessity is also emphasised, for instance, in Recital 47 GDPR, which states that "[t]he processing of personal data strictly necessary for the purposes of preventing fraud […] constitutes a legitimate interest of the data controller concerned."

30. It should be noted that, in practice, it is generally easier for a controller to demonstrate the necessity of the processing to pursue its own legitimate interests than to pursue the interests of a third party, and that the latter kind of processing is generally less expected by the data subjects.

C. 3rd step: Methodology for the balancing exercise

31. Provided that the interest pursued by the controller is legitimate and the processing is necessary for the purposes of that interest, the last condition to be met to rely on Article 6(1)(f) GDPR as a legal basis is that the legitimate interest in question must not be overridden by the interests or fundamental rights and freedoms of the data subject. This section of the present guidelines outlines this third step (referred to in these guidelines as the "balancing test" or "balancing exercise").

---

[40] Cf. for instance EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects (Version 2.0, 8 October 2019), paras. 23-25.

[41] See CJEU, judgment of 16 December 2008, Case C-524/06, *Huber* (ECLI:EU:C:2008:724), para. 52.

[42] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 108.

[43] Ibid. See also by analogy EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects (Version 2.0, 8 October 2019), para. 25.

[44] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 109; CJEU, judgment of 11 December 2019, Case C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), para. 48; CJEU, judgment of 4 October 2024, Case C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), paras. 42-43 and 51-52.

[45] 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), para. 88; CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 126.

32. This condition entails a balancing of the opposing rights and interests at issue which depends in principle on the specific circumstances of the particular case.[46] Further to the assessment of the legitimate nature of the interest pursued by the controller or by a third party and the analysis of the necessity of the processing, as described above, the controller must identify and describe:

i) The data subjects' interests, fundamental rights and freedoms.
ii) The impact of the processing on data subjects, including
   a. The nature of the data to be processed,
   b. The context of the processing, and
   c. Any further consequences of the processing.
iii) The reasonable expectations of the data subject.
iv) The final balancing of opposing rights and interests, including the possibility of further mitigating measures.

33. It should be recalled that the purpose of the balancing exercise is not to avoid any impact on the interests and rights of the data subjects altogether. Rather, its purpose is to avoid a disproportionate impact and to assess the weight of these aspects in relation to each other.

34. Lastly, it should be recalled that, with the entry into force of the GDPR, many actions that could have been considered to limit the impact of processing on the data subjects, or could have been considered mitigating measures under Directive 95/46/EC, are now legal obligations for the controller. This is crucial in the balancing test, which presupposes that the controller already complies with the principles and obligations set out in the GDPR. Therefore, the following sub-sections only consider actions to limit impact or mitigating measures when they go beyond what is required of the controller under the GDPR.

1. Data subjects' interests, fundamental rights and freedoms

35. Article 6(1)(f) GDPR provides that in assessing the different components to be balanced against each other, the controller must take into account the interests and the fundamental rights and freedoms of the data subject.

36. The explicit reference to "interests or fundamental rights and freedoms" in Article 6(1)(f) GDPR has a direct impact on the balancing test to be carried out under that provision. It provides more protection for the data subject, as it requires the data subjects' "interests" to be taken into account, not only their fundamental rights and freedoms.

37. The fundamental rights and freedoms of the data subjects include the right to data protection and privacy, but also other fundamental rights and freedoms, such as the right to liberty and security, freedom of expression and information, freedom of thought, conscience and religion, freedom of assembly and association, prohibition of discrimination, the right of property, or the right to physical and mental integrity, which may be affected by the processing, either directly or indirectly (e.g. through a chilling effect, see para. 46 below).

38. The interests of the data subjects to be taken into account as part of the balancing test include any interest that may be affected by the processing at stake, including, but not limited to, financial interests, social interests or personal interests.

[46] See CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 110.

2. Impact of the processing on the data subjects

39. After having identified the fundamental rights and interests that may be affected by the processing, the controller should carefully assess the likely impact of the processing on the data subject. This assessment should focus on the various ways in which individuals may be affected – positively or negatively, actually or potentially – by the processing of their personal data. The impact of the processing on the data subject may be influenced by the nature of the data to be processed, the context of the processing and the further consequences that the processing may have.

2.1. The nature of the data to be processed

40. In qualifying the nature of the data to be processed, the controller should pay special attention to, among other things:

- The fact that special categories of personal data enjoy additional protection under Article 9 GDPR and, that the processing of special categories of personal data ("sensitive data") is only allowed under specific additional conditions set out in Article 9(2) GDPR.[47] In this regard, it should be kept in mind that a set of data that contains at least one sensitive data item is deemed sensitive data in its entirety, in particular if it is collected *en bloc* without it being possible to separate the data items from each other at the time of collection.[48] Further, it should be recalled that data are deemed sensitive if such data allow information falling within one of the categories referred to in Article 9(1) GDPR to be revealed.[49] It is irrelevant whether or not the information revealed by the processing operation in question is correct and whether the controller is acting with the aim of obtaining information that falls within one of the special categories referred to in that provision.[50] Hence, according to the jurisprudence of the CJEU, the relevant question is whether it is objectively possible to infer sensitive information from the data processed, irrespective of any intention of actually doing so.
- The fact that personal data relating to criminal convictions and offences enjoy additional protection under Article 10 GDPR.
- The types of data that data subjects generally consider to be more private (e.g., financial data, location data, etc.), or rather of a more public nature (e.g., data concerning one's professional role).

41. As a general rule, the more sensitive or private the nature of the data to be processed, the more likely it is that the processing of such data will have a negative impact on the data subject, and the more weight should be attributed to it in the balancing test. However, this does not mean that seemingly less sentitive data may be regularly processed under Article 6(1)(f) GDPR. The impact of the processing of such data may nevertheless be significant, for example because of the context in which the processing takes place.

42. It should further be underlined that the controller should have already verified whether or not the processing of personal data is necessary for the pursuit of the legitimate interest. If further limitations to the categories of data to be processed are possible at this stage, the controller should revert to step 1 of the legitimate interest test (if its objectives have changed) or to step 2 of the legitimate interest test (to review necessity based on the newly defined scope of the processing).

2.2. The context of the processing

[47] It should be reiterated that meeting the conditions laid down in Article 9(2) GDPR does not automatically fulfil the conditions of Article 6(1)(f) GDPR. If this legal basis for processing is to be used, the controller must satisfy the requirements of both GDPR provisions when it processes special categories of personal data.
[48] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 89.
[49] Ibid., para. 68.
[50] Ibid., para. 69.

43. The context of the processing and the specific data processing methods may also influence the impact that the processing may have on the rights and interests of the data subject. In this respect, the controller should have due regard, among other things, to:

- the scale of the processing and the amount of personal data to be processed (in terms of overall volume of data, volume of data per data subject, and the number of data subjects affected),[51]
- the status of the controller, including vis-à-vis the data subject (e.g., an employer-employee relationship will likely require an assessment that is different from the one concerning a service provider-customer relationship),
- whether or not the personal data to be processed are combined with other data sets,
- the degree of accessibility and/or publicity of the data to be processed,[52] and
- the status of the data subject (e.g., vulnerable individuals).

44. Moreover, it is apparent from the very wording of Article 6(1)(f) GDPR that it is necessary to pay particular attention to the situation where the data subject is a child. As the CJEU held,[53] referring to Recital 38 GDPR, children merit specific protection with regard to the processing of their personal data because they may be less aware of the risks, consequences and safeguards concerned and of their rights related to such processing of personal data. The CJEU ruled that such specific protection should, in particular, apply to the processing of personal data of children for the purposes of marketing or creating personality or user profiles or offering services aimed directly at children.[54]

2.3. Further consequences of the processing

45. The consequences of the envisaged processing may further impact the rights, freedoms and interests of the data subjects. Factors that the controller may need to take into account – depending on the context and nature of the data to be processed – may include:

- Potential future decisions or actions by third parties that may be based on the personal data to be processed by the controller,
- The possible production of legal effects concerning the data subject,
- Exclusion of or discrimination against individuals,
- Defamation, or more broadly, situations where there is a risk of damaging the reputation, negotiating power or autonomy of the data subject,
- Financial losses which may be incurred by the data subject,
- Exclusion from a service for which there is no real alternative, and
- Risks to freedom, safety, physical and mental integrity or life of natural persons.

46. In addition to adverse outcomes that can be specifically foreseen,[55] the controller may need to take into account also possible broader emotional impacts resulting from a data subject losing control over

[51] Ibid., para. 116.

[52] The fact that personal data have been manifestly made public does not automatically mean that they may be processed under Article 6(1)(f) GDPR (see in this respect CJEU, judgment of 4 May 2017, Case C-13/16, *Rīgas satiksme* (EU:C:2017:336), para. 32; CJEU, judgment of 11 December 2019, Case C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), para. 54; CJEU, judgment of 24 November 2011, Joined Cases C-468/10 and C-469/10, *ASNEF* (ECLI:EU:C:2011:777), para. 44). However, this can be a factor to be taken into account when performing a balancing test.

[53] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 111.

[54] Ibid.

[55] For example, the CJEU held that, when a controller intends to transmit personal data to a provider of games of chance and casino games based on Article 6(1)(f) GDPR, the possible harmful effects that may derive from such transmission should be taken into account since data subjects could be exposed to the risks associated with the development of gaming addiction. See CJEU, judgment of 4 October 2024, Case C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), para. 56.

personal information, or realising that it has been misused or compromised. The chilling effect on protected behaviour, such as freedom of research or freedom of expression, that may result from continuous monitoring/tracking or from the risk of being identified, should also be given due consideration. For example, continuous online monitoring of online activities by a platform may give rise to the feeling that a data subject's private life is being continuously observed.[56]

47. The impact that the processing may have on the rights, freedoms and interests of the data subject should be taken into account by way of an objective assessment. When it is clear that a large number of data subjects share the same interests, a combined assessment of such interests may suffice (e.g. in the area of video surveillance). However, the more intrusive a processing operation is, the more specific circumstances should be factored into the assessment. In addition, the controller should not base its assessment of the interests at stake on an assumption that all of the affected data subjects share the same interests when it has – or should have – concrete indications of the existence of particular individual interests or when, from an objective perspective, it is simply not likely that all data subjects will have the same interest(s) the controller has assumed. This is especially true in the context of an employer-employee relationship.

48. In carrying out this assessment, the controller should bear in mind that the GDPR already requires it to implement measures, by design, in order to limit the processing of personal data and its impact on data subjects only to what is necessary for the specified purpose pursued (see in particular Articles 5 and 25 GDPR)[57]. The impact weighed in the balancing test should therefore already be the minimum impact under the GDPR, notwithstanding the adoption of measures that go beyond the obligations set out in the GDPR which can be applied as mitigating measures, as outlined in section 4 below in this chapter.

49. Moreover, if high risks are identified in the context of this assessment, the controller should consider performing a Data Protection Impact Assessment (DPIA) in accordance with Article 35 GDPR.[58]

3. Reasonable expectations of the data subject

50. Recital 47 GDPR makes clear that "[t]he legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller." That Recital further states that "[a]t any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data is processed in circumstances where data subjects do not reasonably expect further processing."[59]

51. The controller should therefore take into account the reasonable expectations of data subjects when weighing its legitimate interest(s) and the interests or fundamental rights and freedom of data subjects.

[56] Ibid., para. 118.

[57] See EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, adopted on 20 October 2020.

[58] See Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01), which have been endorsed by the EDPB.

[59] See further CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 112; CJEU, judgment of 11 December 2019, Case C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), para. 58; CJEU, judgment of 4 October 2024, Case C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), para. 55.

52. The data subjects' reasonable expectations play an important role in the balancing test, in particular to limit the risks that data subjects are unduly surprised by the processing or by its consequences or implications. In this respect, it is important to distinguish between the notion of reasonable expectations and what is considered common practice in certain sectors. The fact that certain types of personal data are commonly processed in a given sector does not necessarily mean that the data subject can reasonably expect such processing.[60]

53. Reasonable expectations do not necessarily depend on the information provided to data subjects. While the omission of information can contribute to the data subject being surprised of a certain processing, the mere fulfilment of the information obligations set out in Articles 12, 13 and 14 GDPR is not sufficient in itself to consider that the data subjects can reasonably expect a given processing.[61]

54. Although not exhaustive, the following list is meant to illustrate contextual elements which can be considered in the assessment of the reasonable expectations of data subjects:

- Characteristics of the relationship with the data subject or of the service:
    - The very existence of a relationship with the data subject (e.g., one should distinguish between customers and non-customers), including the date of termination of the relationship where there was one;
    - The proximity of the relationship (e.g., cases where a controller is part of a group of companies with one single brand vs. group of companies that only have economic bonds unknown to the average customer, as in the latter case the data subject is less likely to reasonably expect data sharing between group entities);
    - The place and context of the data collection (e.g., data subjects might expect CCTV in a bank but not in sanitary or sauna facilities);
    - The nature and characteristics of the service (e.g., a regular customer and a mere prospective customer who only subscribed to a newsletter will have different reasonable expectations); and
    - Applicable legal requirements in the relevant context (e.g., confidentiality requirements applicable to the relevant relationship).

- Characteristics of the "average" data subjects whose personal data is to be processed. The balancing test should consider the "average" data subject – unless the processing is likely to affect different groups of data subjects with different characteristics[62] – and take into account:
    - The age of the data subject (minors' reasonable expectations can be different from those of adults),
    - The extent to which the data subject is a public figure, and
    - The (professional) position that the data subject holds and the level of understanding and knowledge of the envisaged processing that they are likely to have in a certain context (e.g., the personnel to be involved in a job interview process would often expect some of their personal data to be shared with job applicants).

[60] See in particular CJEU, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 117, in which the Court held: "it is important to note that, despite the fact that the services of an online social network […] are free of charge, the user of that network cannot reasonably expect that the operator of the social network will process that user's personal data, without his or her consent, for the purposes of personalised advertising."

[61] EDPB, Guidelines 8/2020 on the targeting of social media users, Version 1.0, para. 66. However, it should be noted that contractual provisions regarding personal data may have a bearing on the reasonable expectations of data subjects. See CJEU, judgment of 12 September 2024, Joined Cases C-17/22 and C-18/22, *HTB Neunte Immobilien Portfolio* (ECLI:EU:C:2024:738), para. 64.

[62] See further para. 47 above in these guidelines.

Example 5:

An online social network is financed through online advertising, which is tailored to the individual users of the social network according, inter alia, to their consumer behaviour, interests, purchasing power and personal situation. Such advertising is made possible in technical terms by the automated production of detailed profiles in respect of the network users. To that end, in addition to the data provided by the users directly when they sign up for the online service, other user- and device-related data are also collected on and off that social network, and linked to their user account. The aggregate view of the data allows detailed conclusions to be drawn about those users' preferences and interests.

Despite the fact that the services of the online social network are free of charge, the user of that network cannot reasonably expect that the operator of the social network will process that user's personal data, without his or her consent, for the purposes of personalised advertising.[63] Further, the users of the online social network cannot reasonably expect those data to be processed even for other purposes such as product improvement.[64]

Nb: this example solely aims at illustrating the reasonable expectations a data subject may have in this context and is without prejudice to compliance of the processing at stake with other elements of Article 6(1)(f) or other provisions of the GDPR or other relevant laws.

Example 6:

A company is printing marketing flyers using images of people's faces publicly available on the internet and social media platforms. The people appearing in the photos are the ones who have published them.

In this case, even when the photos were made public by the data subjects themselves, they could not reasonably expect that their photos would be processed and published by a third party.

Nb: this example solely aims at illustrating the lack of reasonable expectations of a data subject and is without prejudice to compliance with other provisions of the GDPR or other relevant laws.

4. Finalising the balancing test

55. Once the controller has identified and assessed the legitimate interest(s) being pursued, the relevant interests, rights and freedoms of the data subject, the impact of the processing, and the reasonable expectations of the data subject, the controller should be able to strike a balance between all the interests, rights and freedoms identified. If the outcome of this assessment is that the legitimate interest(s) being pursued are not overridden by the data subject's interests, rights and freedoms, the envisaged processing may take place.

56. However, if the data subject's interests, rights and freedoms seem to override the legitimate interest(s) being pursued, the controller may consider introducing mitigating measures to limit the impact of the

[63] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 117.
[64] Ibid., para. 123.

processing on data subjects, in view of achieving a fair balance between the rights, freedoms and interests involved.

57. Yet, these mitigating measures should not be confused with the measures that the controller is legally required to adopt anyway to ensure compliance with the GDPR, irrespective of whether the processing is based on Article 6(1)(f) GDPR. For that reason, mitigating measures can, for instance, not consist of measures meant to ensure compliance with the controllers' information obligations, security obligations, obligations to comply with the principle of data minimisation, or the fulfilment of data subject rights under the GDPR, and must go beyond what is already necessary to comply with these legal obligations under the GDPR. For example, introducing additional safeguards above and beyond the safeguards required under the GDPR may be seen as a mitigating measure (e.g., allowing the data subject to exercise the right to erasure even when the specific grounds listed in Article 17(1) GDPR do not apply, allowing the data subject to exercise the right to object without any of the limitations in Article 21 GDPR, allowing the data subject to exercise the right to data portability even when the processing is based on Article 6(1)(f), etc.).[65]

58. Moreover, if controllers decide to implement mitigating measures, they should perform the balancing test anew, in order to assess whether the legitimate interest(s) being pursued are overridden by the data subject's interests, rights and freedoms, after the adoption of the mitigating measures.

59. Even though the controller should aim to strike this balance as objectively as possible, any balancing exercise remains a case-by-case evaluation. The duty is upon the controller to demonstrate that the balancing test has been conducted appropriately and that the legitimate interest(s) being pursued are not objectively overridden by the data subject's interests, fundamental rights and freedoms.

60. If the data subject's interests, rights and freedoms override the legitimate interests being pursued, and no sufficient mitigating measures can be taken, the processing cannot be based on Article 6(1)(f) GDPR.

III. RELATIONSHIP BETWEEN ARTICLE 6(1)(F) GDPR AND DATA SUBJECT RIGHTS

1. Introduction to data subject rights

61. Chapter III of the GDPR provides for data subject rights and sets out the requirements for exercising them, imposing obligations on the controller. It should be stressed that, pursuant to Article 12(1) GDPR, the controller shall take appropriate measures to provide any information about the processing and any communication in the context of the exercise of data subject rights in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The controller shall also facilitate the exercise of the data subject rights in accordance with Article 12(2) GDPR.[66] In response to a request for exercising the data subject rights laid down in Articles 15 to 22, the controller shall provide information on the action taken – or information on the reasons for not taking action – without undue delay, and in any event within one month of receipt of the request.[67]

[65] For further examples of possible mitigating measures, see WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, p. 42 and following.
[66] The EDPB already issued guidance on the interpretation of Article 12(1) and (2) GDPR. See WP29, Guidelines on transparency under Regulation 2016/679 (WP260 rev.01), as last revised and adopted on 11 April 2018 (endorsed by the EDPB); and EDPB, Guidelines 01/2022 on data subject rights – Right of access, Version 2.1, adopted on 28 March 2023.
[67] In certain circumstances this deadline may be extended, see Article 12(3) GDPR.

62. While complying with the GDPR provisions on data subject rights is a legal obligation (and therefore not something that controllers can consider as a mitigating measure in a balancing exercise), some of the rights laid down in those provisions are subject to specific conditions. Going beyond what is strictly required under the GDPR may be seen as an additional safeguard that could be considered in the balancing test.[68]

63. It is also worth mentioning in this context that Article 25 GDPR makes clear that it is the responsibility of the controller to implement appropriate technical and organisational measures in an effective manner and to integrate the necessary safeguards into the processing activities to protect the rights of the data subject at the time of the determination of the means of the processing and at the time of the processing itself. [69]

2. Transparency and information to be provided to data subjects

64. As for any personal data processing falling within the scope of the GDPR, controllers that undertake processing activities based on Article 6(1)(f) GDPR must comply with their transparency obligations under Articles 12, 13 and 14 GDPR.

65. Transparency is intrinsically linked to the fairness principle.[70] The latter principle requires, for example, that personal data are not processed in a way that is unjustifiably detrimental, discriminatory, unexpected or misleading to the data subject. In this respect, it should be noted that the adoption of measures and safeguards implementing the fairness principle may support the data subject's transparency rights under the GDPR.[71]

66. Transparency is also an essential element to ensure the effective exercise of data subject rights. Where personal data are collected directly from the data subject, information to him or her shall be provided at the time when personal data are obtained.[72]

67. Pursuant to Article 12(1) GDPR, any information and communication relating to the processing of personal data must be easily accessible and easy to understand, in particular when information is provided to children.[73] Under Articles 13(1)(c) and 14(1)(c) GDPR, the information that must be provided to a data subject should notably include the legal basis for the processing. Therefore, data subjects should be specifically informed that the processing is based on Article 6(1)(f) GDPR, if the controller intends to rely on this legal basis. Furthermore, when the processing is based on Article 6(1)(f) GDPR, the specific legitimate interest(s) pursued must be precisely identified and communicated to the data subject in accordance with Article 13(1)(d) and 14(2)(b) GDPR.[74]

[68] See the section on the "balancing test" above in these guidelines.
[69] See further EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, adopted on 20 October 2020.
[70] The principles of transparency and fairness are laid down in Article 5(1)(a) GDPR. Note that Articles 13(2) and 14(2) GDPR also refer to a "fair and transparent processing".
[71] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, adopted on 20 October 2020, para. 69.
[72] See Article 13(1) GDPR. Where personal data have not been obtained from the data subject, the time limits for providing information are stated in Article 14(3) GDPR.
[73] See also Recitals 39 and 58 GDPR.
[74] The importance of providing the data subject with information on the legitimate interest(s) pursued where the processing is based on Article 6(1)(f) GDPR is also underlined by the CJEU. See CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 107.

68. It should be noted that the controller can also provide the data subject with information from the balancing test in advance of any collection of personal data. To avoid information fatigue, this can be included within a layered privacy statement/notice. In any case, information to the data subjects should make it clear that they can obtain information on the balancing test upon request. This is essential to ensure effective transparency and to allow data subjects to dispel possible doubts as to whether the balancing test has been carried out fairly by the controller or assess whether they might have grounds to file a complaint with a supervisory authority.[75] Such transparency obligation also follows from the accountability principle in Article 5(2) GDPR, which requires the controller to be able to demonstrate compliance with each of the principles set out in Article 5(1) GDPR, including the lawfulness principle. Furthermore, as described above (see paras. 51-53), the reasonable expectations of data subjects should be considered in the balancing test. While a failure to provide information can contribute to the data subjects being surprised, the mere fulfilment of information duties according to Articles 12, 13 and 14 GDPR is not sufficient in itself to consider that the data subjects can reasonably expect a given processing.

3. Right of access

69. In order to exercise data subject rights, such as the right to object and the right to erasure, it is helpful to first be aware of what data is processed and for what purposes.[76] According to Article 15(1) GDPR, the data subject has the right to obtain confirmation from the controller as to whether personal data concerning him or her are being processed and to have access to the personal data that are being processed. The data subject must also be provided with further information about the processing in accordance with Article 15(1) and (2) GDPR.[77]

70. Unlike the information required under Articles 13 and 14 GDPR, there is no explicit obligation under Article 15(1) GDPR to provide information about the legal basis for the processing. However, the EDPB has recommended that controllers provide also this information – or indicate where this information can be found – in response to a request for access.[78] In this respect, it should be noted that, as made clear in Recital 60 GDPR, the controller should provide the data subject with any further information necessary to ensure a fair and transparent processing. Furthermore, it should be stressed that the right of access must enable the data subject to verify that their personal data are processed in a lawful manner,[79] and that the controller has a duty to demonstrate compliance with the lawfulness principle.[80] Moreover, without knowing the legal basis for the processing, the data subjects would in some cases not be in a position to assess what data subject rights they can exercise, since some of those rights depend on the applicable legal basis.

4. Right to object

71. When processing is based on Article 6(1)(f) GDPR, the data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or

[75] See the Guidelines on transparency under Regulation 2016/679 (WP260 rev.01), page 36. These guidelines have been endorsed by the EDPB.
[76] On the importance of the right of access for the exercise of other data subject rights, see e.g. CJEU, judgment of 12 January 2023, Case C-154/21, *Österreichische Post* (ECLI:EU:C:2023:3), paras. 37-38.
[77] The EDPB has published more extensive guidance on the right of access under the GDPR. See EDPB Guidelines 01/2022 on data subject rights – Right of access.
[78] Ibid, para. 114.
[79] CJEU, judgment of 22 June 2023, Case C- 579/21, *Pankki S* (ECLI:EU:C:2023:501), para. 57.
[80] See CJEU, judgment of 4 May 2023, Case C-60/22, *UZ v. Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), para. 53.

her under Article 21(1) GDPR.[81] However, the fact that the data subject has not elaborated much on their "particular situation" in their objection is not *per se* sufficient to dismiss the objection. If the controller has doubts as to the "particular situation" of the data subject, it may ask the data subject to further specify the request.

72. After an objection, the controller shall no longer process the personal data unless there are overriding compelling legitimate grounds which take precedence over the interests and rights and freedoms of that person, which it is for the controller to demonstrate.[82] Thus, contrary to Directive 95/46/EC, the GDPR places the burden of proof on the controller, and provides a presumption in favor of the data subject.[83]

73. The notion of "compelling legitimate grounds" is not defined in the GDPR. However, it is clear from the wording of Article 21 GDPR that the assessment to be made by the controller to demonstrate that there are legitimate grounds that take precedence over the interests and rights and freedoms of the data subject is different from the balancing exercise to be made under Article 6(1)(f) GDPR.[84] If a data subject has invoked their right to object against a processing based on Article 6(1)(f) GDPR, it is not sufficient for the controller to just demonstrate that its earlier legitimate interest assessment regarding that processing was correct. The balancing test to be made under Article 21(1) GDPR is to be carried out in view of the particular situation of the data subject and requires the legitimate grounds invoked by the controller to be *compelling*, implying a higher threshold for overriding data subject objections.[85] In other words, not all conceivable legitimate interests that may justify processing under Article 6(1)(f) GDPR are relevant in this context. Only interests that can be recognised as "compelling" may be balanced against the rights, freedoms and interests of the data subject to assess whether there are grounds for processing that take precedence, despite the objection of the data subject.[86] In essence, the grounds invoked should be essential to the controller (or to the third party in whose legitimate interest the data are being processed) to be considered compelling.[87] This might be the case, for example, if a controller is compelled to process the personal data in order to protect its organisation or systems from serious immediate harm or from a severe penalty which would seriously affect its business.[88] In contrast, showing that the processing would simply be beneficial or advantageous to the controller would not necessarily meet this threshold. The presence of compelling legitimate grounds needs to be assessed on a case-by-case basis and be linked to a specific objection.

74. After having identified the relevant compelling legitimate grounds, the controller should proceed to assess whether the compelling legitimate grounds identified override the interests, rights and freedoms of the data subject who objected to the processing, taking into account the "particular situation" of that data

[81] It should be emphasised that the data subject enjoys such a right to object also when the processing is lawfully based on Article 6(1)(e) (see further Recital 69 GDPR). Furthermore, the data subject enjoys a specific right to object to processing for direct marketing purposes (which may or may not be based on Article 6(1)(f) GDPR) under Article 21(2) GDPR, and that right may not be trumped by showing that there are overriding legitimate grounds which take precedence over the interests and rights and freedoms of the data subject. For further details on the latter right, see the section on "processing for direct marketing purposes" below in these guidelines.

[82] 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), para. 111. See also Recital 69 GDPR.

[83] See EDPB, Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR
(part 1), Version 2.0, Adopted on 7 July 2020, para. 30.

[84] See EDPB, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, revised version of 6 February 2018, p. 19.

[85] Ibid.

[86] See EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, p. 15.

[87] Ibid.

[88] Ibid.

subject. This entails an assessment of the impact of the processing on the particular situation of the data subject.[89]

75. The balancing exercise carried out by the controller to assess whether the identified compelling legitimate grounds take precedence over the competing interests of the data subject needs to be duly documented in accordance with the accountability principle.

5. Right to erasure

76. Under the GDPR, data subjects enjoy a right to obtain from the controller the erasure of their personal data.[90] This right may often be exercised also when the controller relied upon Article 6(1)(f) GDPR to process the data. For example, the data subject may request the deletion of their personal data when: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;[91] the controller has unduly relied upon Article 6(1)(f) GDPR to process the personal data;[92] the data subject has successfully invoked its right to object against a processing based on Article 6(1)(f) GDPR, in accordance with the conditions laid down in Article 21 GDPR.[93] As noted above, under the GDPR, data subjects enjoy a right to object, unless there are overriding compelling legitimate grounds which take precedence over the interests and rights and freedoms of that person, which it is for the controller to demonstrate. If the controller fails to provide such proof, the data subject is entitled to request the erasure of the data on the basis of Article 17(1)(c) GDPR, where he or she objects to the processing in accordance with Article 21 GDPR.[94]

77. The right to erasure is often closely linked, from a conceptual and practical perspective, to the right to object, in particular when the processing is based on Article 6(1)(f) GDPR. As a result, it might happen that the data subject's request is not completely clear about whether the data subject wishes to obtain the erasure of their personal data or objects to the relevant processing. In this respect, it should be noted that the GDPR does not introduce any formal requirements for the exercise of data subject rights. Therefore, the controller cannot refuse to act on a data subject's request simply by referring to the lack of indication of the legal ground of the request, especially to the lack of a specific reference to the right to erasure or object, or to the GDPR.[95] Nor will it be sufficient, in case of a request that the controller considers to be unclear, for the controller to only take the steps required in response to an objection to processing as a default reaction, instead of evaluating whether the data subject's request suggests that what the data subject actually wishes to obtain is the full deletion of their data. The indications provided by the data subject in the request, as well as the context of the request, should be taken into account to decide what action should be taken by the controller to appropriately address the request. In case of doubts on the scope and nature of a data subject's request, it is recommended that the controller asks the data subject to specify their request.

78. Furthermore, it should be stressed that, in general, the criteria to determine whether an objection or an erasure request should be granted are essentially the same under Article 21 and Article 17 (i.e., the

[89] See by analogy CJEU, judgment of 9 March 2017, Case C-398/15, *Manni* (ECLI:EU:C:2017:197), para. 47; CJEU, judgment of 13 May 2014, Case C-131/12, *Google Spain* (ECLI:EU:C:2014:317), para. 76.
[90] See Article 17 GDPR.
[91] See Article 17(1)(a) GDPR.
[92] See Article 17(1)(d) GDPR.
[93] See Article 17(1)(c) GDPR.
[94] 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), paras. 111-112.
[95] Cf. by analogy EDPB Guidelines 01/2022 on data subject rights - Right of access, Version 2.0, adopted on 28 March 2023, para. 50.

request should be granted unless one can demonstrate "overriding legitimate grounds"). This implies that, as a rule, if an objection under Article 21(1) GDPR is granted, a related erasure request under Article 17(1)(c) GDPR should also be granted.[96]

79. The GDPR does not specify how controllers should ensure deletion. However, it should be noted that controllers have to be able to demonstrate that the right to erasure has been entirely complied with in accordance with the principle of accountability laid down in Article 5(2) GDPR,[97] and that the data subject may lodge a complaint or initiate a legal action concerning the erasure.

6. Automated individual decision-making, including profiling

80. The GDPR specifically addresses automated decision-making in Article 22, and confers on the data subject the right not to be the subject of a decision solely based on automated processing, including profiling. [98] That provision lays down a prohibition in principle, the infringement of which does not need to be invoked individually by such a person.[99] Therefore, this kind of processing should not take place, unless one of the exceptions listed in Article 22(2) GDPR applies.[100]

81. In any event, even when this kind of automated processing is authorised in the cases referred to in Article 22(2) GDPR, the processing will be lawful only if the controller is able to identify a valid legal basis for the processing in Article 6(1) GDPR. In this respect, the CJEU noted with regard to Article 6(1)(f) GDPR that Member States cannot, under Article 22(2)(b) GDPR, dismiss the requirements resulting from the case-law of the Court, in particular, by definitively prescribing the result of the balancing of the rights and interests at issue.[101] For the sake of clarity, it should also be emphasised that Article 6(1)(f) GDPR should not be considered Union law authorising automated decision-making within the meaning of Article 22(2)(b) GDPR.

82. Not all profiling activities lead to automated decision-making that falls under Article 22 GDPR. However, regardless of whether the controller intends to engage in profiling that would lead to automated decision-making that falls under Article 22 GDPR, the following elements are particularly relevant when performing the balancing exercise before invoking Article 6(1)(f) GDPR as a legal basis:

- the level of detail of the profile (a data subject profiled within a broadly described cohort such as "people with an interest in English literature", or segmented and targeted on a granular level);
- the comprehensiveness of the profile (whether the profile only describes a small aspect of the data subject, or paints a more comprehensive picture);
- the impact of the profiling (the effects on the data subject);
- the possible future combination of profiles; and
- the safeguards ensuring fairness, non-discrimination and accuracy in the profiling process.[102]

[96] Cf. EDPB Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1), Version 2.0, adopted on 7 July 2020, para. 30.
[97] See e.g. CJEU, judgment of 4 May 2023, Case C-60/22, *UZ v. Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), para. 53.
[98] For further guidance on Article 22 GDPR, see Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01), as last revised and adopted on 6 February 2018.
[99] CJEU, judgment of 7 December 2023, Case C-634/21, *SCHUFA Holding (Scoring)* (ECLI:EU:C:2023:957), para. 52.
[100] Ibid., para. 53.
[101] Ibid., para. 70.
[102] Ibid.

7. Right to rectification

83. According to Article 16 GDPR, the data subject has the right to ask and obtain from the controller the correction of inaccurate data and the completion of incomplete data. This right is of great importance to enable data subjects to have control over their own personal data.[103]

84. The right to rectification can be invoked regardless of which of the legal bases for processing applies. Nonetheless, this right is especially relevant in situations where the data have not been obtained from the data subject, as the likelihood of inaccuracies and incompleteness is generally higher in such situations. In practice, this may often be the case when the processing is based on Article 6(1)(f) GDPR.

85. The CJEU has made clear that the assessment of whether personal data is accurate and complete must be made in the light of the purpose for which that data was collected.[104] Therefore, one should have due regard to these purposes when assessing the accuracy and completeness of the relevant data.

86. The data subject may have a legitimate interest in having their data rectified.[105] However, in principle, the right to rectification can be successfully invoked by the data subject only when they can substantiate that the data being processed is objectively incorrect or incomplete.[106] Conversely, the right in question may not be used to make sure that a certain evaluation reflects the personal opinions of the data subject, or to enable a candidate to "correct", a posteriori, answers at a professional examination that are "incorrect".[107]

8. Right to restriction of processing

87. In certain circumstances, the data subjects may request a restriction of the processing of their personal data, which entails the marking of stored personal data with the aim of limiting their processing in the future.[108] As a result, the controller may retain the personal data that are being processed, but must cease other processing activities (except for the specific kinds of processing activities mentioned in Article 18(2) GDPR).[109]

88. The right to restriction of processing may be invoked in four different instances specified in Article 18(1) GDPR, one of which is especially relevant when the processing is based on Article 6(1)(f) GDPR: the data subject has the right to obtain from the controller restriction of processing when they have objected to a processing based on Article 6(1)(f) in accordance with Article 21(1) GDPR.[110] In this case, the restriction of processing is limited in time, as it applies only pending the verification of whether the legitimate grounds of the controller override the rights, interests and freedoms of the data subject.[111] Once that assessment has been completed, the data should either be deleted (if the interests, rights and freedoms of the data subject prevail), or the restriction may be lifted (if the controller is able to demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject).

[103] As illustrated by Advocate General Pikamäe in the context of data processing by credit information agencies. See Opinion of Advocate General Pikamäe in Case C-634/21, *Schufa (scoring)* (ECLI:EU:C:2023:220), para. 50.
[104] CJEU, judgment of 20 December 2017, Case C-434/16, *Nowak* (ECLI:EU:C:2017:994), para. 53.
[105] See Opinion of Advocate General Kokot in Case C-434/16, Nowak (ECLI:EU:C:2017:582), paras. 37-39.
[106] Cf. ECHR, judgement of 27 April 2010, 27138/04, *Ciubotaru v. Moldova* (ECLI:CE:ECHR:2010:0427JUD002713804), para. 59.
[107] CJEU, judgment of 20 December 2017, Case C 434/16, *Nowak* (ECLI:EU:C:2017:994), para. 52.
[108] See Article 4(3) GDPR.
[109] See Article 18(2) GDPR.
[110] See Article 18(1)(d).
[111] See the section on the right to object, above in these guidelines.

89. As noted above, where processing has been restricted under Article 18(1) GDPR, the personal data may not, as a rule, be subject to processing operations beyond their mere storage. However, in exceptional circumstances, the personal data may be processed for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.[112] This processing could often be based on Article 6(1)(f) GDPR as a legal basis (provided that the necessity and balancing tests yield positive results).

IV. CONTEXTUAL APPLICATION OF ARTICLE 6(1)(F) GDPR

90. Article 6(1)(f) GDPR may be relevant as a legal basis in a wide variety of contexts. The present chapter of these guidelines describes several contexts where this legal basis might be relied upon, or that present specific features that should be given careful consideration when assessing whether to rely on Article 6(1)(f) GDPR as a legal basis.

1. Processing of children's personal data

91. Children deserve specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerning their rights in relation to the processing of personal data.[113] Article 6(1)(f) GDPR, unlike Article 7(f) Directive 95/46/EC, expressly refers to the protection of children's personal data.

92. While, in general terms, the legal basis in Article 6(1)(f) GDPR allows for a proportionate level of interference with the rights of data subjects, the balancing test should be recalibrated where the data subjects are children. This is specifically emphasised in Article 6(1)(f) GDPR, which demands a careful balancing exercise "*in particular* where the data subject is a child" (emphasis added).

93. Where children are concerned, this provision is to be interpreted in light of Article 24(2) of the Charter, which states that "[i]n all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration". [114] The wording of this provision is based on Article 3(1) of the United Nation's Convention on the Rights of the Child (hereafter "UNCRC").[115] The WP29's opinion on the protection of children's personal data under Directive 95/46/EC also specifically noted the need to take special care when the data subject is a child. [116] In particular, it highlighted that, when performing a balancing exercise to assess whether a processing may be based on Article 6(1)(f) GDPR, special care must be taken in relation to the status of children as data subjects, using their best interest as a guide.[117]

[112] See Article 18(2) GDPR.
[113] See *inter alia* Recital 38 GDPR.
[114] The concept of the child's best interests should be assessed on a case-by-case basis, either in relation to an individual child or children in general. The assessment should include the impact on all the rights enshrined in the Convention on the Rights of the Child and its Optional Protocols and not only the impact on the rights to privacy and to data protection.
[115] Convention on the Rights of the Child, signed on 20 November 1989 and ratified by all the Member States.
[116] WP29, Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), adopted on 11 February 2009.
[117] Ibid., page 9.

94. While this does not mean that there will never be a situation in which the interests of the child can be overridden, it does mean that the interests of children as data subjects should have high priority and will very often outweigh the interests of the controller or third parties.[118]

95. The EDPB considers that Article 6(1)(f) GDPR may be invoked as a legal basis by a controller where the legitimate interests pursued coincide with the interests of the child. However, when there is a conflict between a controller's legitimate interests (including regarding processing of personal data for commercial purposes)[119] and the interests or fundamental rights and freedoms of a child, the interests or fundamental rights and freedoms of the child should in general prevail. It is important to highlight, though, that this conclusion does not prevent the use of other legal bases, such as consent, performance of a contract, performance of a task in the public interest or legal obligation, when applicable. The EDPB also considers that there are certain types of data processing operations, such as those consisting of extensive profiling and targeted advertising activities, which – subject to certain limited exceptions – will generally not align with the obligation to ensure specific protection of children.[120] According to Recital 38 GDPR, children merit specific protection with regard to the processing of their personal data because they may be less aware of the risks, consequences and safeguards concerned and of their rights related to such processing of personal data. Thus, such specific protection should, in particular, apply to the processing of personal data of children for the purposes of marketing or creating personality or user profiles or offering services aimed directly at children.[121] Therefore, unless controllers can demonstrate that the activities in question which rely on the processing of children's personal data do not negatively affect the children's interests, such activities should not be undertaken. It is also worth recalling that EU laws other than the GDPR, namely Regulation (EU) 2022/2065 (DSA), prohibit targeted advertising based on the profiling of children's personal data.

96. When Article 6(1)(f) GDPR can be used as a legal basis for processing children's personal data, the controller must ensure and be able to demonstrate that the children's best interests were taken into account as a primary consideration and that appropriate safeguards are in place.

---

[118] See Committee on the Rights of the Children, General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1), paras. 36-40. See further Articles 7, 8 and 24(2) of the Charter as well as Article 16 of the UNCRC.

[119] Commercial purposes means any purpose related to "commercial practices", as defined in Article 2(d) of the Unfair Commercial Practices Directive2005/29/EC: "any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers".

[120] The EDPB guidelines on the targeting of social media users notes, for instance, that "[t]he potential adverse impact of targeting may be considerably greater where vulnerable categories of individuals are concerned, such as children. Targeting can influence the shaping of children's personal preferences and interests, ultimately affecting their autonomy and their right to development." See EDPB, Guidelines 8/2020 on the targeting of social media users, version 2.0, adopted on 13 April 2021, para. 16. In the same vein, the WP29's guidelines on automated individual decision-making and profiling note that "[b]ecause children represent a more vulnerable group of society, organisations should, in general, refrain from profiling them for marketing purposes. Children can be particularly susceptible in the online environment and more easily influenced by behavioural advertising. For example, in online gaming, profiling can be used to target players that the algorithm considers are more likely to spend money on the game as well as providing more personalised adverts. The age and maturity of the child may affect their ability to understand the motivation behind this type of marketing or the consequences." See WP29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), adopted on 3 October 2017, as last revised and adopted on 6 February 2018, page 29. See also Committee on the Rights of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment, para. 42 (stating that "States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes").

[121] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 111.

97. Furthermore, it is important to note that a child is every human below the age of majority. However, that does not mean that all children should be treated equally without having due regard to their age. When taking into account the best interests of a child and a child's reasonable expectations in the context of assessing the potential reliance on Article 6(1)(f) GDPR as a legal basis, the controller should bear in mind that this assessment will likely vary greatly with regard to, for example, different age-groups with varying level of understanding or children with disabilities.

2. Processing by public authorities

98. Article 6(1), second indent, of the GDPR states that the legal basis under Article 6(1)(f) shall not apply to processing carried out by public authorities in the performance of their tasks. Recital 47 of the GDPR clarifies the reason: "it is for the legislator to provide by law for the legal basis for public authorities to process personal data". Such provision indeed relates to the fact that, as a general rule, processing undertaken by public authorities falls under the scope of their tasks and missions provided for by EU or Member State law.

99. Nevertheless, these provisions do not prevent from relying, in exceptional and limited cases, on Article 6(1)(f) GDPR when the processing is not linked to or does not relate to the performance of their specific tasks or the exercise of their prerogatives as public authorities, but concerns, where permitted by the national legal system, other activities that are lawfully carried out. Relying on Article 6(1)(f) GDPR in such exceptional cases should be documented internally. In no circumstances, public authorities may rely on Article 6(1)(f) for processing activities falling within the scope of the performance of their tasks.

3. Processing for the purpose of preventing fraud

100. According to Recital 47 GDPR, data processing in the field of fraud prevention may find its legal basis in Article 6(1)(f) GDPR. This Recital clarifies that the processing of personal data strictly necessary for the purposes of preventing fraud may constitute a legitimate interest of the controller. This does not mean, however, that it is automatically possible to rely on Article 6(1)(f) GDPR as a legal basis to engage in any processing of personal data for the purpose of fraud prevention, as in order to lawfully rely on Article 6(1)(f) GDPR the envisaged processing needs to be based on an interest that is legitimate and fulfill both the necessity and balancing tests.

101. Indeed, the requirements for data processing for the purpose of fraud prevention are strict against the backdrop of the impact that such processing can have on data subjects.

102. Recital 47 does not contain a definition of "fraud prevention". However, the core element of any fraud is the intentional deceptive act or omission by one or more persons in order to obtain an advantage or benefit the person(s) is (or are) not entitled to, or to obtain it in an unlawful manner (e.g. financial fraud, offering counterfeited goods, etc.). Fraud prevention hence includes all measures intended to prevent fraudulent behavior. The detection of fraud can, in principle, also be considered to be covered, since on the one hand there is typically a risk of repetition, and on the other hand this is the only way to carry out the necessary analysis of weaknesses in order to prevent further fraud. However, it must be assessed on a case-by-case basis whether a measure implemented to detect fraud can also be considered suitable for fraud prevention.

103. A service provider may have a legitimate business interest in ensuring that its customers will not misuse the service (or will not be able to obtain services without payment), while at the same time, the

customers of the company, as well as other third parties, may also have a legitimate interest in ensuring that fraudulent activities are discouraged and detected when they occur.[122]

104. However, the processing of personal data for the legitimate interest of fraud prevention does not apply without conditions and limitations, in particular because this kind of processing may have a significant impact on data subjects. For example, Recital 47 makes clear that the processing of personal data must be "strictly necessary for the purposes of preventing fraud", which must be examined in conjunction with the "data minimisation" principle enshrined in Article 5(1)(c) GDPR.[123] At the same time, the principle of storage limitation in Article 5(1)(e) GDPR should be taken into account when deciding the data retention policies that apply to data processed for fraud detection or prevention purposes.

105. In the context of the balancing exercise to be carried out, the interest of a controller to report fraudulent behaviour to competent law enforcement authorities[124] may possibly outweigh the interests, rights and freedoms of the data subjects only if the controller processes data that is accurate and demonstrably relevant to assess whether a data subject is at risk of becoming the victim of fraud or is (un)reliable. For example, the controller may have an overriding legitimate interest in checking the veracity of a specific professional certification mentioned in a CV provided in the context of a job application, when it constitutes an essential criterion for the good performance of the professional position. Controllers should be specific about what type of fraud they are trying to prevent, and what data they really need to process in order to prevent that type of fraud. The fraud the controller is trying to prevent should be of substantial importance, otherwise, the balancing of interests will most likely turn out in favour of the data subject, and the controller will not be able to rely on Article 6(1)(f) GDPR in this respect.

106. The EDPB recalls that any processing of personal data must comply with the principles set forth in Article 5(1) GDPR and that any failure to comply with these principles has the consequence that the respective processing may not take place. The principle of purpose limitation laid down in Article 5(1)(b) GDPR requires that data shall be only collected for specified, explicit and legitimate purposes. It should therefore be noted that a generic reference to the purpose of "combating fraud" to define the legitimate interest, for example in the privacy policy, is not sufficient to meet the transparency and documentation obligations under the GDPR.

107. Controllers should also consider that, to the extent that certain data processing operations in the context of fraud detection and prevention are specifically required by applicable law, the appropriate legal basis for such processing would be Article 6(1)(c) GDPR in connection with the applicable legislation.

108. In some cases, data which have initially been collected for other purposes may incidentally indicate that fraud is taking place, and therefore be further processed by controllers for the purpose of fraud prevention. The EDPB notes that in such situations, controllers must respect the GDPR requirements for further processing.[125]

4. Processing for direct marketing purposes

4.1. The notion of direct marketing

[122] WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217, Adopted on 9 April 2014), p. 35.
[123] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 109.
[124] See further the section 7.1 on "transmission to competent authorities" below in these guidelines.
[125] For more details, see para. 26 of the present guidelines.

109. According to Recital 47 GDPR, the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. Direct marketing is not defined in the GDPR. However, CJEU case law suggests that personalised advertising could be considered a form of direct marketing.[126] Moreover, the CJEU has interpreted the notion of communication for direct marketing purposes under the ePrivacy Directive,[127] which is closely linked to the GDPR[128] and regulates the sending of direct marketing communications.[129] In particular, the CJEU found that to assess whether a communication is made for direct marketing purposes it must be ascertained whether such a communication pursues a commercial purpose and is addressed directly and individually to a consumer.[130] In this respect the CJEU found that it is irrelevant whether the advertising at issue is addressed to a predetermined and individually identified recipient or is sent on a mass, random basis to multiple recipients.[131] What matters is that there is a communication for a commercial purpose, which reaches, directly and individually, a consumer.[132] In this regard, it should be noted that the Court found, for instance, that, based on these criteria, advertising consisting in displaying advertising banners, disguised as emails, into the private email inboxes of the users of an email service – funded by advertising and provided for free to users – is a form of direct marketing (even though such advertising does not entail the sending of an email to a specific consumer).[133] This understanding of the notion of direct marketing purposes may in principle be used by way of analogy to understand its meaning also within the GDPR. This is because the interpretation of a provision of EU law requires that account be taken not only of its wording and the objectives it pursues, but also of its context and the provisions of EU law as a whole. 134

110. The fact that Recital 47 GDPR states that the processing of personal data for direct marketing purposes *may* be carried out to fulfil a legitimate interest does not mean that direct marketing always constitutes a legitimate interest, and that it is automatically possible to rely on Article 6(1)(f) GDPR to engage in all kinds of direct marketing activities.

111. For some cases of direct marketing, a different legal basis – such as consent – may be required, thus precluding the use of legitimate interest as a legal basis in this context, as explained below.

112. Furthermore, it has to be borne in mind that, as outlined above, reliance on legitimate interest requires that three cumulative conditions be fulfilled, namely, first, the pursuit of a legitimate interest by the controller or by a third party; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the interests or fundamental freedoms and rights of the person concerned by the relevant processing do not take precedence over the legitimate interest of the controller or of a third party (see further Chapter II above in these guidelines). [135] It follows from this that the processing of personal data for direct marketing purposes cannot be based on Article 6(1)(f) GDPR if these

[126] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 115.

[127] CJEU, judgment of 25 November 2021, Case C-102/20, *StWL Städtische Werke Lauf a.d. Pegnitz* (ECLI:EU:C:2021:954), paras. 47-50.

[128] The ePrivacy Directive seeks to translate the principles set out in the data protection legal framework into specific rules for the telecommunications sector (see Recital 4 ePrivacy Directive). See further EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019.

[129] See Article 13 ePrivacy Directive.

[130] CJEU, judgment of 25 November 2021, Case C-102/20, *StWL Städtische Werke Lauf a.d. Pegnitz* (ECLI:EU:C:2021:954), para. 47.

[131] Ibid, para. 50.

[132] Ibid.

[133] Ibid., paras. 19-22 and 47-51.

[134] CJEU, judgment of 10 December 2018, Case C-621/18, *Wightman and Others* (ECLI:EU:C:2018:999), para. 47. For an example of how a term in an EU legal act can be interpreted by looking at how the same term is used in other EU acts, see Opinion of Advocate General Tanchev in Case C-617/15, *Hummel Holding* (ECLI:EU:C:2017:13), paras. 30 and following.

[135] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 106; CJEU, judgment of 29 July 2019, Case C-40/17, *Fashion ID* (ECLI:EU:C:2019:629), para. 95.

criteria are not fulfilled. For instance, Article 6(1)(f) GDPR may not be relied on if the direct marketing at issue is unlawful, or if the interests of the data subjects override those of the controller in view of the fact that, for example, they cannot reasonably expect that their data are used for direct marketing purposes.[136]

4.2. Compliance with specific legal requirements that preclude reliance on Article 6(1)(f)

113. Before engaging in the processing of personal data for direct marketing purposes, controllers should consider specific European, as well as national, legislation which may require consent for certain operations in the context of direct marketing, or prohibit some kinds of direct marketing.

114. Most significantly, under the ePrivacy Directive, the sending of unsolicited communications for purposes of direct marketing by email, SMS, MMS and other kinds of similar applications can only take place with the prior consent of the individual recipient.[137] In this respect it should be noted that the consent to be obtained should meet the requirements set out in Article 4(11) GDPR.[138] Therefore, in this context, the processing for direct marketing purposes may not be based on Article 6(1)(f) GDPR.

115. It should be noted that Article 5(3) ePrivacy Directive also requires consent for the use of tracking techniques, such as storing cookies or gaining access to information in the terminal equipment of the user.[139] Therefore, when these techniques are used in the context of direct marketing activities, such consent requirements under Article 5(3) ePrivacy Directive must be respected. Any processing operations of personal data following the aforementioned processing operations, including processing personal data obtained by accessing information in the terminal equipment, must have a legal basis under Article 6(1) GDPR in order to be lawful. Therefore, consent will likely constitute the appropriate legal basis both for storing and gaining access to information already stored on the user's device and for the subsequent processing of personal data,[140] thus normally precluding reliance on Article 6(1)(f) in this context.

116. However, the ePrivacy Directive provides for exceptions to the consent requirements it imposes. For instance, an exception to the requirement of consent is permitted under Article 13(2) ePrivacy Directive when the electronic contact details are lawfully obtained – i.e., are obtained in accordance with the GDPR – from one's own customers in the context of the sale of a product or a service. In this case, the entity that obtained these electronic contact details from its customers may use them for direct marketing of its own similar products or services, as long as the customers can clearly and distinctly object to such use, in an easy manner and free of charge, and have been informed accordingly when the contact details were initially collected and on the occasion of each message in case the customer has not refused such use.

117. It should be borne in mind that an interplay between the GDPR and the ePrivacy Directive arises when the processing of personal data falls within the material scope of both these pieces of legislation.[141] For instance, direct marketing via electronic means of communication but not involving the processing of personal data (e.g., direct marketing addressed to legal persons) is only governed by the ePrivacy

[136] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 117.
[137] See Article 13(1) and Recitals 40 and 67 ePrivacy Directive. It should be noted that the CJEU found that the list of means of communication referred to in Recital 40 and in Article 13(1) of that Directive is not exhaustive. See CJEU, judgment of 25 November 2021, Case C-102/20, *StWL Städtische Werke Lauf a.d. Pegnitz* (ECLI:EU:C:2021:954), paras. 38-39.
[138] See Article 2(f) ePrivacy Directive and Article 94(2) GDPR.
[139] See further EDPB, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, adopted on 7 October 2024
[140] See EDPB, Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, version 2.0, adopted on 9 March 2021, para. 15. See further EDPB, Guidelines 8/2020 on the targeting of social media users, version 2.0, adopted on 13 April 2021, paras. 71-78 and 83-88.
[141] EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019, para. 21.

Directive.[142] However, when the processing of personal data is at stake the ePrivacy Directive is to be considered as *lex specialis* to the extent that it governs such processing.[143] In contrast, communications for the purpose of direct marketing which are not provided by electronic means of communication (e.g., a letter) are not covered by the material scope of the ePrivacy Directive and would therefore not require consent under that Directive. In any event, controllers should also assess the scope of application of the national rules implementing the ePrivacy Directive at Member State level, which may occasionally impose consent requirements that go beyond those laid down in that Directive (e.g., with respect to direct marketing towards professionals).

4.3. Case-by-case assessment to be made when reliance on Article 6(1)(f) is not precluded by law

118. When reliance on Article 6(1)(f) GDPR is not precluded by law, controllers should assess on a case-by-case basis whether the envisaged processing meets the three cumulative conditions set out in Article 6(1)(f) GDPR – in line with the methodology described above – before they start processing personal data based on that legal basis for direct marketing purposes. Controllers should therefore ensure that the balancing test is fulfilled, and consider the adoption of appropriate safeguards and mitigating measures.

119. When assessing whether the envisaged processing may be based on Article 6(1)(f) GDPR, it is of essence that controllers ascertain whether the marketing interest pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental freedoms and rights of the data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter, and make sure to respect the "data minimisation" principle enshrined in Article 5(1)(c) GDPR.[144] Moreover, to make sure that the balancing test is fulfilled, controllers may have to implement appropriate safeguards and mitigating measures, such as using privacy-enhancing technologies. The scale of the processing at issue, as well as its impact on the data subject (notably on their rights and freedoms) must also be taken into account.[145]

120. Certain marketing practices can be considered intrusive from the perspective of the data subject, notably if they are based on extensive processing of potentially unlimited data.[146] In this respect, it should be noted that the level of intrusiveness of the envisaged marketing practices can be a particularly relevant factor to be taken into account when carrying out the balancing test under Article 6(1)(f) GDPR. For example, the balancing test would hardly yield postive results for intrusive profiling and tracking practices for marketing purposes, for example those that involve tracking individuals across multiple websites, locations, devices or services.[147] Conversely, it may be easier for controllers to justify relying on Article 6(1)(f) GDPR with respect to less intrusive marketing activities, for example in the context of an advertising campaign consisting in sending the same commercial communication (e.g., a catalogue of products) to all existing customers who have already bought products similar to those that are advertised.

[142] Ibid., para. 22.

[143] It should be noted that Art. 13 ePrivacy Directive only governs the sending of unsolicited direct advertising messages but not other processing, such as for instance, the collection of personal data for the purpose of sending direct advertising messages. Nevertheless, if sending direct advertising messages is not permitted under the national law implementing Art. 13 ePrivacy Directive, there would be no legitimate interest that the controller could invoke in order to justify the collection of personal data for sending such messages.

[144] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v Bundeskartellamt* (ECLI:EU:C:2023:537), para. 121.

[145] Ibid., para. 112 and 116.

[146] Ibid., para. 118.

[147] See WP29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, page 15.

121. As mentioned above in these guidelines, the reasonable expectations of the data subject should also be taken into account when carrying out the balancing test.[148] Relevant factors for the controller to consider with respect to direct marketing include elements such as whether the person receiving the direct marketing is an existing customer, the nature of the products and services the controller wishes to market, and whether it is likely that the data subject would expect to receive direct marketing about such products and services.[149]

4.4. The right to object to processing for direct marketing

122. Where personal data are processed for the purposes of direct marketing, the data subject has a specific right to object to such processing under Article 21(2) GDPR.[150] Contrary to the more general right to object that data subjects enjoy under Article 21(1) GDPR (see paras. 71 and following above), the right to object to processing of personal data for direct marketing purposes pursuant to Article 21(2) GDPR is unconditional and irrespective of the legal basis relied on by the controller. There is no requirement that the data subject provides any reasoning when objecting, as the purpose of the objection is immaterial, and there is no need for any "balancing of interests" to assess whether the objection should be granted.[151] It is enough that the data subject puts forth an objection for the objection to be successful. Therefore, when personal data are processed for direct marking purposes, the controller should always comply with the objections it receives, without having the possibility to continue the processing for such purposes by demonstrating that there are overriding compelling legitimate grounds that justify it. Furthermore, in accordance with Article 12(2) GDPR, the controller should facilitate the exercise of the right to object to direct marketing by allowing the data subject to object at any time in an easy way and free of charge.

5. Processing for internal administrative purposes within a group of undertakings

123. According to Recital 48 GDPR, controllers that are part of a group of undertakings may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data.[152] Therefore, this kind of processing may find its legal basis in Article 6(1)(f) GDPR, provided that the necessity and balancing tests have been appropriately carried out and have yielded positive results. In other words, the transmission of personal data within a group may not necessarily always find its justification in Article 6(1)(f), but Recital 48 may be taken into account, in particular in the context of the first step of the Article 6(1)(f) three-step assessment (see paras. 14 and following above). It should also be noted that whether the entities that wish to transmit personal data within the group qualify as controllers should be assessed on a case-by-case basis, as not all undertakings in a group would necessarily qualify as controllers.[153]

124. In addition, it should be borne in mind that when such processing takes place, and especially when it concerns the personal data of employees, controllers should give due regard to the specific rules regarding the processing of personal data in the employment context that Members States have provided in

[148] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v Bundeskartellamt* (ECLI:EU:C:2023:537), para. 117; CJEU, judgment of 4 October 2024, Case C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), para. 55.

[149] See Recital 47 GDPR.

[150] See also Recital 70 GDPR.

[151] WP29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01), p. 19.

[152] Article 4(19) GDPR defines "group of undertakings" as "a controlling undertaking and its controlled undertakings".

[153] See further EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, Adopted on 02 September 2020.

accordance with Article 88 GDPR,[154] in particular as they may include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights with particular regard to the transfer of personal data within a group of undertakings.[155] Such national rules may also have an impact on the legal basis that may be relied on to transmit personal data within a group of undertakings, as the rules may envisage specific legal obligations or contractual arrangements, thus enabling reliance on Article 6(1)(c) or (b) GDPR.

125. It must be noted that regardless of the legal basis for the transmission of personal data within the group, employers should always ensure that they meet their obligation to provide employees with the required information about the processing activities affecting their personal data in accordance with Articles 12, 13 and 14 GDPR. Therefore, employees should be given adequate information about the transmission of their personal data within the group, including on the legal basis for such processing, as required by Articles 13(1)(c) and 14(1)(c) GDPR.

Example 7:

To improve services within their corporate group, the headquarters of such group decide to make statistics on how long clients of their subsidiaries have actually been clients, if they have raised complaints about a subsidiary during this period, etc. This is to enable the group to assess if organisational changes need to be made to better retain clients in the future. To be able to do so, certain information about the clients is shared by the subsidiaries with the group's headquarters. As this processing by the company's headquarters is not directly linked to the contractual relationship with the clients, such processing of personal data may be based – depending on the concrete circumstances and subject to compliance with other provisions of the GDPR – on Article 6(1)(f) GDPR.

6. Processing for the purpose of ensuring network and information security

126. Measures to ensure an appropriate level of network and information security may entail processing of personal data. Such processing activities may, in principle, be based on Article 6(1)(f) GDPR, provided that its conditions (including the necessity and balancing tests) are complied with. This was acknowledged – although indirectly – by the CJEU in *Breyer*,[156] as well as in Recital 49 GDPR, and in Recital 121 of Directive (EU) 2022/2555.[157]

127. When assessing whether Article 6(1)(f) GDPR may be relied on, one should bear in mind that:

– The collection and analysis of personal data for the purposes of ensuring a high level of network and information security must meet both the necessity and balancing tests. This implies that the objective of

[154] For an overview of the rules that Member States have adopted in accordance with Article 88 GDPR, see EU Member States notifications to the European Commission under the GDPR, available at: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu/eu-member-states-notifications-european-commission-under-gdpr_en.

[155] See Article 88(2) GDPR.

[156] See CJEU, judgment of 19 October 2016, Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland* (ECLI:EU:C:2016:779). The underlying dispute concerned the processing of (dynamic) IP addresses for ensuring the general operability of online media and the CJEU held Article 7(f) of Directive 95/46/EC including its balancing test should be applicable to such processing.

[157] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

security cannot justify an excessive processing of personal data. In this regard, the WP29 stressed in previous Opinions the risks inherent in certain security solutions (including firewalls, anti-virus and anti-spam), as they may lead to the large scale deployment of deep packet inspection and other kinds of intrusive analysis of communication content and meta data, which may have a significant impact on the outcome of the balancing test.[158]

– In *Meta v. Bundeskartellamt*,[159] the CJEU found that it has to be ascertained whether and to what extent the processing of personal data collected from sources outside a social network is actually necessary to ensure that the internal security of that network is not compromised. It should also be verified whether the legitimate interest pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental freedom and rights of the data subjects, and whether the data minimisation principle enshrined in Article 5(1)(c) GDPR has been observed.

– Information security also covers operational risks different from the protection of personal data and that are therefore not covered by the GDPR, for example the protection of trade and business secrets which is mandated by other sectoral rules.

128. As already recognised by the WP29,[160] other legal bases such as compliance with a legal obligation (under Article 6(1)(c) GDPR) or performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (under Article 6(1)(e) GDPR) may also be relied on in an information security context where their conditions are met.

7. Transmission of personal data to competent authorities

7.1. Indicating possible criminal acts or threats to public security to competent authorities

129. According to Recital 50 GDPR, "indicating possible criminal acts or threats to public security and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal acts or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller". The reference to "individual cases" and "same criminal acts or threats" suggests that the generalised and preventive collection of personal data by private business operators to systematically report possible criminal acts or threats to law enforcement authorities is not what is envisaged by Recital 50 as a legitimate interest pursued by the controller. In any event, such transmission should be prohibited if the processing is incompatible with legal, professional or other binding obligation of secrecy of the controller.

130. In the view of the EDPB, since Recital 50 refers to the purpose limitation principle outlined in Article 6(4) GDPR, the aim of this statement is not only to explain that the processing described in that Recital should be regarded as pursuing a legitimate interest. Its aim is also to clarify that, if the personal data were originally lawfully collected for different purposes and the controller wishes to process them for new purposes (e.g., sharing information with law enforcement authorities), this further processing can often be considered as compatible with the original purpose.

131. It should be noted, however, that in *Meta v. Bundeskartellamt* the CJEU found that, in principle, collecting and sharing personal data with law enforcement authorities in order to prevent, detect and prosecute

[158] See WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (844/14/EN- WP217), section III.3.4., page 39.
[159] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 119 and following.
[160] See WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, of 9 April 2014, section III.2.3. and section III.2.5.

criminal offences is not an objective that is capable of constituting a legitimate interest pursued by a private business operator whose activity is essentially economic and commercial in nature. Therefore, such an operator would generally be unable to rely on such a legitimate interest, which is unrelated to its economic and commercial activity, to process personal data for that purpose on the basis of Article 6(1)(f) GDPR. Conversely, a private business operator may share information with law enforcement authorities on the basis of Article 6(1)(c) GDPR, provided that that processing is necessary to comply with a specific legal obligation to which that operator is subject.[161]

132. However, if the controller does not collect and store personal data in a preventive and systematic manner specifically to be able to provide such data to law enforcement authorities,[162] but rather wishes to report to law enforcement authorities possible criminal acts or threats it may occasionally become aware of, it may consider relying on Article 6(1)(f) GDPR to share information with law enforcement authorities, also in light of Recital 50 GDPR.

Example 8:

A controller is victim of a cyber-attack resulting in a personal data breach that is likely to result in a risk to the rights and freedoms of the data subjects whose data have been leaked. In accordance with Article 33 GDPR, the controller notifies without undue delay the personal data breach to the supervisory authority, including some personal data necessary to determine the level and likely consequences of the personal data breach. By doing so, the controller is processing data to comply with a legal obligation to which it is subject, on the basis of Article 6(1)(c) GDPR. However, the attacked controller is also in possession of other personal data in relation to the cyber-attack and its perpetrators, such as IP addresses and online identifiers. The controller may want to share these data with the law enforcement authority competent in the area of cybercrime and the competent authority responsible for cybersecurity,[163] where such notification is not already compulsory under national and or Union law,[164] to help prevent potential future cyber-attacks and thus protect data subjects. This processing could be based on Article 6(1)(f) GDPR if, in each specific case, it is necessary and the legitimate interest pursued by the controller to indicate possible criminal acts or threats to public security is not outweighed by the interests and rights and freedoms of concerned data subjects. The processing must also be compatible with legal, professional or other binding obligation of secrecy of the controller.

7.2. Requests from and disclosure to third country authorities

133. Controllers may need to assess whether they have any legal ground to disclose and transfer personal data in response to a request they received from a third country authority. Such request may be originating, for example, from a third country law enforcement authority or a public administration requiring the transmission of personal data from the controller.

[161] See CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 124 and 132.

[162] Such activities may possibly be based on Article 6(1)(c) GDPR. See CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 132.

[163] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[164] Such as under Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol), amended by Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022. In cases where the disclosure of personal data is expressly required by Union or Member State law, Article 6(1)(c) will be the appropriate legal basis for such a disclosure.

134. The controller must first analyse the context and legal framework of the request. If it results from the implementation of an international agreement, which makes such request binding and enforceable under EU or Member State law, the disclosure may be mandatory and, thus, constitute a legal obligation under Article 6(1)(c) GDPR.[165] In such cases, there is no need to assess whether the processing may rely upon Article 6(1)(f) GDPR as a legal basis. Similarly, in situations where disclosure based on an international agreement is not mandatory, but such cooperation is permitted under EU or Member State law, Article 6(1)(e) GDPR could apply. Furthermore, in specific cases, the vital interests of the data subject (or another natural person)[166] may justify the reply to a request from a third country authority, provided that the conditions set out in international law are met and, thus, Article 6(1)(d) GDPR could be applicable. [167]

135. A controller could nevertheless have a legitimate interest in complying with a request to disclose personal data to a third country authority, in particular if the controller is subject to third country legislation and non-compliance with such request would entail sanctions under foreign law.

136. However, as recalled above,168 any processing based on a legitimate interest pursued by the controller must also be necessary and balanced against the interests or fundamental rights and freedoms of the data subjects. In this context, it can be noted that the EDPB, in a specific situation, has previously taken the view that the interests or fundamental rights and freedoms of the data subject, under those particular circumstances, would override the controller's interest in complying with a request from a third country law enforcement authority in order to avoid sanctions for non-compliance.[169]

137. Finally, it should be kept in mind that replying to a request by transmitting personal data to an authority outside the EU/EEA constitutes a transfer to a third country. In any case of transfer to a third country, the controller must not only have a legal basis for the processing, but also comply with the provisions of Chapter V, including ensuring that there is a ground for transfer and that the level of protection afforded by the GDPR will not be undermined.

[165] Note that if such international agreement provides for appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available, the controller may also rely on this instrument as a tool for transfer under Article 46(2)(a) GDPR.

[166] Note that, as follows from Recital 46 GDPR, processing of personal data based on the vital interest of *another natural person* should in principle take place only where the processing cannot be manifestly based on another legal basis.

[167] For instance, this could be the case with respect to requests to access personal data concerning abducted minors or other situations where the disclosure is in the vital interest of the data subjects themselves.

[168] See Section B and C in these guidelines.

[169] See the annex to the EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection.