



The Hamburg Commissioner for Data Protection and Freedom of Information

January 8, 2026

Three-step legitimate interest assessment

Legitimate interest pursuant to Article 6(1)(f) of the GDPR (General Data Protection Regulation) is one of the six legal bases provided for by the GDPR for the lawful processing of personal data. This central and at the same time challenging legal basis should neither be selected prematurely for rare or unexpected cases in which other legal bases for processing personal data could apply, nor should it be applied simply because it appears to be less restrictive than other legal bases. While the GDPR does contain examples of legitimate interests, there is no exhaustive list, and controllers are obliged to always carefully examine and document in each specific case whether the conditions for a legitimate interest are met.

In order for data processing to be based on legitimate interest, three conditions must be cumulatively fulfilled:

- There must be a legitimate interest.
- The processing of personal data must be necessary to pursue this interest.
- The interests or fundamental rights and freedoms of the data subject must not outweigh this interest.

Because the legislator has phrased this legal base in an open manner, there are often uncertainties and questions: When is there actually a legitimate interest? How should the necessary balancing of interests be carried out? And how can it be documented in a comprehensible manner that the rights and freedoms of the data subjects do not outweigh this interest?

In order to provide practical guidance to controllers, data protection officers, and all interested parties, we are making this questionnaire for a legitimate interest assessment available as a resource. It is based on the European Data Protection Board's (EDPB) "Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR" and follows its recommendations for the data protection-compliant application of legitimate interest as a legal basis. The questionnaire is intended to help systematically review the requirements for legitimate interest and to document the essential aspects of the balancing of interests in a comprehensible manner. It is aimed in particular at practitioners who regularly face the challenge in their daily work of basing the permissibility of data processing on this legal basis before starting the respective processing operations.



The balancing of interests should be carried out objectively, taking into account both one's own interests and those of third parties, as well as the interests of the data subjects. If there are doubts or if the interests of the data subjects may prevail, the technical and organizational measures should be reviewed and it should be ensured that the principles of the GDPR are consistently implemented.

It is not always necessary to answer all the questions in this guide in detail and down to the smallest detail. Rather, it always depends on the specifics of the individual case. Depending on the complexity and sensitivity of the data processing, it may be useful to examine individual aspects in more detail or to consult additional sources.

With this guide, we aim to create transparency and strengthen the traceability of decision-making – both for controllers and for data protection supervisory authorities. The publication is intended to contribute to clarifying the legal framework and supporting the practical application of legitimate interest.

For a well-founded and legally secure assessment, we recommend that you also consult other relevant sources, such as the EDSA's "Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR" and the current case law of the European Court of Justice (ECJ) when conducting your review. This guide does not claim to be complete, up-to-date, or a substitute for legal advice. For binding information or specific legal questions, it is recommended that you consult a qualified legal advisor.

This guide serves to document the balancing of interests pursuant to Art. 6 (1) (f) GDPR and can be used or submitted to the Hamburg Commissioner for Data Protection and Freedom of Information or other parties as evidence of a comprehensive balancing of interests.



Assessment for determining legitimate interest

Before beginning data processing on the basis of legitimate interest within the meaning of Art. 6 (1) (f) of the General Data Protection Regulation (GDPR), controllers must carefully check and document whether all three necessary conditions of this legal basis are cumulatively fulfilled.

Information on data processing

Controller:

Description of data processing:

Data concerned:

Date and name of the processor:



1. Legitimate interest

"In order for processing to be based on Art. 6 (1) (f) GDPR, a legitimate interest must be pursued."

First, a "legitimate interest" must be identified by the controller or a third party. The "interest" in this first step of the assessment is the broader interest or benefit that a controller or third party may have in a particular processing activity. In principle, a wide range of legal, factual, economic, or idealistic interests can be considered legitimate.

Note: As the controller, you are obliged to inform the data subject about the legitimate interests.

Stage	Question	Context/Note/Examples	Documentation/Answer
1.1	What is the interest in the processing activity?	This refers to the general benefit expected from the processing activity. <i>Example: "Marketing of products"</i> Recitals 47 to 49 of the GDPR contain examples of legitimate interests.	
1.2	What is the specific purpose of the planned processing?	This refers to the objective/specific reason for the planned data processing. <i>Example: "Direct advertising to own customers by postal mail (e.g., an advertising catalog) "</i>	



1.3	Who is pursuing the interest?	Art. 6 (1) (f) GDPR covers own and third-party interests. A "third party" is a natural or legal person, public authority, agency, or other body other than the data subject, the controller, the processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data, Art. 4 No. 10 GDPR.	
1.4	Is the interest legitimate and does it not violate applicable law?	Interests that violate applicable EU/Member State law are not legitimate.	
1.5	Is the interest clearly and precisely formulated?	The scope of the legitimate interest pursued must be clearly defined so that it can be weighed against the interests and fundamental rights of the data subject in the third stage.	
1.6	Is the interest real and present (not speculative)?	Speculative or hypothetical interests cannot be properly assessed and therefore cannot justify data processing. <i>Example: "Data retention for future and as yet unspecified business ideas."</i>	



2. Necessity

"Necessity of processing for the purposes of the legitimate interests pursued"

Here, it must be examined whether the purpose of data processing can also be achieved with less data or in a less intrusive manner. The processing must be compatible with the principle of data minimization specified in Article 5(1)(c) GDPR.

Note: The data processed should be relevant to the purpose to be achieved and limited to what is necessary. If there are other means by which the interests of data processing can be achieved just as effectively and which are less restrictive of the fundamental rights and freedoms of the data subjects, these should be used.

2.1	Is processing absolutely necessary to achieve the interest, or are less intrusive means also possible?	There must be no less intrusive means available. Alternatives must be examined. <i>Example: "Anonymization, pseudonymization, synthetic data instead of real data, etc."</i>	
2.2	Is the data to be processed limited to what is necessary?	The principle of data minimization must be observed. (Art. 5 (1) (c) GDPR) Only data that is adequate, relevant, and necessary for the specific purpose may be processed. In particular, the processing of sensitive data (Art. 9 GDPR) is only permitted in narrowly defined exceptional cases regulated by law (Art. 9 (2) GDPR).	



2.3	Is the number of data subjects limited to the minimum necessary to achieve the purpose?	<i>Example: "Limiting the number of data records, sampling instead of full surveys, anonymization, etc."</i>	
2.4	Is data processing carried out on a one-off or ongoing basis?	In the case of ongoing processing, the necessity must be permanent. A legitimate interest that has been established once does not automatically justify ongoing data processing (see also section 2.6).	
2.5	Are all processing steps necessary for the purpose, or can individual steps be omitted?	The processing steps must be considered and evaluated individually.	



2.6	Is there a deletion concept? Is the storage period defined?	<p>Is a process for continuous data protection management evaluation established (Art. 32 GDPR)?</p> <p>Personal data may only be stored for as long as it is necessary for the intended purpose (Recital 39 and Art. 17(1)(a) GDPR). Once the purpose no longer applies, there is a general obligation to delete the data.</p> <p>On the other hand, there are statutory retention periods, e.g., from the German Commercial Code (HGB), the German Fiscal Code (AO), the Income Tax Act (EStG), social security law, or the Trade Regulation Act. The storage period should be documented for each data category and automated deletion processes should be in place.</p>	
2.7	Is there an overview of existing and planned data flows?	<p>The data flow must also be comprehensible and transparent for third parties. A data flow diagram serves for your own illustration and accountability and illustration to management, customers, data subjects, supervisory authorities, etc.</p>	



3. Balancing of interests

"Do the interests, fundamental freedoms, and rights of the data subjects outweigh the legitimate interests of the controllers?"

Here, it must be examined whether the legitimate interest examined in Number 1 and 2 is not overridden by the interests or fundamental rights and freedoms of the data subject. This requires a balancing of the conflicting rights and interests, which generally depends on the specific circumstances of the individual case of the planned processing. The assessment must take into account the nature of the personal data, the reasonable expectations of the data subjects, the possible effects of the data processing, and the processes and protective measures in place.

Fundamental rights, freedoms, and interests of the data subjects

3.1	Which fundamental rights of the data subjects are affected?	Right to privacy, data protection, non-discrimination, freedom and security, freedom of expression and information, freedom of thought, conscience, and religion, freedom of assembly and association, prohibition of discrimination, right to property, or right to physical and mental integrity, among others.	
3.2	Are the fundamental freedoms of the persons concerned affected?	Free movement of goods, freedom of movement for workers, freedom of establishment, freedom to provide services, free movement of capital and payments under the TFEU.	



3.3	Are the "interests" of the persons concerned taken into account in addition to fundamental rights and freedoms?	<p><i>All interests that could be affected by the processing in question.</i></p> <ul style="list-style-type: none"> • <i>Financial interests: e.g., protection against impacts on investments, earning opportunities, retirement provisions, credit ratings, and insurance coverage.</i> • <i>Social interests: e.g., protection of the social sphere, damage to reputation, discrimination, unwanted contact</i> • <i>Personal interests: e.g., protection of intimacy and privacy through the processing of data relating to a person's sex life or sexual orientation</i> 	
Type of personal data			
3.4	What type of data is to be processed?	In what capacity are the persons affected? <i>E.g.: "in their personal or professional capacity"</i>	



3.5	Does this involve special categories of personal data (Art. 9 GDPR)?	<p>This sensitive data includes, in particular:</p> <ul style="list-style-type: none"> • ethnic origin and race • political opinions • religious or philosophical beliefs • trade union membership • genetic and biometric data (e.g., fingerprints) • Health data • Data concerning a person's sex life or sexual orientation <p>If this data is processed, the potential interests of the data subjects are given high priority in the balancing of interests. In addition, the requirements of Art. 9 (2) GDPR must be met.</p> <p>Even if an exception under Article 9(2) GDPR applies, the balancing of interests under Article 6(1)(f) GDPR may still be in favor of the interests of the data subject (see ECJ ruling of December 21, 2023 (Ref. C-667/21)).</p>	
3.6	Does the data relate to children?	<p>In all data processing measures concerning children, the best interests of the child must be a primary consideration. All rights must be taken into account here, not just data protection rights, cf. Recital 38 to the GDPR.</p>	



3.7	Does the data relate to criminal convictions and offenses pursuant to Art. 10 GDPR?	Art. 10 GDPR Data (e.g., "a certificate of good conduct") is also particularly sensitive. Processing should only take place under official supervision or if it is permitted under Union or national law.	
3.8	Is it private data?	Some data is considered particularly sensitive or private by data subjects, even if it is not specifically listed in Art. 9 GDPR or Art. 10 GDPR. <i>Example: "Financial, location, or family data."</i>	



Reasonable expectations of the data subjects (Recital 47(1) of the GDPR)			
<i>Can the data subject reasonably foresee, at the time the personal data is collected and in view of the circumstances in which it is collected, that it may be processed for the intended purpose?</i>			
3.9	Where and when is the data collected?	An indication in favor of the data subject exists if the data is used for a completely new, unrecognizable purpose or for a purpose that goes beyond the original purpose and the data subject could not reasonably have expected the data to be processed at the time of collection (see also Art. 6(4) GDPR).	
3.10	How is the data collected?	What technologies and methods (e.g., "online surveys, competitions, web scraping, AI, etc.") are used? Are these practices generally known and transparent to the data subjects?	
3.11	How is data processing made transparent to the data subjects?	The information requirements under Articles 13 and 14 of the GDPR must be observed. This information must be provided immediately upon data collection. Otherwise, the lawfulness of the processing fails due to a lack of transparency.	



3.12	Is there a relationship with the data subjects?	If a relationship already exists between the data subject and the controller, this increases the predictability of data processing, Recital 47(2) of the GDPR. <i>Example: "the data subject is already a customer of the controller."</i>	
Likely impact of processing on data subjects			
3.13	How extensive is the data collection and how many individuals are affected?	The greater the scope of data processing, the higher the risk of affecting the rights and interests of the data subjects.	
3.14	What are the possible negative effects of the processing on data subjects?	How likely and serious are the potential effects? Has a data protection impact assessment or threshold test been carried out?	
3.15	Are there any positive effects of the processing on data subjects?	Is the processing in the objective, presumed interest of the data subject? E.g., <i>time savings, monetary benefits.</i>	
3.16	Do the individuals concerned lose control over the use of their personal data?	Are there safeguards in place to minimize the impact? Can the individuals concerned take safeguards themselves, if necessary?	



3.17	Who processes the data? How many people have access?	What qualifications do the persons/companies processing the data have? Is the data treated confidentially? Are there access restrictions within the meaning of Art. 32 (4) GDPR?	
3.18	Does automated decision-making take place in accordance with Art. 22 GDPR?	<p>Pursuant to Art. 22(2) GDPR, the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.</p> <p>If such data processing takes place, the possible interests of the data subjects are given high priority in the balancing of interests. In addition, the requirements of Art. 22(2) GDPR must also be met.</p> <p>Even if an exception under Art. 22(2) GDPR applies, the balancing of interests under Art. 6(1)(f) GDPR may still be in favor of the interests of the data subject.</p>	



Measures and processes for data protection			
3.19	Is the balancing of interests within the meaning of Article 6(1)(f) GDPR explained when providing information within the meaning of Article 15 GDPR?	<p>The controller should provide the data subject with information on the balancing of interests within the meaning of Art. 6 (1) (f) GDPR before collecting personal data. In order to avoid overwhelming the data subject with too many details, it is advisable to provide this information in a multi-level privacy policy or notice. It is important to inform the data subject that they can obtain this information at any time upon request.</p> <p>In addition, the controller should in any case provide the information in response to a request for information pursuant to Art. 15 GDPR.</p>	
3.20	What options for objection or rights of intervention do data subjects have? Is there an opt-out option for them? What requirements are there for justifying the objection?	Article 21 GDPR grants data subjects the right to object. The objection is not subject to any formal requirements.	



3.21	Is there an established process for complying with an objection to the planned processing or a request for erasure?	Following an objection (Art. 21 GDPR) or a request for erasure (Art. 17 GDPR), personal data may not be further processed unless there are specific exceptions or compelling reasons. To this end, the controller must carry out a new assessment and document it. In the case of direct marketing, an objection to advertising must be implemented immediately, even without justification.	
3.22	Is there a process for complying with the right to rectification within the meaning of Art. 16 GDPR?	The data subject has the right to request the controller to rectify inaccurate personal data concerning them without delay.	
<p>Final result of the balancing of interests: After weighing up all factors, do the legitimate interests of the controller or third parties outweigh the interests of the data subjects?</p>			
<p><i>Please enter the overall result here, taking all of the above points into account:</i></p>			



4. Documentation/compliance			
<i>"Document the result of the balancing of interests!"</i>			
4.1	Please document these answers and the result of your assessment.	The accountability requirement under Article 5(2) GDPR obliges the controller to be able to demonstrate compliance with data protection principles.	
4.2	Has the assessment been reviewed by data protection officers or independent bodies?	Internal approval processes strengthen legal certainty.	
4.3	Is there a process for regularly reviewing and updating the assessment?	It is necessary to adapt to changing circumstances.	