IMY. Integritetsskydds myndigheten

Guidance on impact assessment

Legal interpretative support

Annex to *A practical guide*

February 2025

IMY. Guidance on impact assessment - Legal interpretative support
If you have questions about the content, please contact the Swedish Authority for Privacy Protection, telephone 08-657 61 00, e-mail imy@imy.se,
or visit www.imy.se

Contents

1. Responsibility for the impact assessment

The controller[1] is ultimately responsible for ensuring compliance the requirements of the GDPR[2] and other data protection legislation. This follows from the principle accountability expressed in Article 5(2) of the GDPR.
This responsibility also includes implementing appropriate technical and organizational measures and ensuring a level of security appropriate to the risk to the rights and freedoms of natural persons posed by the processing.

The controller shall ensure that a data protection impact assessment is carried out where it is mandatory, and that it is carried out and followed up in an acceptable manner. The person or persons who actually carry out the impact assessment itself, or any actions resulting from it, may be persons inside or outside the organization.

Any *processor*[3] shall assist the controller in ensuring that the obligation to carry out a pursuant to Article 35 of the GDPR is fulfilled, taking into account the type of processing and the information available to the processor.[4] The responsibility of the processor shall be regulated in the processor agreement.

The controller is also responsible for ensuring that *the DPO*, if any, is provided with accurate and sufficient information about the processing and the process in order to perform his or her tasks under the GDPR.

In-depth information

Section 6. Role of the DPO in the impact assessment

1 According to Article 4(7) of the GDPR, a controller is a natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data.
2 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 (General Data Protection Regulation).
3 According to Article 4(8) of the GDPR, a processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
4 Article 28(3)(f) of the GDPR.

2. Methodology and documentation

There are certain explicit requirements that the controller must meet when carrying out an impact assessment and certain minimum requirements for its content[5].
However, there is no set methodology for conducting an impact assessment. It is therefore up to the controller to choose a methodology that meets the requirements of the GDPR, based on, for example, type of processing involved and the activity carrying out the processing.

The European Data Protection Board (EDPB) has stated that there is flexibility in the "exact structure and form" of DPIAs, but that a DPIA should always (regardless of its form) be a genuine risk assessment that enables controllers to take measures to manage the risks[6]
The EDPB has developed criteria in Annex 2 of its guidelines on DPIA that can be used by controllers to assess whether a DPIA, or a methodology for conducting a DPIA, is sufficient to meet the requirements of the GDPR. The EDPB considers that the methodology chosen should be consistent with these criteria.[7] IMY's DPIA guidance and suggested approach is consistent with the requirements of the GDPR and with the EDPB's criteria. Such methodological support developed in accordance with industry practice may also be useful to adapt the impact assessment to the industry specificities of the activity.

There are no specific requirements on how detailed the documentation of the impact assessment should be. It must be adapted to the circumstances of the case, such as the processing in question, the organization's resources and existing processes. Under the accountability principle, the controller must be able to demonstrate compliance with the GDPR. This means that the impact assessment must be documented in an acceptable manner. The documentation should be done in a way that enables the supervisory authority to verify that the minimum requirements of Article 35 of the GDPR have been met and that other provisions, which are relevant in the context of the individual impact assessment, are complied with.

5 Cf. Article 35(2), 7-9 of the GDPR. Recital 90 of the GDPR.
6 Article 29 Working Party *Guidelines on data protection impact assessment and determining whether processing is "likely to result in a high risk"* within the meaning of Regulation 2016/679 (WP 248, rev. 01), p. 19.
7 See WP 248, p. 22.

3. Article 35 in the data protection-regulation

The provisions on data protection impact assessment are contained in Article 35 of the GDPR. The article is reproduced in full below.

Article 35 Data protection impact assessment

1. Where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, in particular with the use of new technologies, taking into account its nature, scope, context and purposes, the controller shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data prior to the processing. A single assessment may cover a series of similar processing operations presenting similar high risks.

2. The controller shall consult the DPO, if appointed, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall be required in particular in the following cases

   a) A systematic and extensive evaluation of personal aspects relating to natural persons, based on automated processing, including profiling, on which decisions are based that produce legal effects concerning natural persons or similarly significantly affect natural persons.

   b) Processing on a large scale of special categories of data, as referred to in Article 9(1), or of personal data relating to criminal convictions and offences, as referred to in Article 10.

   c) Systematic monitoring of a public place on a large scale.

4. The supervisory authority shall establish and make public a list of the type of processing operations subject to the requirement of a data protection impact assessment in accordance with paragraph 1. The supervisory authority shall transmit those lists to the Board referred to in Article 68.

5. The supervisory authority may also draw up and publish a list of those processing operations which do not require a data protection impact assessment. The supervisory authority shall transmit those lists to the Management Board.

6. Before adopting the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such a list involves processing operations relating to the offering of goods or services to data subjects, or to the monitoring of their behavior in several Member States, or which could substantially affect the free movement of personal data within the Union.

7. The assessment shall include at least

   a) a systematic description of the planned treatment and its objectives including, where appropriate, the legitimate interest of the controller,

   b) an assessment of the need for and proportionality of the treatment in relation to to the objectives,

   c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

   d) the measures envisaged to address the risks, including safeguards, security measures and procedures to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. The compliance of the controllers or processors concerned with the approved codes of conduct referred to in Article 40 shall be taken into account, as appropriate, when assessing the impact of the processing operations carried out by those controllers or processors, in particular for the purposes of developing a data protection impact assessment.

9. The controller shall, where appropriate, seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing.

10. Where processing under Article 6(1)(c) or (e) has a legal basis in Union law or in the national law of a Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply, unless Member States consider it necessary to carry out such an assessment prior to the processing.

11. The controller shall carry out a review, where necessary, to assess whether the processing is carried out in accordance with the data protection impact assessment at least when the risk posed by the processing changes.

The reasons for Article 35 of the GDPR

The recitals of the GDPR are important in interpreting its provisions. The recitals of the GDPR that specifically address impact assessments are recitals 89-94.

(89) Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. This obligation imposed administrative and economic burdens, but did not always improve the protection of personal data. Such horizontal and general notification obligations should therefore be abolished and replaced by effective procedures and mechanisms that instead focus on the types of processing operations that are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. These processing operations may be those which, in particular, involve the use of new technologies or are of a new type, for which a data protection impact assessment has not previously been carried out by the controller, or which become necessary due to the time that has elapsed since the initial processing operation.

(90) In such cases, the controller should, before processing, taking into account the nature, scope, context and purposes of processing and the origin of the risk, carry out a data protection impact assessment in order to assess the specific likelihood and severity of the high risk and its origin. The impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged to mitigate that risk, to ensure the protection of personal data and to demonstrate compliance with this Regulation.

(91) This should apply in particular to large-scale data processing operations intended to process a significant amount of personal data at regional, national or supranational level, which could affect a large number of data subjects and are likely to present a high risk, for example due to the sensitive nature of the data, where, in accordance with the level of technical knowledge achieved, a new technology is used on a large scale, and to other processing operations presenting a high risk to the rights and freedoms of data subjects, in particular where such processing makes it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be carried out where personal data are processed for the purpose of taking decisions relating to specific natural persons following a systematic and extensive assessment of the personal aspects of natural persons on the basis of profiling of those data or following processing of special categories

of personal data, biometric data or data relating to criminal convictions, offences or related security measures. Similarly, a data protection impact assessment is required for large-scale surveillance of public places, in particular when using optical-electronic devices, or for any other processing where the competent supervisory authority considers that the processing is likely to
will pose a high risk to the rights and freedoms of data subjects, in particular because it prevents data subjects from exercising a right or using
a service or contract or because it is systematically carried out on a large scale. Processing of personal data should not be considered as large-scale if it concerns personal data of patients or clients processed by individual doctors, other health professionals or legal representatives. In these cases, a data protection impact assessment should not be mandatory.

(92) Sometimes it may be sensible and economical for a DPIA to focus on a broader area than a single project, for example when authorities or bodies intend to create a common application or processing platform or when several controllers plan to implement a common application or processing environment for an entire industry or segment or for a widely used horizontal activity.

(93) Member States may consider it necessary to carry out such a pre-processing assessment in the context of the adoption of Member States' national law underlying the performance of the tasks of the authority or public body and regulating the specific processing operation or set of operations concerned.

(94) Where a data protection impact assessment indicates that, without safeguards, security measures and risk mitigation mechanisms, the processing will result in a high risk to the rights and freedoms of natural persons, and the controller considers that the risk cannot be mitigated by measures that are reasonable in terms of the available technology and the costs of implementation, the supervisory authority should be consulted prior to the start of the processing. Such a high risk is likely to be caused by certain types of processing and by a certain scope and frequency of the processing, which may also result in damage to or infringement of the rights and freedoms of natural persons. The supervisory authority should respond to a request for consultation within a specified time; however, a failure by the supervisory authority to respond within that time should not prevent possible intervention by the supervisory authority in accordance with its tasks and powers under this , including the power to prohibit processing. As part of that consultation process, the results of a data protection impact assessment carried out with regard to the processing in question may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

Read more:

The recitals of the GDPR that specifically address risk are recitals 75-77

4. Support in assessing whether to carry out an impact assessment

4.1 Interpreting Article 35(1) of the GDPR

Article 35(1) of the GDPR contains a provision on *when* the controller must carry out a DPIA. However, the article cannot be interpreted solely on the basis of its wording. Under the EU law method of interpretation, provisions must also be interpreted, inter alia, in the light of the objectives pursued by them and the context in which they are used, and concepts must often be given an independent and uniform interpretation throughout the Union.[8] The IMY's interpretation of the provision in Article 35(1) of the GDPR.

A type of treatment

When assessing whether a processing operation is a *type of processing* covered by the requirement for a DPIA, controllers shall take into account the factors set out in Article 35(1), the paragraphs of Article 35(3) and the criteria set out in the IMY list under Article 35(4) of the GDPR.

The focus on *the type of processing* means that more processing operations will be subject to DPIA than if the actual planned processing had been determining factor. This is because it is irrelevant (for the purposes of the obligation to carry out a DPIA) that the controller has decided to implement several risk mitigation and effectiveness measures for a given processing operation. In other words: If a planned processing operation is *the type of processing* that requires a DPIA to be carried out, it is irrelevant that, after the implementation of various measures, the processing operation is unlikely to result in a high risk in practice. The measures that can reduce or eliminate the identified risks for the specific processing operation envisaged should only be taken into account when the impact assessment is actually carried out.[9] If the requirement of Article 35(1) of the GDPR had been aimed at the actual processing, many high-risk processing operations would never be subject to an impact assessment. High risks would be more likely to be overlooked.

This interpretation of the concept of *type of processing* is based on the purpose and context of the provision in accordance with the EU law method of interpretation. One of the purposes of the requirement to carry out an impact assessment is to ensure that processing operations that may typically lead to high risks are subject to risk mitigation measures. If circumstances to be considered and documented during the impact assessment itself are already taken into account when asking whether the impact assessment is necessary, the possibilities for ex-post control would be reduced. As regards the context of the provision, it can be noted that both Article 35(4) and (5) contain the concept of "processing operation" and not "a processing operation". This is also to ensure that the concept in Article 35(1) is not equated with the actual processing.

The factors listed are

IMY considers that the factors listed in Article 35(1) of the GDPR should be understood as follows.

- ***Use of new technologies***
  It refers to the use of the latest technologies and technological knowledge, such as artificial intelligence, machine learning and deep learning, autonomous vehicles and intelligent transportation systems, and some Internet of Things applications. It can also involve new and innovative uses of existing technologies. New forms

8 Judgment of the Court of Justice of the European Union of 14 December 2023, C340/21 (Natsionalna agentsia za prihodite), EU:C:2023:986, p. 23 and where
the case law cited.

9 See for a similar reasoning: Ambrock J., Moritz K. (2023), Art. 35 - Data protection impact assessment, p. 692. In: Döhmann I. S., Papakonstantinou V., Hornung G., De Hert P., General Data Protection Regulation - ArticlebyArticle Commentary, pp. 687-705.

of data collection and use often pose a higher risk to individuals' rights and freedoms. This is because the personal and social consequences of using new technologies may be unknown.[10] A DPIA helps data controllers to understand and manage such risks.

Examples of the use of new technologies

A generative AI system that has been trained on large amounts of data and whose behavior has not been extensively analyzed would likely fall under *the use of new technologies* criterion. However, a system that uses AI techniques that are known, well proven and have been analyzed in the past could fall outside the criterion.

- ***Nature of the treatment***
  The term refers to the type of processing, how it is to be carried out and the types of personal data to be processed. Examples of different types of processing are communication, storage and processing. The way in which the processing is carried out may concern, for example, the technology to be used or the practicalities of collecting, using, storing or sharing the personal data. The types of personal data processed include whether the data are sensitive or otherwise privacy-sensitive and whether they relate to vulnerable or particularly vulnerable persons. The latter may include, for example, children, persons with disabilities or individuals who are dependent on the controller.

- ***Scope of the treatment***
  The concept refers to volume of personal data, the number of data subjects, the duration and frequency of the processing and the geographical scope the processing. To clarify the scope of the processing, the controller may ask itself, for example, whether the processing involves a large number of data subjects, whether it involves a large number of personal data relating to each data subject, how long the data will be stored, and how many and who will have access to the data.

- ***The context of treatment***
  The concept refers to the processing in a broader perspective, taking into account various internal and external factors, such as the origin of the data, the controller's relationship with the individuals and the extent to which individuals have control over their data. Other factors to be taken into account are whether individuals can reasonably expect the processing or whether it can be perceived as unpredictable. For example, the controller may ask whether the processing will take place in a particularly trusting context where there is an expectation of confidentiality due to professional secrecy or confidentiality (such as for healthcare professionals, journalists, lawyers, whistleblowing channels, etc.). The context of the processing also includes whether there are relevant codes of conduct or other certification schemes.

- ***Purpose of the treatment***
  The term refers to the actual reason why the controller wants to carry out the processing and the effect it will have on individuals. Sometimes the word purpose is used instead of objective. To clarify the purpose of the processing, the controller may, for example, ask itself what are the expected benefits of the processing for the business or for the data subjects. Purpose of the processing

10 See WP 248, p. 12.

can be more or less privacy-sensitive. For example, if the purpose of a service is to reveal, single out, control or monitor certain individuals, or for data subjects to be profiled in various ways, the purpose of the processing is more privacy-sensitive than if the purpose is to be able to contact customers for a customer satisfaction survey.

Likely to lead to

Likely leads to means an estimate and forecast of how likely it is that something (a certain type of processing) will cause or result in a certain outcome (high risk to the rights and freedoms of natural persons). The case law of the CJEU does not provide further guidance on how to interpret the concept.

High risk

Despite the prominence of the concept of *risk* in the GDPR, it is not explicitly defined in the GDPR. However, the concept is developed in recitals 75-77 of the GDPR. In the EDPB Guidelines on Impact Assessment, risk has been described as "a scenario describing an event and its estimated consequences in terms of severity and likelihood".[11] In interpreting the concept of "risk" under the GDPR, guidance can also be drawn from various international standards on general risk management, such as ISO 3100026.[12]

What is required for a processing operation to present a high risk to the rights and freedoms of individuals is also not explicitly defined in the Regulation. However, guidance can be drawn from the examples given in Article 35(3) of the GDPR, the IMY list under Article
35(4) of the GDPR and the criteria in the EDPB Guidelines on Impact Assessment.

Rights and freedoms of natural persons

Natural persons are the group that constitutes the interest to be protected, and whose rights and freedoms are to be taken into account. Note that it does not say "data subjects". Thus, it is not only the risks to the individuals whose personal data will be processed that must be considered. *Rights and freedoms* refer primarily to the right of natural persons to the protection of their personal data, privacy and integrity, but also to other fundamental rights (e.g. freedom of expression, freedom of thought, freedom of movement, prohibition of discrimination, freedom of conscience and religion)[13]

IMY believes that the concept of "rights and freedoms" should be given a broad interpretation and that most negative effects of various physical, material or non-material harms on an individual's private life should be taken into account in this context.[14] Examples include stigmatization in social contexts, inferior contractual terms on inappropriate grounds, manipulation influencing important decisions, or restriction of communication or freedom of expression through self-censorship. Other examples include identity theft, financial loss and reputational damage[15].

4.2 Interpret Article 35(3)(a) to (c) of the GDPR

The items listed in Article 35(3) of the GDPR are examples of situations where a processing operation *is likely to result in a high risk*[16] and an impact assessment should always be carried out. It is not an exhaustive list. Other processing operations that present similar high risks to those set out in these paragraphs should also be preceded by a DPIA.

11 WP 248, p. 7.
12 See WP 248, p. 5, note 9 and p. 19.
13 See WP 248, p. 7.
14 See recital 75 of the GDPR.
15 See recital 75 of the GDPR.

4. Support in assessing whether an impact assessment should be carried out 16 WP 248, p. 9 f.

The paragraphs of Article 35(3) of the GDPR aim to ensure a consistent interpretation of the situations in which a DPIA is mandatory.[17] However, the fact that the paragraphs are examples does not mean that the obligation to carry out a DPIA is optional in these cases. If the envisaged processing operation falls under one of the examples, the controller is obliged to carry out a DPIA.

Systematic (points a and c)

The GDPR does not contain a definition of the word *systematic*. According to the EDPB however, a *systematic treatment* should be understood as a treatment:

- which takes place according to a system,
- that is pre-arranged, organized or methodical,
- under a general data collection plan, and/or
- carried out as part a strategy[18]

Automatic processing (point a)

Paragraph (a) refers to assessments and decisions that are "based on" *automated processing*, rather than "solely" automated processing. This means that it does not have to be a "fully automated" decision within the meaning of Article 22 of the GDPR for the provision to apply[19].

Legal consequences (point a)

Examples of *legal consequences* referred to in point (a) are the termination of a contract, the refusal of a statutory social benefit or a ban on entry into a country. Examples of 'similarly significantly affecting natural persons' are decisions affecting someone's access to health care, employment opportunities or access to education.[20]

To a large extent (points b and c)

As regards the concept of *substantial scale*, there are no explicit thresholds. However, the EDPB recommends that the following factors be taken into account in particular when assessing whether the processing is carried out on a large scale.

- the number of persons concerned (either as a specific number or as a proportion of the population concerned)
- the amount of data and/or the number of types of data processed
- the duration of treatment
- the geographical scope of treatment[21]

Recital 91 of the GDPR states that the obligation to carry out an impact assessment should apply in particular to large-scale data processing operations aimed at processing significant amounts of personal data at regional, national or supranational level. However, the processing of personal data should not be considered as large-scale if it concerns personal data of patients or clients processed by individual doctors, other health professionals or legal representatives. The EDPB Guidelines on Data Protection Representatives emphasize that there is a large grey area between the extremes mentioned in Recital 91.[22]

17 WP 248, p. 5.
18 Article 29 Working Party *Guidelines on Data Protection Officers* (WP 243, rev 01), p. 11. The EDPB has endorsed the Guidelines, Endorsement 1/2018.
19 Article 29 Working Party Guidelines on automated individual decision-making and profiling under Regulation (EU) 2016/679 (WP 251, rev 01), p. 31.
20 WP 251, p. 22 f.
21 WP 248, p. 11 and WP 243, p. 10.
22 WP 243, note 14.

Controllers must be prepared to justify their assessment in this respect. It is therefore important to make an informed estimate of the amount of personal data to be processed.

Systematic monitoring (point c)

CCTV involving the processing of personal data is typically considered systematic surveillance of people.[23] Another example is surveillance that may be carried out through positioning systems.

A public place (point c)

The EDPB Guidelines on Impact Assessment state that the concept of a public place should be given a broad meaning and include all places accessible to the public, such as squares, shopping malls, streets, markets, train stations and public libraries.[24] Furthermore, it has been stated in the legal literature− with reference to the European Court of Justice's Ryneš judgment[25]− that the concept probably has an EU-wide meaning.[26] The Ryneš judgment shows that the private exception is to be interpreted restrictively and that areas adjacent to a private person's home that partly cover a public road and the entrance to a private home opposite are areas to which the public has access. Taken together, this suggests that the concept has a broad meaning.

4.3 EDPB criteria and IMY list under Article 35(4)

EDPB guidelines on impact assessment

The European Data Protection Board (EDPB) was established with the entry into force of the GDPR in 2018. The EDPB is composed of representatives of the supervisory authorities of the EU Member States and the European Data Protection Supervisor (EDPS). The EDPB has a task, as set out in the GDPR, to ensure the consistent application of the Regulation by issuing guidelines, recommendations and best practices.[27] The EDPB's guidelines are not legally binding.[28]

The EDPB replaced the Article 29 Working Party (Working Party on the Protection of Individuals with regard to the Processing of Personal Data), which was established by Article 29 of the Data Protection Directive.[(29)] In 2017, the Article 29 Working Party adopted *Guidelines on data protection impact assessment and determining whether processing is "likely to result in a high risk" within the meaning of Regulation 2016/679* (WP 248 rev. 01). These guidelines have been endorsed by the EDPB in a decision.[30] The guidelines are important as guidance on DPIAs, supporting both the work of data controllers in complying with the requirements of the Regulation and the activities of supervisory authorities. The Guidelines have also been one of the main sources of this guidance.

23 See definition of "systematic" in WP 243, p. 11 and reference in WP 248, p. 10.
24 WP 248, note on p. 11.
25 Judgment of the Court of Justice of the European Union of 11 December 2014, C212/13 (Ryneš) EU:C:2014:2428, p. 29.
26 Öman S., *The General Data Protection Regulation (GDPR) etc. Commentary on Article 35(3)(c).*
27 Article 70 of the Data Protection Regulation.
28 The Supreme Administrative Court has requested a preliminary ruling from the Court of Justice of the European Union on the question of the legal weight to be given to the EDPB's statements when interpreting the GDPR. On June 13, 2024, the Supreme Administrative Court decided to request a preliminary ruling in case no. 87023 (IMY's case, no. IMY20231305).
29 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
30 EDPB, Endorsement 1/2018.

The Guidelines set out the criteria that the EDPB considers should be taken into account when assessing whether a type of treatment requires an impact assessment. The purpose of these criteria is to provide concrete examples of types of treatments that require an impact assessment due to their 'inherent high risk'[31]

Read more

EDPB Guidelines on data protection impact assessment and determining whether processing is 'likely to result in a high riskwithin the meaning of Regulation 2016/679

IMY's list under Article 35(4) of the GDPR

As a supervisory authority, IMY is responsible, among other things, for enforcing the application of the GDPR and contributing to the consistent application of data protection rules within the EU. This includes, in accordance with Article 35(4) of the GDPR, drawing up and maintaining a list of the types of processing activities covered by the requirement
on an impact assessment. The IMY has decided[32] to establish and publish such a list.[33] The IMY list is based on the criteria set out in the EDPB Guidelines on Impact Assessment.

The purpose of the national lists under Article 35(4) of the GDPR is not to replace the provision of Article 35(1) of the GDPR, but to complement the examples given in Article 35(3) of the GDPR.[34] By further specifying what may constitute "high risk", and providing examples of processing operations that require a consistency assessment to be carried out, the IMY list provides support in the interpretation of the concept.

As a general rule, controllers must carry out a DPIA if a planned processing operation meets at least two of the criteria in the list. The list provides a number of examples of processing operations that meet at least two criteria and where a DPIA must be carried out. It is important to be aware that the list is not exhaustive and that an impact assessment may need to be carried out in an individual case even if only one of the criteria in the list is met.

In some cases, a processing operation may meet two or more of the criteria, or be close to one of the examples, but the controller still considers that it is *unlikely to result in a high risk*. In such cases, the controller should always fully justify and document the reasons for this, and include any comments from the DPO (if one exists).[35]

Read more:

IMY's list under Article 35(4) of the GDPR
IMY's listing decision under Article 35(4) of the GDPR

31 WP 248, p. 10.
32 IMY case number DI-2018-13200.
33 IMY's list under Article 35(4) of the GDPR.
34 It can be noted that the provision of Article 35(1) takes precedence over the national lists under Article 35(4) in the hierarchy of jurisdiction.
35 IMY's list under Article 35(4) of the GDPR.

Criteria in the IMY list under Article 35(4) and EDPB Guidelines

For ease of comparison, each criterion is listed in parallel below.

IMY List of when to carry out an impact assessment under Article 35(4) An impact assessment shall be carried out if the planned treatment meets at least two of the following criteria:	**Criteria to be considered by the EDPB when assessing whether a treatment *is likely to result in a high risk***
1. evaluates or scores people, for example, a company offering genetic tests to consumers to assess and predict disease risks, a credit reference agency or a company profiling internet users	**1. evaluation or scoring, including profiling** and prediction, in particular "aspects relating to the data subject's work performance, financial situation, health, personal preferences or interests, reliability or behavior, location or movements" (recitals 71 and 91). Examples of this could include financial screening their customers against a database for credit reporting purposes or against an anti-money laundering and counter-terrorist financing database, or a biotechnology company offering genetic tests directly to consumers to assess and predict disease/health risks, or a company developing behavioral or marketing profiles based on the use of or navigation on its website.
2. processes personal data for the purpose of taking automated decisions which produce legal effects or similarly significant effects on the data subject	**2. automated decision-making with legal or similarly significant consequences:** processing operations intended to produce decisions regarding data subjects which produce "legal effects concerning natural persons" or "similarly significantly affect natural persons" (Article 35(3)(a)). For example, processing may result in the exclusion or discrimination of individuals. Processing that has little or no impact on individuals does not meet this specific criterion.
3. systematically monitoring people, for example through camera surveillance of a public place or by personal data from internet use in public environments	**3. "Systematic monitoring" means** processing used to observe, monitor or control data subjects, including data collected through networks or "systematic monitoring of a public place" (Article 35(3)(c)). This type of surveillance is a criterion as personal data may be collected in situations where data subjects may not be aware of who is collecting their data or how it will be used. In addition, it may be impossible for individuals to avoid being subject to such processing in public places (or publicly accessible places).

The table continues on the next page.

IMY List of when to carry out an impact assessment under Article 35(4) An impact assessment shall be carried out if the planned treatment meets at least two of the following criteria:	Criteria to be considered by the EDPB when assessing whether a treatment *is likely to result in a high risk*
4. processes sensitive personal data as referred to in Article 9 or data of a highly personal nature, such as a hospital storing patient records, a company collecting location data or a bank handling financial data	**4. sensitive data or data of a highly personal nature:** this includes special categories of personal data as defined in Article 9 (e.g. information on individuals' political opinions) as well as personal data relating to criminal convictions and offences as defined in Article 10. In addition to these provisions of the Regulation, certain categories of data may be considered to increase the potential risk to the rights and freedoms of individuals. Such personal data are considered sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality must be protected), or because they affect the exercise of a fundamental right (such as location data whose collection calls into question the freedom of movement) or because the violation of these rights has unambiguously serious consequences for the daily life of the data subject (such as financial data that could be used for payment fraud). In this respect, it may be relevant whether the data have already been made public by the data subject or by third parties. The fact that the personal data have been made public may be taken into account as a factor in assessing whether the data were expected to be further used for specific purposes. This criterion may also include data such as personal documents, emails, diaries, comments from tablets equipped with commenting features and highly personal information in applications that record activities.

The table continues on the next page.

IMY List of when to carry out an impact assessment under Article 35(4) An impact assessment shall be carried out if the planned treatment meets at least two of the following criteria:	**Criteria to be considered by the EDPB when assessing whether a treatment *is likely to result in a high risk***
5. processes personal data on a large scale	**5. data processed on a large scale:** the Regulation does not define what is meant by large scale, although some guidance is given in recital 91. In any case, the Working Party recommends that the following factors be taken into account in particular when assessing whether processing is carried out on a large scale: a. The number of data subjects concerned, either as a specific number or as a proportion of the population concerned. b. The amount of data and/or the variety of managed data elements. c. the duration of the data processing or durability. d. the geographical scope of the treatment.
6. combines personal data from two or more processing operations in a way that deviates from what the data subjects could reasonably , for example merging records	**6. matching or combining data sets,** for example resulting from two or more data processing operations carried out for different purposes and/or by different controllers in a way that exceeds the data subject's reasonable expectations.
7. processes personal data of persons who, for whatever reason, are in a disadvantaged or dependent position and are therefore vulnerable, such as children, employees, asylum seekers, the elderly and patients	**7. data relating to vulnerable data subjects** (recital 75): the processing of this type of data is a criterion due to an increased power imbalance between the data subjects and the data controller. controller, which means that it may be difficult individuals to easily give consent or object to the processing of their data or exercise their rights. Vulnerable data subjects may include children (they may be considered incapable of consciously and reasonably objecting or giving consent to the processing of their data), employees, more vulnerable groups of the population in need of social protection (mentally ill persons, asylum seekers, elderly persons, patients, etc.), and in any case situations where an imbalance can be identified in the relationship between the data subject and the controller.

The table continues on the next page.

IMY List of when to carry out an impact assessment under Article 35(4) An impact assessment shall be carried out if the planned treatment meets at least two of the following criteria:	**Criteria to be considered by the EDPB when assessing whether a treatment *is likely to result in a high risk***
8. uses new technologies or new organizational solutions, such as an Internet of (IoT) application	**8. innovative use or application of new technical or organizational solutions,** such as a combination of fingerprints and facial recognition for improved physical access control, etc. The Regulation clarifies (Article 35(1) and recitals 89 and 91) that the use of new technologies, defined 'in accordance with the state of the art' (recital 91), may require a DPIA. This is because the use of such technologies may involve new forms of collection and use of data, possibly with high risk to the rights and freedoms of individuals. The personal and social consequences of the use of new technologies may be unknown. A DPIA helps the controller to understand and manage such risks. For example, some 'Internet of Things' applications may have a significant impact on individuals' daily lives and privacy and thus require a DPIA.
9. processes personal data for the purpose of preventing data subjects from accessing a service or entering into a contract, for example when a bank checks its customers against a credit reference database to decide whether to offer them a loan.	**9. If the processing itself "prevents the subject from exercising a right or using a service or contract"** (Article 22 and Recital 91). This includes processing operations aimed at granting, modifying or denying data subjects access to a service or entering into a contract. An example of this is when a bank checks its customers against a credit reference database to decide whether to offer them a loan.

Examples of processing operations requiring an impact assessment to be carried out as listed by IMY under Article 35(4)

The examples given in the IMY list are given below. It is important to be aware that this is not an exhaustive list in each area.

In the world of work

- An employer systematically monitors how employees use the internet and email (criteria 3 and 7).
- An employer implements an employee access system that involves the processing of biometric data for the purpose of identifying a specific natural person, such as fingerprinting (criteria 3, 7 and 8).
- An organization implements a common system in which it is possible to notify workplace misconduct - whistleblowing system (criteria 4 and 7).
- Recruitment agencies setting up candidate or skills databases (criteria 1 and 4).
- Organizations carrying out background checks for recruitment (criteria 1, 4 and 6).

Marketing and promotion

- A business uses customers' location data, for example obtained through a mobile app, to target marketing to the customer or to plan its marketing strategies (criteria 3 and 4).
- A company collects data from social media to profile natural persons and then target marketing to certain selected groups (criteria 1 and 3).
- An Internet search engine collects data on individuals who use the service for creating customer profiles and targeting marketing (criteria 1 and 3).

Sensitive personal data

- Establishments offering genetic tests to humans to assess and predict risks of diseases or health conditions or to provide information on ethnic origin (criteria 1 and 4).
- Processing of personal data of patients by healthcare providers on other than a minimal scale. An example of a small scale is when a doctor is the sole practitioner and processes data on his patients (criteria 4, 5 and 7).
- Processing, including storage for archiving purposes, of pseudonymized sensitive personal data relating to data subjects from research projects or clinical trials (Criteria 4 and 7).
- Activities that collect and store sensitive personal data to be used a basis for selection for future research purposes (criteria 4 and 7).

Other private sector

- A bank or other credit institution that makes automated decisions regarding a credit should be granted or not (criteria 1, 2 and 9).
- A company processes financial data on natural persons on a large scale in order to be able to disclose them to other actors for credit information purposes (credit information activities) (criteria 4 and 9).

- A company that provides a platform for communication (social media) - aimed at the public and where users themselves can publish text, image or sound - and collects detailed data on the use of the service (criteria 3 and 5).

- A company that extensively processes data on customers' past misconduct (a so-called blacklist) in order to determine whether or not the person should be allowed to return as a customer (criteria 4, 5 and 9).

Public sector

- A municipality collects personal data including, among other things, location data for use in, for example, urban and traffic planning (criteria 3, 4 and 5).

- Processing of children's personal data in school activities, if there is a large number registered (criteria 5 and 7).

- A municipality processing personal data in social care, if there is a large number of data subjects (criteria 4, 5 and 7).

- An authority that, individually or jointly with other controllers, provides services to the public through digital platforms, leading to large-scale processing of personal data (criteria 4, 5 and 8).

Technology

- A company that provides internet-connected products for consumers' homes (smart home products), for example to remotely control heating, lighting or audio playback, collects detailed data on how customers use the services (criteria 3, 4 and 8).

- Social care activities that use welfare technologies, such as robots or CCTV, in people's homes (criteria 3, 4 and 8).

- Operations using an intelligent video analytics system to distinguish cars and automatically recognize license plates in order to monitor driving behaviour on motorways (criteria 3, 4 and 8).

- A parking company that uses camera surveillance that can distinguish registers number for the purpose of charging parking fees (criteria 3 and 8).

- Activities that collect personal data, including, inter alia, location data, resulting from the use of smart cars, e.g. to develop the technology (criteria 3, 4 and 8).

- Installation of smart meters at the premises of electricity consumers in order to collect, transmit and analyze consumer data at a detailed level (criteria 3 and 8).

- Organizations making major changes to their technical infrastructure and processing personal data in areas such as health or social care (criteria 4, 7 and 8).

4.4 No obligation to carry out an impact assessment

Not a type of treatment likely to lead to high risk

Only if a type of processing is "likely to result in a high risk to the rights and freedoms of natural " is there an obligation to carry out a .[36] In other cases, there is no such obligation. Controllers are obliged to continuously assess risks arising from their processing of personal data in order to be aware of whether a processing operation is becoming a "type of processing" likely to result in a high risk to the rights and freedoms of natural persons.[37]

Article 35(5) of the GDPR allows IMY to draw up and publish a national list of "those processing operations" that do not require a DPIA. A number of national supervisory authorities have drawn up such a list, including the French CNIL[38] and the Spanish AEPD[39].

IMY has made some statements on when there is no obligation to conduct a DPIA. The decision on IMY's list under Article 35(4) of the GDPR states, among other things, that a DPIA is not regularly required when checking against a sanctions list by a controller who has a legal obligation to do so. A simple check against a sanctions list should not require a DPIA, whereas a more complex cross-checking of different registers should.[40] It is also clear from the IMY list that the processing of personal data of patients by a healthcare provider on a small scale (such as when a doctor is the sole practitioner and processes data of his/her patients) does not need to be subject to a DPIA.[41]

Very similar to another treatment for which impact assessment was carried out

A controller plans several similar processing operations

Article 35(1) of the GDPR states that a single DPIA may cover a series of similar processing operations that present similar high risks. This means that one DPIA can be used to assess several processing operations that are similar in nature, scope, context, purposes and risks.[42] Therefore, a controller planning several similar processing operations does not always need to prepare a completely new DPIA for each planned processing operation. For example, an already completed DPIA can be used as a reference in the new DPIA. The reason for this is, of course, that there is often no need to analyze situations (which may present a high risk to the rights and freedoms of natural persons) when such a situation has already been analyzed.[43] However, the controller must be able to justify that the nature, scope, context, purposes and risks of the envisaged processing are sufficiently similar to the previous processing. In IMY's view, a high degree of similarity the processing operations is required for the conditions to be met.

36 See Article 35(1) of the GDPR.
37 WP 248, p. 7.
38 Commission Nationale de l'Informatique et des Libertés (CNIL), Analyse d'impact relative à la protection des données: publication d'une liste des traitements pour lesquels une analyse n'est pas requise, October 9, 2019, https://www.cnil.fr/fr/listetraitementsaipdnonrequise (accessed January 17, 2025).
39 Agencia Española Protección Datos (AEPD), Indicative list of the typers of data that do not require a data protection impact assessment under art 35.5 GDPR, https://www.aepd.es/documento/listadpia355ingles.pdf, (accessed January 17, 2025).
40 IMY Decision on the list pursuant to Article 35(4) of the EU General Data Protection Regulation 2016/679, No DI201813200, p. 4.
41 Examples in the IMY list under Article 35(4).
42 WP 248, p. 8.
43 WP 248, p. 8.

Several controllers plan several similar processing operations

Article 35(1) of the GDPR also allows several controllers planning similar processing operations to conduct a joint DPIA if the processing operations are similar in nature, scope, context, purposes and risks.[44] For example, companies planning to create a common platform for processing personal data in the framework of a trade association should be able to conduct a joint DPIA - provided that the respective processing operations and their risks are sufficiently similar. Similarly, governmental authorities planning to implement a common IT system provided by the same supplier should generally be able to carry out a joint impact assessment - provided that the planned processing operations involve the same level of risk.

Where several controllers carry out a joint DPIA, it should be made clear in writing which of the controllers is responsible for the various measures taken to protect the rights and freedoms of individuals. It is important to be aware that regardless of how responsibility for the security measures is allocated, each controller must ensure that an acceptable DPIA is carried out for its own processing operations. This means, among other things, that
the controller must be able to justify that the requirements of the GDPR have been met by carrying out a joint impact assessment[45]

A controller completes an impact assessment

A controller purchasing a technical product (such as a piece of hardware or software) should also be able to refer, where appropriate, to the DPIA carried out by the organization that provided the product, if one exists. However, the controller is responsible for carrying out its own DPIA for the specific use of the product in question[46].

Where several controllers carry out a joint DPIA for a common system, but one of the controllers has an add-on module or its own development of the system, the latter may need to complement the joint DPIA with a DPIA for its own processing. This is of course only the case if the add-on involves processing that is subject to the DPIA requirement, and in particular if it involves higher risks than the rest of the system. Even then, the controller needs to be able to justify that the GDPR requirements are met by using a previously conducted, or joint, DPIA.

A general impact assessment has been carried out

The legislator may carry out a general impact assessment as part of the legislative process in order to facilitate the work of the controllers concerned, such as the authorities or other actors who will be assigned tasks under the new .[47] It follows from Article 35(10) of the GDPR that the controller does not need to carry out a DPIA if such a general impact assessment has been carried out and the envisaged processing has its legal basis in
in the law or regulation.

44 WP 248, p. 8.
45 See WP 248, p. 8.
46 See WP 248, p. 9.
47 Article 35(10) of the GDPR. See recital 93 of the GDPR.

For the controller to be able to refrain from carrying out a DPIA on the basis of a general DPIA, all the conditions set out in Article 35(10) of the GDPR must be met. This means that

- the legal basis for the processing shall be Article 6(1)(c) or (e) of the Data Protection The regulation
- there must be legislation or other regulations governing the processing
- the legislator must have carried out an impact assessment (as part of a general impact assessment) when adopting the legal basis.

However, it is rarely possible to carry out a comprehensive impact assessment as required by the GDPR at the legislative stage. The legislator may leave it to the controller to assess in more detail the specific technical solution to be used to implement the mandate given in the legislation. The controller may therefore need to complement the general DPIA with its own DPIA on the practical, technical and organizational conditions of the processing[48].

In the legislative dossier, the legislator may sometimes outline privacy risks and consider how different safeguards can minimize privacy risks to achieve proportionality. This means that the controller can generally take guidance from the general considerations made by the legislator when conducting its supplementary DPIA.

48 E.g. IMY's consultation response of September 14, 2023 in IMY20238865; Bill 2021/22:177, *Coherent health and care documentation*, p. 54; SOU 2024:33, *Shared health data - double benefit*, p. 320 f.

5. IMYs supervisory decisions

As a supervisory authority, IMY is responsible for, among other things, monitoring the application of the GDPR and other data protection regulation, raising public and controller awareness of the risks and obligations under the regulation, and handling complaints.

To ensure compliance with the GDPR, IMY has several investigative and corrective powers. For example, if controllers do not comply with the requirements for impact assessments, IMY can use these. This can happen both when a controller has failed to carry out a DPIA when it is mandatory, and when a DPIA has been carried out inadequately.

Below are summaries of a number of supervisory decisions in which IMY has found deficiencies in relation to Article 35 of the GDPR.

Digital school platform (IMY20231647)

IMY's review concerned the decision by the Children and Education Board of Östersund municipality to migrate a new version of an existing digital school platform to its own domain and start up the service in the municipality's own IT environment. The service was used in 24 of the municipality's schools.

The IMY found, inter alia, the following. The changes in the use of the service have resulted in new personal data processing by the Board. Faced with such extensive processing
of children's personal data in school activities, the controller must carry out an impact assessment to identify risks and the need for protection measures, which the Board had not done. The children, as pupils, were in a vulnerable position in relation to the controller. The processing also concerned employees who were in a dependent relationship with the Board. Moreover, the processing involved to some extent feedback on school assignments, which may be considered an evaluation of the data subjects' performance.

On November 28, 2023, the IMY decided that the Children and Education Board should pay an administrative fine for infringement of Article 35(1) of the Data Protection Regulation. The supervisory decision has acquired legal force.

Read the decision: IMY-2023-1647

CCTV in assisted living facilities (DI20197782)

IMY's review was based on a complaint from a relative of a resident of a LSS home who alleged that the resident was being illegally monitored by cameras, including in his bedroom.

The IMY found several shortcomings, including that an impact assessment had not been carried out.

On November 24, 2020, IMY decided that Gnosjö Municipality - Socialutskottet would pay an administrative fine for violation of, among other things, Article 35 of the Data Protection Regulation. The supervisory decision has gained legal force.

Read the decision: DI20197782

Digital school platform (DI20197024)

IMY's audit concerned an IT system used by schools in the City of Stockholm for including student administration.

The IMY found, inter alia, the following. The audit showed that there were serious shortcomings in security. An impact assessment had not been carried out despite the fact that

large systems with many children and staff registered, and with both sensitive and privacy-sensitive personal data. If the Board of Education had carried out a full impact assessment, the shortcomings identified could probably have been avoided.

On November 23, 2020, IMY decided that the Education Board of the City of Stockholm should pay an administrative fine for violation of several articles of the Data Protection Regulation and ordered the Board to urgently carry out an impact assessment accordance with Article 35 of the Data Protection Regulation for three subsystems. The supervisory decision has become final.

Read the decision: DI20197024

Facial recognition for student attendance monitoring (DI20192221)

IMY's review was carried out against the background of the fact that the Skellefteå municipality's Upper Secondary School Board had used facial recognition to register pupils' attendance in a pilot project at an upper secondary school. The Board referred to a "risk assessment carried out" which concluded that the legal basis referred , and
the security of the processing meant that there was no need for a "specific risk assessment" of the sensitive personal data.

The IMY concluded, inter alia, that There was no basis for processing bio-metric personal data in the way that was done. The processing operations in question involved a number of factors which suggested that an Article 35 impact assessment of the GDPR should have been carried out before the start of the processing operations. The "risk assessment" presented by the Board could not be considered to meet the requirements of Article 35 of the GDPR. It lacked an assessment of the risks to the rights and freedoms of data subjects, as well as an account of the proportionality of the processing in relation to its purposes. The processing operations should have triggered a request for prior consultation with IMY before the processing was initiated, which meant that the processing operations were also in breach of Article 36 of the GDPR.

On August 20, 2019, IMY decided that the Skellefteå High School Board should pay an administrative fine for violation of, among other things, Article 35 of the Data Protection Regulation. The supervisory decision has gained legal force.

Read the decision: DI20192221

6. Role of the Data Protection Officer in the impact assessment

Article 35(2) of the GDPR states that the controller shall consult the DPO when carrying out a DPIA.
The GDPR does not regulate in detail when and how this should happen, or how the DPO should be involved in the DPIA process.[49] There is therefore some room for variation depending on the organization's structure, data protection policies and other circumstances, as long as the controller takes into account the other provisions on DPOs.[50]

The key provisions on the tasks of the DPO are contained in Articles 37-39 of the GDPR. Article 39 states that the DPO shall, upon request, advise the controller on the impact assessment and monitor its implementation. It also states, inter alia, that the DPO shall act as a contact point for IMY if the controller requests prior consultation under Article 36 of the GDPR. The position of the DPO is set out in Article 38 and the relevant qualifications for a DPO are set out in Article 37(5).
Article 38(1) states that controllers shall ensure the proper and timely involvement of the DPO in all matters concerning the protection of personal data. This includes, inter alia, the work on impact assessments.

To determine how the DPO should or should not be involved in DPIAs, the controller can refer to the EDPB Guidelines on DPIA and the EDPB Guidelines on DPOs for guidance.

IMY's position is that the DPO should generally be involved on an ongoing basis, at several stages of the conduct of the impact assessment and in relation to key decisions. It is appropriate that the DPO is involved as early as possible in the process, for example to provide advice on methodology and to reduce the risk of inaccurate scoping.

The controller should determine who is responsible for involving the DPO and build controls into the processes to detect when this has not been done. It is the responsibility of the controller to ensure that the DPO is provided with accurate and sufficient information about the processing and the process in order to carry out his or her duties.

6.1 IMY believes that the DPO should do the following in the process:

1. Provide advice for an impact assessment

The controller should consult the DPO before determining the scope and boundaries of a DPIA. For example, the DPO should be consulted on whether a DPIA should be carried out for a particular processing operation and before the controller decides not to carry out a DPIA despite the fulfilment of two criteria in the IMY list under Article 35(4) of the GDPR.[51] The DPO may also suggest that the controller carries out a DPIA for a particular processing operation.[52]

2. Advise on the methodology of the impact assessment

The DPO should regularly and where necessary advise on whether the methodology of the impact assessment is appropriately designed. Methodology here refers to how the impact assessment is carried , such as the order in which things are , who

49 See WP 248, p. 19.
50 See WP 248, p. 19.
51 See WP 243, p. 20.
52 WP 248, p. 17.

should be involved and whether the impact assessment should be carried out internally or externally.[53] The DPO can, for example, review relevant policy and supporting documents, such as process and procedure descriptions, templates and guidance. The DPO can also recommend appropriate measures and follow up on their implementation.

3. Advise on risk management

IMY believes that the controller should consult the DPO where necessary in the context of the risk assessment and in the assessment of which risk mitigation measures should be taken. For example, the DPO can help to evaluate the quality of the risk assessment.[54] It is suggested that the DPO can participate in any workshops on risk management.

Handling of the DPO's advice

IMY recommends that the DPO distinguishes between general advice on the one hand and formal recommendations to the controller on the other. What the controller should do in response to the advice and recommendations given by the DPO depends on the circumstances of the individual case. If the DPO makes a formal recommendation to take or refrain from taking an action and the controller decides not to follow it, the controller should document the reasons why[55].

4. Monitor the implementation of the impact assessment

The DPO's task of monitoring the implementation of the impact assessment should be risk-based.[56] The DPO's task in this regard should thus be adapted to the assessed level of risk of the processing. In order to enable the DPO to perform his or her task, the party conducting the impact assessment should send regular status reports on the implementation.

5. Evaluate the outcome of the impact assessment

Before implementing the mitigation measures and determining the residual risk, the DPO should evaluate the outcome of the impact assessment. In particular, the DPO should evaluate whether the documentation, assessments and conclusions are of sufficient quality. The DPO should also help to evaluate whether the residual risk is acceptable.

In general, it is appropriate for the DPO to prepare a written statement, including how the DPO has been involved in the implementation and the documentation on which the statement is based. Such a statement should be adapted to the complexity of the impact assessment, the scope of the planned processing and the assessed risk. In some cases, it may be sufficient for the DPO to sign a ready-made text prepared according to a template.[57] The DPO's opinion should be documented in the DPIA.[58]

53 See WP 243, p. 20.
54 WP 248, p. 17.
55 See WP 248, p. 13 and WP 243, p. 16.
56 See WP 243, p. 22.
57 See judgment of the Court of Justice of the European Union of 16 February 2023, C349/21, HYA and others, EU:C:2023:102, p. 53 et seq.
58 WP 248, p. 13 and WP 243, p. 16.

A DPO who considers that the impact assessment has been deficient in any part should provide a justification that clarifies the deficiency and, if possible, how it can be remedied. The DPO should not, however, take over the conduct of the impact assessment[59].

Below are a number of questions that the DPO may ask himself/herself when evaluating the outcome of the impact assessment.

Examples of questions to ask during the evaluation

- Has the DPO been sufficiently involved in the impact assessment process? Has the DPO been provided with accurate and sufficient information to carry out his/her task?
- Is the description of the processing sufficiently detailed to determine whether the purpose limitation principle is fulfilled?
- Does it appear that sufficient work has been done in identifying the risks and that the risk assessment is well justified?
- Are the identified measures appropriate to manage the risks?
- Is there a clear division of responsibilities within the organization to implement the risk reduction measures?
- Is the assessment of the potential residual risk clearly described and justified?
- Is it clear who is responsible for the residual risk within the organization?[60]
- Is the assessment of the necessity and proportionality of the treatment sufficiently justified? Is the assessment reasonable?
- Is it clear when the impact assessment will be reviewed and who who is responsible for monitoring any changes in the risks?

6. Monitor overall compliance

The GDPR requires the DPO to monitor overall compliance with applicable data protection provisions[61] and to report to the highest level of management of the controller[62]. Thus, in addition to advising on individual DPIAs, the DPO should also monitor the organization's work on DPIAs in general. This could include, for example, investigating how many DPIAs are carried out, which parts of the organization carry them out, how long it takes to carry them out and what their quality is.

59 See for example Articles 35(2), 39(1)(c) and 38(6) of the GDPR.
60 Note that the internal responsibility within the organization should not be confused with the personal data responsibility under Article 4(7) of the GDPR.
61 See Article 39(1)(b) of the GDPR.
62 See Article 38(3) third sentence of the GDPR.

6.2 What the DPO should *not* do in the impact assessment

The DPO shall not carry out the DPIA or responsible for its implementation.[63] The DPO cannot independently quality assure, verify or audit anything he or she has done. It is the responsibility of the controller to ensure that the methodology for conducting a DPIA and the results of individual assessments comply with the GDPR.

The process should not be designed so that the DPO is in practice assigned responsibilities for assessments that turn out to be incorrect, for example that a risk has been underestimated or that the processing is not necessary in some part. The DPO does not have the ultimate responsibility for preventing processing that does not comply with the GDPR or for ensuring that processing is aligned with the recommendations proposed by the DPO. This risks undermining the independence of the DPO[64].

The controller should design its DPIA process so that the division of responsibilities between the DPO and the controller is clear to all involved.

63 See for example Articles 35(2), 39(1)(c) and 38(6) of the GDPR.
64 Cf. the IMY decision of June 27, 2024 in supervisory case IMY20237980 (concerning the controller's obligation to ensure that the DPO's tasks do not lead to a conflict of interest).

IMY. Integritetsskydds myndigheten

This is the Data Protection Authority

The Data Protection Authority works to protect all your personal data, such as health and financial information, so that it is handled correctly and does not fall into the wrong hands. We are the ones who check that companies, public authorities and other actors comply with the GDPR - the General Data Protection Regulation.
the General Data Protection Regulation. We train and guide those who process personal data. We want to see a sustainable and privacy-friendly digitalization. We are convinced that it is possible to ensure the safety of citizens and the security of society without unjustified mapping and surveillance. Together with the other data protection authorities in the EU, we are working to ensure that citizens' personal data protected equally across the Union. We are also working to ensure credit checks are carried out correctly.
Our vision is a secure information society, where we work together to protect privacy.

Contact the Data Protection Authority

E-mail:imy@imy.se
Web: www.imy.se
Tel: 08-657 61 00
Postal address: Privacy Protection Authority,
Box 8114, 104 20 Stockholm