GUIDANCE NOTE

Belgium - Privacy Impact Assessment

Stephanie DeSmedt
LOYENS LOEFF

Virginie de France
LOYENS LOEFF

Bram Goetry
LOYENS & LOEFF

Olivier Verhasselt
LOYENS & LOEFF

Last Updated: June 2, 2025

June 2025

Please note that this Guidance Note focuses on the legislation and specific requirements in relation to Privacy Impact Assessments in Belgium. For more information on the requirements under the General Data Protection Regulation (GDPR), please see the EU - GDPR - Privacy Impact Assessment Guidance Note.

1. Laws

1.1. Laws and regulations

1.1.1. What laws and/or regulations apply to Privacy Impact Assessments?

In addition to the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), the following national laws apply:

- the Law of July 30, 2018 on the Protection of Individuals regarding the Processing of Personal Data, which ensures the local law implementation of the GDPR (only available in Dutch here and in French here) (the Act); and
- the Law of December 3, 2017, establishing the Belgian Data Protection Authority (only available in Dutch here and in French here) (the Law establishing Belgian DPA).

Citation	Not applicable.
Applicable persona	Not applicable.

1.2. Supervisory authority

1.2.1. Who is responsible for enforcing the laws and/or regulations and issuing guidelines?

The Belgian Data Protection Authority (Belgian DPA) is the main supervisory authority. Its decisions may be appealed before the Markets Court (which is a division of the Brussels Court of Appeal).

The supervisory authority for ensuring compliance by Flemish public bodies is the Vlaamse Toezichtscommissie (VTC).

Citation	Not applicable.
Applicable persona	Not applicable.

1.3. Guidelines

1.3.1. Have any guidelines been issued on Privacy Impact Assessments?

Yes, the following guidelines were issued by the Belgian DPA:

- Data Protection Impact Assessment (DPIA) Guide, version 4.0, issued by the DPA on April 21, 2021 (only available in Dutch here and in French here) (the DPIA Guide);
- Decision 1/2019 on the list of processing activities for which a DPIA needs to be carried out, issued on January 16, 2019, by the General Secretariat of the DPA (only available in French here and in Dutch here);
- Recommendation 1/2018 on data protection impact assessments and prior consultation, issued on February 28, 2018, by the Belgian Commission for the Protection of Privacy (predecessor of the DPA) (only available in French here and in Dutch here);

Additionally, the VTC issued DPIA guidelines and a DPIA assessment tool specifically for Flemish public bodies (only available in Dutch here).

Citation	Not applicable.
Applicable persona	Not applicable.

1.3.2. Has a Privacy Impact Assessment blacklist been released?

Yes, both at the level of the Belgian DPA and at the level of the VTC:

Belgian DPA

- Initial list: Recommendation 1/2018, issued on February 28, 2018, by the Belgian Commission for the Protection of Privacy (predecessor of the Belgian DPA) - Annex 3 (only available in French here and in Dutch here) (Recommendation 1/2018); and
- Updated list: Decision 1/2019 on the list of processing activities for which a DPIA needs to be carried out, issued on January 16, 2019, by the General Secretariat of the DPA (only available in French here and in Dutch here) (Decision 1/2019);

VTC

List applicable to processing by Flemish public bodies, issued by the VTC on January 14, 2020, and applicable since May 15, 2020 (only available in Dutch here) (the VTC Public Bodies List).

Citation	Recommendation 1/2018Decision 1/2019 The VTC Public Bodies List
Applicable persona	Not applicable.

1.3.3. Has a Privacy Impact Assessment whitelist been released?

No. An unofficial draft whitelist was proposed by the Belgian Commission for the Protection of Privacy (predecessor of the Belgian DPA) in 2018 (see Annex 2 of Recommendation 1/2018), but never formally adopted.

Citation	Annex 2 of Recommendation 1/2018
Applicable persona	Not applicable.

1.3.4. Has a Privacy Impact Assessment template been released?

Not by the Belgian DPA. The VTC has published a template on January 5, 2022 (only available in Dutch here) (the VTC DPIA template)

Citation	The VTC DPIA template
Applicable persona	Not applicable.

2. Definitions

2.1. Key terms

2.1.1. How is data controller (or equivalent) defined?

There are no national law variations from the GDPR. except for legal provisions expressly designating certain public bodies or public authorities as

data controllers in specific cases.

Citation	There are no national law variations from the GDPR.
Applicable persona	Not applicable.

2.1.2. How is data processor (or equivalent) defined?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	Not applicable.

2.1.3. How is data subject (or equivalent) defined?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	Not applicable.

2.1.4. How is processing (or equivalent) defined?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	Not applicable.

2.1.5. How is personal data defined?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	Not applicable.

2.1.6. How is sensitive data defined?

There are no national law variations from the GDPR.

Notably, data related to criminal offences and convictions (Article 10 GDPR) is not included in the definition of special category data but is commonly also deemed included in the notion of 'sensitive data.' The same goes for the unique National Registry Number allocated by the government to all Belgian citizens, and the processing of which is in principle prohibited (except where specifically allowed by law) by the Law of August 8, 1983 on the national registry of national persons (only available in Dutch here and in French here) (Law of August 8, 1983).

Citation	Article 8 of the Law of August 8, 1983
Applicable persona	Not applicable.

2.1.7. How is pseudonymized/de-identified data defined?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	Not applicable.

2.1.8. How is anonymized data defined?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	Not applicable.

2.1.9. How is profiling defined?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.

Applicable persona	Not applicable.

2.1.10. How is automated decision-making defined?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	Not applicable.

2.1.11. How is targeted advertising defined?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	Not applicable.

3. Privacy Impact Assessment requirements

3.1. Legal obligations

3.1.1. Is there a requirement to conduct a Privacy Impact Assessment?

Yes, as Article 35 GDPR is directly applicable in Belgium.

There are no national law variations from the GDPR, with one exception. In the Act, the Belgian legislator made use of the delegation granted by Article 35(10) of the GDPR to stipulate that a specific impact assessment must still be carried out by the relevant data controller, even where a general data protection impact assessment has already been conducted as part of the

adoption of the legal basis of a processing activity pursuant to Article 6(1)(c) or 6(1)(e) GDPR. This means that, when a processing activity is based on a normative text, the entity or entities responsible for carrying out this processing are still required, as data controllers, to conduct an impact assessment themselves. The Belgian DPA also outlines this is the DPIA Guide.

Citation	Article 23 of the Act Section 1.c) of the DPIA Guide
Applicable persona	Controller

3.1.2. Under which circumstances is the requirement to conduct a Privacy Impact Assessment triggered?

In addition to the application of the general criteria of Article 35 GDPR, the Belgian DPA has published the following list of processing activities which in any event trigger the requirement to conduct a DPIA:

- when the processing uses biometric data for the unique identification of the individuals concerned in a public place or in a private place accessible to the public;
- when personal data is collected from third parties in order to be subsequently taken into account in the decision to refuse or terminate a specific service contract with an individual;
- when health data of an individual concerned is collected automatically using an active implantable medical device;
- when data is collected on a large scale from third parties in order to analyze or predict the economic situation, health, personal preferences or interests, reliability or behavior, location, or movements of individuals;
- when special categories of personal data as defined in Article 9 of the GDPR or data of a very personal nature (such as data on poverty, unemployment, youth aid involvement or social work, data on domestic and private activities, location data) are systematically exchanged between multiple data controllers;
- when there is large-scale processing of data generated by devices with sensors that send data via the Internet or other means (Internet of Things applications, such as smart TVs, smart home appliances, connected toys,

"smart cities", smart energy meters, etc.) and this processing is used to analyze or predict the economic situation, health, personal preferences or interests, reliability or behavior, location or movements of individuals;

- when there is large-scale and/or systematic processing of telephone, Internet, or other communication data, metadata, or location data of individuals or enabling the identification of individuals (for example, wifi-tracking or processing location data of travelers in public transport) when the processing is not strictly necessary for a service requested by the individual concerned; and
- when personal data is processed on a large scale where the behavior of individuals is observed, collected, established, or influenced, including for advertising purposes, and this is done systematically via automated processing.

Additionally, the VTC has published a separate blacklist specifically applicable to controllers that are Flemish public bodies.

Citation	Recommendation 1/2018 Decision 1/2019 The VTC Public Bodies List
Applicable persona	Controller

3.1.3. At what stage of processing should a Privacy Impact Assessment be conducted?

It must be carried out prior to the start of the processing. A DPIA should be initiated as early as possible during the design of the processing operation (preferably when the 'idea of creating' a new processing operation arises), even if some aspects of the processing are not yet known. It may also be necessary to repeat certain steps of the assessment as the development process progresses since the selection of specific technical and organizational measures can influence the severity or likelihood of risks arising from data processing (e.g., delegating part of the processing activity to a subcontractor). The DPA has specified that the fact that a DPIA may need to be updated after the actual start of processing is not a valid reason to delay or omit the analysis.

Citation	Paragraphs 33 and 34 of Recommendation 1/2018
Applicable persona	Controller

3.1.4. Is there a requirement to conduct a Privacy Impact Assessment for processing activities that began before the law(s) entered into effect?

The obligation to conduct a DPIA applies from May 25, 2018 (applicability of GDPR). The DPA has however recommended that the data controller, as a good practice, conducts a DPIA for all processing operations existing prior to that date, that are likely to result in a high risk to the rights and freedoms of natural persons. Additionally, also for existing processing operations, the data controller must conduct a DPIA at the appropriate time as part of their overall responsibility and risk management.

Citation	Paragraphs 101 and 103 of Recommendation 1/2018
Applicable persona	Controller

3.1.5. Are there any exemptions?

There are no national law variations from the GDPR (only an unofficial draft 'whitelist').

Citation	Annex 2 of Recommendation 1/2018
Applicable persona	Controller

3.2. Reusing assessments

3.2.1. Does the law(s) permit the use of a Privacy Impact Assessment for more than one processing operation?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.

Applicable persona	There are no national law variations from the GDPR.

3.2.2. Under which circumstances can a Privacy Impact Assessment be used for more than one processing operation?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	There are no national law variations from the GDPR.

3.3. Publication

3.3.1. Is there a requirement to submit Privacy Impact Assessments to the supervisory authority?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	There are no national law variations from the GDPR.

3.3.2. Is there a requirement that Privacy Impact Assessments be made public?

The Belgian DPA has encouraged data controllers to consider publishing their DPIAs. The published DPIA should however not include the entire analysis, especially when it may contain specific information about security risks related to the data controller or disclose trade secrets or commercially sensitive information. In such cases, the published version may simply consist of a summary of the key findings of the DPIA or even just a statement confirming that a DPIA has been conducted.

Citation	Paragraph 89 of Recommendation 1/2018

Applicable persona	Controller

3.4. Review and updates

3.4.1. Is there a requirement to periodically review Privacy Impact Assessments?

Yes. The Belgian DPA has held that performing a DPIA is a continuous process, not a one-time exercise. This becomes even more important when a processing activity or environment is dynamic and subject to constant changes. The continuous updating of the DPIA throughout the project lifecycle ensures consideration of data protection and privacy and encourages the development of solutions that generally promote compliance with the GDPR, particularly the obligation of data protection by design.

Citation	Paragraphs 33 and 34 of Recommendation 1/2018
Applicable persona	Controller

3.4.2. How regularly should a Privacy Impact Assessment be reviewed?

There are no national law variations from the GDPR. The Belgian DPA however recommends reviewing DPIAs whenever the risk associated with a processing activity materially changes, and at least every three years.

Citation	Paragraphs 96-100 of Recommendation 1/2018
Applicable persona	Controller

3.4.3. Is there a requirement to update a Privacy Impact Assessment in light of changes to processing activities?

Yes. The Belgian DPA has held that performing a DPIA is a continuous process, not a one-time exercise. This becomes even more important when a processing activity or environment is dynamic and subject to constant changes.

Citation	Paragraph 34 of Recommendation 1/2018
Applicable persona	Controller

3.5. Concerned parties

3.5.1. Who must participate in a Privacy Impact Assessment?

There are no national law variations from the GDPR. The Belgian DPA has however, issued the following guidelines.

Data controllers

The data controller must ensure that the right people within the company are involved in the risk assessment process.

In this regard, the DPA primarily referred not only to the DPO and/or the security advisor but also to the designers of new applications (such as ICT architects), analysts, corporate lawyers, decision-makers responsible for strategic project development, subcontracting managers, personnel management officers, and staff members (or their representatives) who will use the relevant personal data in the course of their duties, among others.

Furthermore, final decisions made within the framework of a DPIA have to be taken at a sufficiently high hierarchical level. It is recommended to have DPIA decisions taken by or submitted to the highest management level.

When the processing operation involves joint controllers, they must clearly define their respective obligations. Their DPIA should specify which party is responsible for the various measures aimed at addressing risks and protecting the rights and freedoms of the data subjects. Additionally, each controller should express their needs and share relevant information while ensuring that no secrets (such as trade secrets, intellectual property, or confidential business information) are compromised and that no vulnerabilities are disclosed.

Data processors

The processor must, depending on the nature of the processing, assist the data controller in carrying out a DPIA.

The Data Protection Officer (DPO)

See section 6.2 below.

The data subjects or their representatives

See section 6.3 below.

Citation	Paragraphs 67-72 and 75 of Recommendation 1/2018
Applicable persona	Controller and processor

3.5.2. Is it permissible to outsource a Privacy Impact Assessment?

Yes, this is permitted. The DPIA can be conducted by someone else, either within or outside the organization, but the data controller remains ultimately responsible (and liable) for the proper performance of this task.

Citation	Paragraph 67 of Recommendation 1/2018
Applicable persona	Controller

4. Risk management

4.1. Risk assessment

4.1.1. Does the law(s) provide criteria for assessing the risks of processing activities?

There are no national law variations from the GDPR.

Note that the VTC has published a tool (in 2017) that should assist controllers in conducting risk assessments (only available in Dutch here) (the VTC tool). This tool enables a controller to assess the impact of processing on risks to

the rights and freedoms of natural persons. It also helps to demonstrate that the measures taken are sufficient to mitigate the risk of adverse effects. The tool helps determine whether a DPIA needs to be carried out and also provides a starting point for drawing up a DPIA.

Citation	The VTC Tool
Applicable persona	Controller

4.1.2. Does the law(s) provide criteria for assessing the impact on data subjects?

There are no national law variations from the GDPR.

The Belgian DPA has however acknowledged the following elements are relevant for this assessment:

- loss of an opportunity;
- harm to peace of mind or well-being;
- stigmatization or stereotyping;
- denial or restriction of access to places or events that are usually open to the public;
- unfair treatment (e.g., differentiated pricing);
- manipulation (e.g., exploitation of emotions);
- behavioral adaptation (e.g., self-censorship); and
- harm to physical or moral integrity.

Citation	Paragraph 46 of Recommendation 1/2018 The VTC Tool
Applicable persona	Controller

4.1.3. Does the law(s) outline what is considered high-risk?

There are no national law variations from the GDPR. The Belgian DPA has however, published some guidelines in this respect.

First, the Belgian DPA considered that the notion of 'high risk' refers to data processing activities that are or may be likely to have significant negative impacts on the fundamental rights and freedoms of individuals. The expression 'likely to' does not imply a remote possibility of a significant impact. Instead, the significant impact must be more probable than improbable. However, it also means that individuals do not need to be affected; the mere probability that they could be significantly affected is sufficient to meet this criterion.

Second, a 'significant negative impact' means that if the risk materializes, the data subject would be substantially affected in the exercise or enjoyment of their fundamental rights and freedoms.

Finally, the Belgian DPA has reiterated the nine criteria set forth by the Article 29 Working Party (WP29) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679 (the WP29 DPIA Guidelines), which data controllers must take into consideration in their analysis to determine whether the proposed processing is likely to result in a high risk to the rights and freedoms of individuals.

Citation	Paragraph 18 of Recommendation 1/2018 WP29 DPIA Guidelines
Applicable persona	Controller

4.2. Risk mitigation

4.2.1. Does the law(s) provide criteria for mitigating risks?

There are no national law variations from the GDPR.

Citation	The VTC Tool
Applicable persona	Controller

4.2.2. Does the law(s) establish procedures for managing residual risk?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	There are no national law variations from the GDPR.

5. Documentation

5.1. Content

5.1.1. What information must be included in a Privacy Impact Assessment?

There are no national law variations from the GDPR. The Belgian DPA has, however, published guidelines in this respect, proposing the following to be included:

Description

The description must include at least the following elements:

- a clear description of the processing, including any business processes and system requirements;
- the personal data involved, the recipients, and the duration for which the personal data will be stored;
- the assets on which the personal data rely (e.g., hardware, software, networks, people, paper documents, or paper transmission channels).

Among other relevant elements to determine the nature, scope, and context of processing operations, the following can be mentioned: categories of data subjects, the scale of data processing, the origin of the data, the relationship between the data controller and the data subjects, potential consequences for the data subjects, and the ease with which the data subjects can be identified.

The data controller must ensure that the processing operations and purposes of the processing are described with the necessary precision.

Evaluation of necessity and proportionality

When assessing the necessity and proportionality of the intended processing, at least the following elements should be considered:

- the specified, explicit, and legitimate purpose(s) of the intended processing;
- the legal basis for processing the data (Article 6 of the GDPR);
- a justification that the personal data being processed is adequate, relevant, and limited to what is necessary (Article 5(1)(c) of the GDPR);
- a justification for the proposed retention period of the personal data, which should not be kept in a form that allows identification of the data subjects for longer than necessary for the purposes for which the data is processed (Article 5(1)(e) of the GDPR);
- a justification that the interests of the data subject do not override the legitimate interests of the data controller or any third parties.

The Belgian DPA also expects a DPIA to provide an overview of:

- the measures that contribute to the rights of the data subjects, including:
  - the information provided to the data subject (Articles 12, 13, and 14 of the GDPR);
  - the right of access and the right to data portability (Articles 15 and 20 of the GDPR);
  - the right to rectification and the right to erasure of data (Articles 16, 17, and 19 of the GDPR);
  - the right to object and the right to restriction of processing (Articles 18, 19, and 21 of the GDPR);
- the manner in which relationships with data processors are governed (Article 28 of the GDPR);
- the safeguards for any international transfer(s) that will be implemented, where applicable (Chapter V of the GDPR).

Risk evaluation

The concept of 'risk assessment' refers to the entire process of (1) risk identification, (2) risk analysis, and (3) risk evaluation. Risk identification refers to the process of examining, recognizing, and describing the risks. Risk analysis refers to the process implemented to understand the nature of a risk and to determine its level. Risk evaluation is the process of comparing the results of the risk analysis with pre-established risk criteria in order to determine whether the risk (and/or its significance) is acceptable or tolerable. Risk assessment involves determining the likelihood and severity of the risk. When assessing the risk, the data controller must ask the following questions: What is the potential impact on the data subjects, and what is the likelihood that this impact will occur?

The Belgian DPA recommends, as part of a DPIA, to explicitly map all non-negligible risks and identify effective protective measures, as even moderate risks can be a significant factor when assessing the proportionality of the intended data processing.

Measures intended to address the risks.

The relevant measures can be of a technical, organizational, or legal nature. When identifying the intended measures, the data controller must explicitly indicate which measures are intended to mitigate which risks. In this regard, it is recommended that the data controller also explicitly specify:

- what resources will be needed to implement the measures;
- which person(s) will be responsible for implementing these measures;
- the duration for which the measures will be executed;
- how the relevance of the measures will be monitored and evaluated.

Note that the VTC has the VTC tool. It is, however, not mandatory to use this template.

Citation	Section 5 of Recommendation 1/2018 The VTC Tool
Applicable persona	Controller

5.1.2. Is there a requirement to maintain additional documentation to supplement a Privacy Impact Assessment?

There are no national law variations from the GDPR. It is, however, highly recommended to maintain evidence of the accompanying DPO opinion (if there is one). The Belgian DPA also specified that, if the data controller disagrees with the opinion provided by the DPO, they must specifically justify and document in writing within the DPIA documentation why this opinion has not been considered.

Citation	Paragraph 79 of Recommendation 1/2018 the DPIA Guide
Applicable persona	Controller

5.1.3. What must be included in the additional documentation?

There are no national law variations from the GDPR. It is, however, highly recommended to include the DPO opinion, if one was rendered.

Citation	Paragraph 79 of Recommendation 1/2018 the DPIA Guide
Applicable persona	Controller

5.1.4. Where a Privacy Impact Assessment is deemed unnecessary, are companies required to document their reasoning for this decision?

There is no legal requirement in national law to do so. However, the Belgian DPA has held that it is possible that a data controller may not consider a processing activity that, in fact, corresponds to processing 'likely to result in a high risk.' In such cases, the data controller must justify and document the reasons why no DPIA has been performed, and must record the opinions of the DPO (if any) in this documentation.

Citation	Paragraph 21 of Recommendation 1/2018
Applicable persona	Controller

5.2. Format

5.2.1. In what format must Privacy Impact Assessments be kept?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	There are no national law variations from the GDPR.

5.2.2. In which language must Privacy Impact Assessments be conducted?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	There are no national law variations from the GDPR.

5.3. Retention

5.3.1. Is there a requirement to retain Privacy Impact Assessments?

There are no national law variations from the GDPR. However, as the implementation of a DPIA is an ongoing process, and to comply with accountability obligations, the DPIA must in principle be retained.

Citation	Author's recommendation.
Applicable persona	Controller

5.3.2. How long must Privacy Impact Assessments be retained?

The duration in which a DPIA must be retained is not specified in national law, however, the statute of limitations for GDPR claims is generally five years after cessation of the processing activity.

Citation	Article 105 of the Law establishing Belgian DPA
Applicable persona	Controller

6. Consultation

6.1. Authority consultation

6.1.1. Is consultation with the supervisory authority required?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	There are no national law variations from the GDPR.

6.1.2. Under which circumstances is the requirement to consult triggered?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	There are no national law variations from the GDPR.

6.1.3. What information needs to be provided to the supervisory authority in the context of a consultation?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	There are no national law variations from the GDPR.

6.1.4. When should information be provided to the supervisory authority?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	There are no national law variations from the GDPR.

6.1.5. In what format must the information be provided?

The information must be provided by submitting a completed pre-defined form, which is available for download on the Belgian DPA's dedicated webpage (only available in Dutch here, in French here, and in German here) (the prior consultation form). Consultation requests will only be admissible if the completed form is submitted in Dutch, French, or German. Technical annexes can also be submitted in English. The completed form can either be sent to the Belgian DPA by ordinary mail (paper version) or uploaded to the Belgian DPA's website (electronic version).

Citation	The prior consultation form
Applicable persona	Controller

6.1.6. Where should information be provided?

The information should be uploaded on the Belgian DPA's prior consultation form or sent via ordinary postal mail to the following address:

Drukpersstraat/Rue de la Presse 35, 1000 Brussel/Bruxelles.

Citation	The prior consultation form
Applicable persona	Controller

6.1.7. What is the time frame for the supervisory authority to provide a response?

Once the DPIA file is in order and provided that the Belgian DPA considers that the planned processing is contrary to the GDPR, it will issue a written opinion to the controller within a maximum of eight weeks. This period may be extended by six weeks, depending on the complexity of the planned processing. Additional information may be requested at any time if this proves necessary to complete the file, in which case the aforementioned deadlines will be suspended. In case no high risk is identified by the Belgian DPA, it will not issue a formal opinion, but simply inform the controller of this finding.

Citation	The DPIA Guide
Applicable persona	Controller

6.1.8. Are there any exemptions to the requirement to consult?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	There are no national law variations from the GDPR.

6.2. Data protection officer consultation

6.2.1. Is consultation with the data protection officer required?

There are no national law variations from the GDPR. It is, however, highly recommended to consult with the DPO (and, for Flemish public bodies, the

VTC considers this to be mandatory). According to the DPA, the advisory role of the DPO should focus on the following aspects:

- whether a DPIA needs to be conducted;
- the methodology to be followed when carrying out a DPIA;
- whether the DPIA should be conducted internally or outsourced;
- the safeguards (including technical and organizational measures) to be applied to mitigate potential risks to the rights and interests of the data subjects; and
- whether the DPIA has been properly conducted and whether its conclusions (the necessity of the processing and the safeguards to be implemented) comply with the GDPR.

Citation	Paragraph 79 of Recommendation 1/2018 The DPIA Guide
Applicable persona	Controller

6.2.2. Under which circumstances is the requirement to consult triggered?

Whenever the controller has a DPO.

Citation	Paragraph 79 of Recommendation 1/2018, the DPIA Guide
Applicable persona	Controller

6.2.3. Is it mandatory to follow the advice of the data protection officer?

No. However, if the data controller disagrees with the opinion provided by the DPO, they must specifically justify in writing, within the DPIA documentation, why the opinion was not taken into account.

Citation	Paragraphs 76-79 of Recommendation 1/2018 The DPIA Guide

Applicable persona	Controller

6.3. Third-party consultation

6.3.1. Is there a requirement to consult with third parties?

Yes, the Belgian DPA expects such consultation to be considered.

Citation	Paragraphs 80-86 of Recommendation 1/2018
Applicable persona	Controller

6.3.2. Under which circumstances is the requirement to consult with third parties triggered?

Where there are sufficient significant reasons to conduct such a consultation, considering the nature, context, scope, and purpose of the processing, as well as the potential impact on the data subjects, the Belgian DPA considers it necessary for such a consultation to actually take place.

Consulting with data subjects is particularly recommended when they possess essential information or can provide important comments relevant to the conduct of the DPIA. If the data controller deems it inappropriate to seek the opinion of the data subjects, they must document the reasoning for not seeking the opinion of the data subjects.

Consulting data subjects or their representatives can provide significant added value, both in identifying and assessing the risks of the processing and in finalizing a DPIA, to verify whether all risks have been sufficiently addressed. The extent of the consultation (which individuals and how many) should preferably be determined based on the risk and scale of the processing. If a proposed processing only poses risks to a limited number of data subjects (e.g., employees of a small organization), the consultation can be limited to a small group of these employees and/or their representatives. If the proposed processing involves risks to a large number of data subjects (e.g., all residents), a broader consultation should be organized.

The data controller generally has the freedom to decide how the data subjects or their representatives will be consulted. Their opinions can be

gathered in various ways, depending on the context (e.g., a general study regarding the purposes and means of processing, a questionnaire addressed to employee representatives, or regular surveys sent to future clients of the data controller). If their contact details are available, the data controller may directly reach out to ask for their opinion about the proposed data processing (e.g., by email). If the identity of the data subjects is not known beforehand, the data controller could, for example, organize a public consultation. If necessary, the data controller may also arrange a joint consultation session. Although Article 35(9) of the GDPR only mentions "data subjects or their representatives," there may also be value in seeking the views of organizations that generally advocate for the interests of data subjects or consumers.
In the consultation process, the data controller must ensure that questions are posed in a way that generates reliable results.

If the final decision of the data controller differs from the opinion of the data subjects, they must document the reasons for their decision to either proceed or not proceed with the processing.

Citation	Paragraphs 80-86 of Recommendation 1/2018
Applicable persona	Controller

7. Enforcement

7.1. Civil liability

7.1.1. Does the law(s) provide for civil liability for violation of Privacy Impact Assessment requirements?

Yes. In addition to the administrative fines imposed under GDPR (there are no national variations to this), non-compliance with GDPR can lead to civil liability and damages claims from individuals in accordance with general tort law.

Citation	Articles 209 and 216 of the Act

Applicable persona	Not applicable.

7.1.2. What monetary penalties are available under the law(s)?

There are no national law variations from the GDPR.

Citation	There are no national law variations from the GDPR.
Applicable persona	Not applicable.

7.2. Criminal liability

7.2.1. Does the law(s) provide for criminal liability for violation of Privacy Impact requirements?

No criminal liability is triggered directly by a violation of the GDPR requirements regarding DPIAs. However, any refusal to comply with a corrective order or injunction ordered by the supervisory authority is punishable with a criminal fine between EUR 250 and EUR 15,000 (to be multiplied by an indexation factor of 8).

Citation	Article 222 of the Act
Applicable persona	Not applicable.

Topics: Privacy Impact Assessments

Jurisdictions: Belgium