Feedback on the EDPB DPIA Template by ICTRecht

To: European Data Protection Board

ICTRecht, a legal consultancy firm specialising in various areas of IT law (including privacy, artificial intelligence, and information security) in the Netherlands, hereby submits its feedback on the published Data Protection Impact Assessment template (hereinafter: the DPIA template) of the European Data Protection Board (hereinafter: EDPB). In this response, we first provide a number of general observations on the DPIA template and then indicate, paragraph by paragraph, where we have comments or propose changes.

General Observations

Below are a number of general observations on the DPIA template, along with suggested improvements.

Missing Elements

According to article 35 of the General Data Protection Regulation (hereinafter: GDPR), a DPIA must contain at least four elements. One of these elements is an assessment of the risks to the rights and freedoms of data subjects. To identify these risks, the high-risk processing activity must at minimum be tested against all principles in article 5 GDPR. The DPIA template addresses some of these principles, namely purpose limitation, lawfulness, data minimisation, and retention periods. However, the DPIA template does not include a paragraph addressing accuracy, transparency and security measures taken. Paragraph 2.3 of the DPIA template does touch on these but focuses primarily on measures and does not provide sufficient space to describe the current situation of the processing activities (whereas this is in fact provided for the principles of purpose limitation, data minimisation, retention periods, and lawfulness).

We therefore propose expanding paragraph 2 of the DPIA template to include a clear representation of the current situation for each GDPR principle. This representation would then also include which measures have already been taken for each principle.

Furthermore, paragraph 0 lacks a description of the data subject. While other roles are introduced, a description of who the data subject is in relation to the processing activity should also be included separately.

Additionally, a paragraph is missing that provides a clear description for each data subject right in relation to the processing activities. Paragraph 2 does mention data subject rights but only asks for measures taken and an assessment of whether those measures are appropriate. However, whether a data subject right can be properly exercised in a processing activity depends not only on whether measures have been taken. It should describe whether and how a right is exercised, not merely which measures have been taken and if they are sufficient.

Table Format

The DPIA consists entirely of tables in which answers can be entered. While tables often provide useful overviews in a DPIA, they also limit quality in certain places. The tables make the DPIA unnecessarily long because some paragraphs (particularly paragraph 1.1.d) require a thorough description. The table format actually encourages the writer to keep descriptions brief, which diminishes rather than enhances the quality of the DPIA.

ICTRecht
Jollemanhof 12
1019 GW Amsterdam
020 663 1941
contact@ictrecht.nl
www.ictrecht.nl
Chamber of Commerce 72602651
VAT NL859169820.B01
IBAN NL64 RABO 0334 0962 94

We therefore propose that tables are only used where necessary (for example, to provide an overview of processing activities with corresponding purposes, retention periods, and personal data) and avoiding tables where descriptions are expected (for example, when describing processing activities).

Analysis by paragraph

Below, an analysis is provided for each paragraph where necessary, along with suggested improvements.

Paragraph 0.1: Controllers

Paragraph 0.1 of the DPIA template addresses the role allocation under the GDPR. For the controller, it assumes that only one controller is involved in the DPIA and that, where joint controllership exists, the other party or parties should be included in a copied table. However, processing activities may also involve other controllers who can be designated as independent controllers. The DPIA does not provide space for this.

We therefore propose amending the text *"Note: If there are Joint controllers, one table per controller, adding a row to identify their obligations and tasks"* to *"Note: If there are other controllers who are involved in the processing, copy the table below and add a row to identify their obligations and tasks regarding the processing."*

Furthermore, the table does not allow for discussion of the purpose and means that the controller determines. We recommend adding an extra row to the table asking why the party is designated as a controller (considering purpose and means).

Paragraph 0.3: Name of processing

This paragraph asks for the name of the processing. This name refers to the processing activity recorded in the register of processing activities. However, a DPIA is often carried out on multiple processing activities that take place within the same process, such as a recruitment process or a data warehouse. Multiple processing activities occur within such a process which, if all processing activities present a high risk, are assessed in the same DPIA. The current setup of the DPIA template restricts this too much and is not scalable for 2 or more processing activities. The resulting risk is that multiple DPIAs must be carried out containing duplicate information because the processing activities fall within the same process.

We therefore propose that the DPIA template asks for the name of the process to which the DPIA relates and not linking it to the processing activities from the register of processing activities. This link to this register occurs later in the DPIA by naming the specific processing activities for which a high risk exists.

Paragraph 0.4: Planning of the processing

This paragraph addresses the date on which the processing activity will take place and when it may end. According to the GDPR, a DPIA must be carried out prior to the processing. In practice this is often not the case and a DPIA can be carried out retrospectively or during implementation of a processing activity. This would result in the risk that this DPIA template is not used for high-risk processing activities that are already in use. Additionally, there is no option here for updating the DPIA when the processing is reassessed.

We therefore propose adding an option where it can be described if the processing activity is already in use and an option that shows whether the DPIA is being updated.

Paragraph 0.5: DPIA Technical sheet

The first question in the table in paragraph 0.5 addresses changes to the DPIA template. However, changes to a DPIA template should not be necessary. If changes are indeed

necessary to properly conduct a DPIA on a high-risk processing activity, then this indicates that the DPIA template itself is not adequate. Additionally, we see no reason to provide justification for changes to a DPIA template.

We therefore propose removing this question from the DPIA template.

The third question in paragraph 0.5 addresses the guidelines, standards, codes of conduct, and other sources used for conducting the DPIA. However, we do not consider it necessary to mention guidelines (such as EDPB guidelines or standards) as sources for preparing a DPIA. After all, these guidelines must already be complied with.

We therefore propose only asking for relevant sources that provide substantive additions to the content of the DPIA.

The fourth question in paragraph 0.5 addresses the reason for conducting the DPIA. Point 3 of this question refers to the nine criteria published by the EDPB. If two or more of these nine criteria are met, a DPIA must be conducted. However, a tenth option is added, namely the *"other"* option. Including this in the list of criteria creates confusion in relation to the rule that two or more of the nine criteria must be met.

We therefore propose removing this option from this list and including it in point 4 of the fourth question in paragraph 0.5.

Paragraph 1.1.a: Processed personal data

In the table in this paragraph, for each category of personal data it is requested to indicate what type of personal data it concerns and whether the category constitutes as special personal data. However, the options *"sensitive"* or *"criminal"* are not included as types to assign. Although the GDPR does not distinguish sensitive personal data as a separate category, and personal data of a criminal nature are mentioned in the GDPR but not further defined,[1] it is common practice to include these types (alongside normal and special category data) when categorising personal data.

In addition to the above, we note (as also observed earlier in paragraph 0.3) that personal data are not immediately linked to a processing activity. By immediately including a processing activity to which the personal data are linked, along with the corresponding types of personal data, this creates a better overview of the processing activities taking place within the process to which the DPIA relates.

We therefore propose adjusting the table to the following format:

#	Processing activity	Category personal data	Type personal data (normal, sensitive, special or criminal)	Data subject
1				

Paragraph 1.1.b: Purpose of processing

In the table in this paragraph, the purposes for which personal data are processed are introduced. As noted earlier, we recommend including processing activities in this DPIA. These processing activities can then be linked to a purpose. A combination can then be made in the same table with paragraph 1.1.c, where compatibility of purposes is requested. By merging both tables, a clear overview is created of which purpose applies to which processing activity and whether there is compatibility between both purposes.

[1] Article 10 GDPR

We therefore propose adjusting the table to the following format:

#	Processing activity	Purpose: specific and explicit reasons for processing the personal data	Original purpose (if the purpose is a secondary purpose)	If applicable, explain why the original purpose and secondary purpose are compatible	Personal data involved
1					

Paragraph 1.1.d: Nature, scope and context of the processing

This paragraph addresses the nature, scope, and context of the processing activities. The three questions asked here show some overlap, which may result in duplicate answers. Additionally, a description of the nature, scope, and context of the processing activities should appear earlier in the DPIA (namely before paragraph 1.1.a). This is where the processing activities taking place within the process can be described. More context can then be provided about the origin of the processing, in which system the processing takes place, how this system works, and which technologies are involved. Finally, we note that the table format, as mentioned earlier, does not lend itself well to drafting a thorough answer.

We therefore propose merging the three questions in this paragraph into one question, namely: *"Describe the nature, scope and context of the processing (such as the operations involved, technologies used, volume or scale of the data subjects and personal data, geographical and organisational reach, frequency or duration for the data subject, use cases, supported business processes, status of the controller and relationship with the data subjects, categories of data subjects and potentially vulnerable groups, cross-border processing, international transfers)."*

Paragraph 1.2: Functional description

In the table on functional description, a new term is introduced, namely *"processing phase or stage"*. Additionally, it asks to indicate what type of processing activity is involved. The new term creates confusion as it is unclear what this refers to (this could be a purpose or part of a processing activity).

We therefore propose linking the table again to processing activities, with the following suggested format:

#	Processing activity	Type of operations	Explanation
1			

Paragraph 1.3: Means of processing, supporting assets and underlying architecture

This paragraph addresses, as also noted in the explainer accompanying the DPIA template, which assets are used to facilitate the processing activities. However, paragraph 1.1.d already partially covers this. We therefore expect that duplicate answers will be given in both paragraphs.

We recommend combining this paragraph with paragraph 1.1.d to avoid duplicate answers.

Paragraph 1.4: Compliance with approved codes of conduct

This paragraph addresses compliance with certain codes of conduct. However, the scope of a DPIA does not extend to whether a processing activity complies with a code of conduct. Rather, it concerns the elements mentioned in Article 35(4) GDPR.

We therefore see no reason to include this paragraph, as it falls outside the scope of conducting a DPIA. We propose removing this paragraph.

Paragraph 2.1.b: Reasons to lift the processing prohibition

This paragraph addresses the exceptions for processing special categories of personal data. While the exceptions mentioned are correct, these exceptions may be further specified by national legislation. This national legislation should therefore also be mentioned in the DPIA template where applicable.

We therefore propose replacing *"justification"* with: *"Justification (if applicable, mention any national legislation that further justifies the reason to lift the processing prohibition)".*

Paragraph 2.2.a: Data minimisation and retention periods

This paragraph addresses both data minimisation and retention periods. While both topics should be covered in the DPIA, combining them is not logical and creates confusion.

Data minimisation involves testing the necessity of all categories of personal data processed per processing activity. This test comprises of a proportionality element and a subsidiarity element. This paragraph partially requests this test to be carried out, but paragraph 3 then requests it again in more detail.

To avoid duplicate answers, we propose changing the table to the following format and removing paragraph 3 in its entirety:

#	Processing activity	Justification for the proportionality	Justification for the subsidiarity	Are alle personal data necessary?
1				

In the format above, we have omitted recipients and retention periods. For recipients, we propose keeping these parties in paragraph 0 and not mentioning them further here. For retention periods, we propose creating a new paragraph within paragraph 2 with the following format:

#	Processing activity	Reference point	Retention period	Legal regulation of justification for retention period
1				

In the format above, we have also added a new column: the reference point. This reference point indicates from which moment the retention period commences.

Paragraph 2.2.b: Data quality

This paragraph addresses data quality and asks for *"Quality metrics, requirements or thresholds"* per category of personal data. However, it is unclear to us what is meant by this and what exactly is being asked. Further clarification is needed.

Paragraph 2.3.a: Measures supporting compliance with principles in Article 5(1)(a-f) GDPR

This paragraph further addresses all principles under the GDPR. However, this paragraph does not discuss how the processing activities comply with the principles of the GDPR. Instead, it only asks which measures have already been taken in relation to the processing activities and whether these measures are appropriate and effective. A discussion of the latter is then requested to be included in a small cell within the table in this paragraph. However, when a substantive justification is provided, this can result in an unreadable DPIA with lengthy tables.

We therefore propose, as mentioned earlier, creating a separate paragraph for each principle in which the current situation is described in relation to that principle.

Paragraph 2.3.c: Measures supporting compliance with other GDPR requirements

This paragraph addresses other aspects of the GDPR that may need to be complied with. However, we note that the arrangement referred to in article 26 GDPR is missing from this list. We therefore propose adding a row to this table with the following text: *"Relationship with other controllers (Article 26 GDPR)".*

Paragraph 3.1: Impacts of the processing on the rights and freedoms of data subjects

This paragraph addresses the consequences for data subjects arising from the processing activities. While it is appropriate to address this, we see considerable overlap with paragraph 4, where the risk assessment is actually conducted. We therefore consider that this paragraph should not be included here but rather be merged with paragraph 4.

Should you have any further questions following this feedback, please do not hesitate to contact us.

Kind regards,
ICTRecht