Data Protection Impact Assessment for Delivery of Online Assessments by Organization Name

Author: put here your name
Date: put here the date of the DPIA

About this template
This template is provided by Questionmark to aid customers in carrying out a Data Protection Impact Assessment (DPIA) on processing of personal data within the scope of the EU General Data Protection Regulation (GDPR) using Questionmark’s European OnDemand Service. (If you are using Questionmark’s US OnDemand Service, a similar template is available.).

This template is provided in good faith by Questionmark but each organization uses Questionmark products in different ways, and this template should be considered as general information only, that you may consider for your needs. We hope this template will be helpful, but Questionmark provides no warranty that it will meet your needs or that of regulators. This template is neither legal advice nor contractual in effect. It is for customers to decide whether processing of personal data using Questionmark’s European OnDemand Service requires completion of a DPIA.

The template is copyright Questionmark Computing Limited © 2017. It is licensed under a Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0/). You are free to share and adapt but must give the copyright holder attribution.

This template is current as of 12th November 2017. We’d welcome suggestions for how it can be improved. Please email john@questionmark.com with any comments. This template does not constitute legal advice, is provided for general information purposes only and is not contractual in effect. Questionmark does not warrant that this template is suitable for any particular purpose and disclaims all liability in respect of its use.

Suggestions on how to fill in this template

To use this template:
1. Gather information about your assessment project – ensure that you have full information and background.
2. Check in with your Data Protection Officer or other individual responsible for privacy whether your organization or its supervisory authorities have guidelines about DPIAs
3. You may want to consult with data subjects (see section 5 of the DPIA template).
4. Read through this template and highlight areas which need information or attention
5. Go through the template in detail
   - Text in blue italics are suggested instructions and should be removed once you follow them
   - Text in amber is to be filled in and replaced with your details.
   - Text in black is possible text to use but should be amended with text of your own that meets your needs better

The final document should meet your needs, and you should not feel the need to stick with the template wording.
# Table of Contents

1. Overview ................................................................................................................................. 3  
   Introduction ............................................................................................................................. 3  
   Project details ......................................................................................................................... 3  

2. Description of operations of the envisaged processing operations ........................................... 5  
   Processing operations ............................................................................................................. 5  
   Assets including processors and sub-processors .................................................................... 6  
   Personal data captured ............................................................................................................ 6  

3. Necessity and proportionality .................................................................................................. 8  
   General reasons why assessments are beneficial ................................................................... 8  
   Legitimate interests ............................................................................................................... 8  

4. Risks and measures .................................................................................................................. 10  
   Risk methodology .................................................................................................................. 10  
   Threats to personal data ......................................................................................................... 10  
   Risks related to breach of confidentiality or integrity ............................................................. 11  
   Risks related to loss of personal data .................................................................................... 12  
   Risks related to mis-classification ........................................................................................ 12  
   Risks related to exercise of data subject rights in data protection law ................................. 14  

5. Supporting information .......................................................................................................... 15  
   Codes of conduct .................................................................................................................. 15  
   Views of data subjects .......................................................................................................... 15  
   Consultation with data processing officer (DPO) ................................................................. 15  

6. Conclusion ............................................................................................................................... 16  
   Summary ............................................................................................................................... 16  
   Residual risk ........................................................................................................................ 16  

---

**Data Protection Impact Assessment**

v.5.2.2018.18:48
1. Overview

Introduction
This document is a Data Protection Impact Assessment (DPIA) evaluating the use of online assessments using Questionmark’s European OnDemand Service by Organization Name. The DPIA is an analysis of expected processing activities related to assessments and covers details of the processing activity itself and an assessment of the risks associated with the processing activities including any measures that need to be taken to mitigate those risks. It also contains the decision on whether to initiate a prior consultation with the relevant DPA.

This DPIA is being performed due to the requirement that per Article 35 of the GDPR, where processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out an assessment of the impact of the envisioned processing.

This DPIA is based on a template by Questionmark (www.questionmark.com) but has been modified by our organization and reflects our independent and genuine analysis of the impact of our use of assessments.

Assessments have value to individuals, organizations and society. This DPIA assesses the risks to personal privacy of the assessment process and identifies the measures, safeguards and mechanisms in place to mitigate those risks, and identifies whether the necessity of processing personal data balances out the privacy rights of collecting and processing the data.

Project details

The table below sets out key information about the project:

<table>
<thead>
<tr>
<th>Key Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) Data Controller</td>
</tr>
<tr>
<td>Organization name</td>
</tr>
<tr>
<td>Usually the organization who is filling in the DPIA will be the data controller, but if there is a joint data controller or other circumstances, note it here.</td>
</tr>
<tr>
<td>(b) Description of project</td>
</tr>
<tr>
<td>This impact assessment covers the creation, delivery and reporting on assessments by &lt;Organization name&gt; for &lt;put in the general area of use e.g. workplace learning or certification&gt;.</td>
</tr>
<tr>
<td>(c) Purpose of project</td>
</tr>
<tr>
<td>Please fill in the purpose of using assessments, for example:</td>
</tr>
<tr>
<td>• To review the competence of workers for business purposes and to ensure regulatory compliance</td>
</tr>
<tr>
<td>• To assess students as part of formative learning and for summative purposes to give grades</td>
</tr>
<tr>
<td>• As part of the process to issue a formal certification</td>
</tr>
<tr>
<td>(d) Context, scope and background</td>
</tr>
<tr>
<td>Recital 90 of the GDPR suggests you should take into account the context and scope. Include here a short description of the scope of the project and the context</td>
</tr>
<tr>
<td>(e)</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(f)</th>
<th>Types of personal data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The main personal data captured is identification data for the data subject including name and email address and assessment answers and scores including pass/fail. See section 2 below for more details on personal data captured.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(g)</th>
<th>Special categories of data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Special categories of data are not captured.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(h)</th>
<th>Recipients of personal data: who will be able to see and have access to assessment results</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The following roles will have access to assessment results</td>
</tr>
<tr>
<td></td>
<td>• Fill in who is able to see results data, for example your internal team and any external stakeholders who get to see assessment results</td>
</tr>
</tbody>
</table>
2. **Description of operations of the envisaged processing operations**

**Processing operations**

This section of the DPIA gives a systematic description of the envisaged processing operations for the project. *Please adjust this description if your assessments process works in a different way. You could also add further details.*

A functional description of the process follows. The envisaged processing operations can be divided into six phases as shown below:

1. **Planning assessment.**
   Prior to authoring questions or an assessment, a design process defines the goals of the assessment. Part of this process defines topics within an item bank in which questions are placed. An authoring process is then defined with authors given roles within Questionmark OnDemand to allow them to create and review questions and assessments.

2. **Authoring questions.**
   Authors are responsible for writing questions (also called items) which are entered into and stored in Questionmark OnDemand. Depending on the purposes of the assessment, questions are reviewed within our organization and Questionmark OnDemand holds the history of the questions including the details of review and changes made.

3. **Construct and finalize assessment.**
   An author then constructs an assessment using the questions authored in the previous step and ensuring that the assessment meets the design needs. In many cases, there is also a pilot and review stage by us to ensure this. Part of the process is to set a pass/fail or cut score. The assessment is then published within the Questionmark OnDemand platform and scheduled for participants to take.
   *If you use an LMS, you might add here “The assessment is made available within the organization’s Learning Management System” or similar.*

4. **Deliver to participants.**
   Participants take the assessment by logging in and answering the questions. Personal data and answers to questions are recorded at this time and stored in the Questionmark OnDemand system.
5. **Reports available.**
   Once a participant finishes an assessment, Questionmark OnDemand calculates scores using the criteria defined by Questionmark OnDemand. We have a review process to ensure that scores are calculated correctly and an appeals process in case of participant concern. *(Modify if appropriate to reflect your organization practices.)*

6. **Results shared.**
   After the assessment, we make results available to participants and the roles identified in the key project details. Results can be made available by logging into Questionmark OnDemand or by exporting reports including in PDF format. Such reports typically contain personal data.

### Assets including processors and sub-processors

This section of the DPIA contains a list of the assets through which personal data processing takes place, both internal and external to the organization.

1. **Internal IT**
   Personal data necessarily flows through the personal computers and internal computer systems of Organization name. We use reasonable security measures to ensure the safety of our systems and to train our employees in security. *Add to this if appropriate.*

2. **Questionmark Computing Limited of 30 Coleman Street, London EC2R 5AL (“Questionmark”)**
   Questionmark supply the cloud-based, Questionmark OnDemand system on which assessments are conducted. Questionmark’s technical and organizational measures are documented at [www.questionmark.com/go/eu-od-measures](http://www.questionmark.com/go/eu-od-measures). Questionmark’s sub-processors are documented at [www.questionmark.com/go/eu-od-subprocessors](http://www.questionmark.com/go/eu-od-subprocessors).

*Further processors should be added, for example if you are using an LMS and LMS users have access to assessment data, you might add the LMS supplier. Also add any significant assets used to run the project, for example any test centers used or any software or systems used to analyze results.*

### Personal data captured

This section describes at a high level the types of personal information captured on participants.

The following general information may be captured on participants:

- First and last name
- Email address
- Language selected to take assessments in
- The group or category within the organization that the participant is associated with
- Date/time user was created and last logged in

*Please add to or amend this list if you use Questionmark to capture further or different general information about a participant, e.g. demographics or organizational status. Please also add to this list if you capture authentication/identity information, e.g. when proctoring the exam. And also add to this list if you capture any information as part of the assessment process outside Questionmark software.*
For each assessment delivered, the following information is also captured and is associated with the person taking the assessment:

- Name of the assessment
- IP address of the device on which the assessment is taken
- User agent string of browser (which gives details of which browser the participant is using and some limited information on the device used)
- Language browser is running in
- Date/time of test starting
- Date/time of answering each question (in some cases also the time taken to review and answer the question)
- The answer given by the participant to each question, along in some cases with any textual comment by the participant
- Feedback set by the assessment author given to the participant
- Information derived by Questionmark from the answers including the score and outcome to each question and the score and outcome to the assessment
- Whether the assessment is passed or failed

If you integrate with Questionmark using SAML, a learning management system or call assessments from another system, you may need to add any personal information passed through from the calling system.

If you use Questionmark for surveys or to capture demographic information as part of a test, quiz or exam, you should include any personal information you capture in such questions within this part of the template. In particular, if you ask for any information about race, religion or anything covered by the GDPR’s special data categorization, you should definitely describe.
3. Necessity and proportionality

General reasons why assessments are beneficial

Before considering the specific rationale for this project, it’s helpful to consider the general benefit of assessments to society.

One of the great benefits of assessments is that they give equality of opportunity. Open public examinations let people from any origin show merit. Since their invention in Imperial China, exams have become a powerful way to give equality of opportunity to all and encourage advancement by merit and not by nepotism or chance.

Assessments are the one of the most effective ways to measure knowledge, skills and attitudes. A properly constructed assessment gives objective data about competence. Without measurement of competence, it is hard for individuals to improve their own competence or organizations to help others improve. As the scientist Lord Kelvin famously said: “If you cannot measure it, you cannot improve it”.

Assessments make our society and the world safer. Medical professionals, aircraft pilots, air traffic controllers, power station workers, and even anyone who drives a car, has to pass an exam. There are still accidents and mistakes, but we are all safer than we would be without assessments.

For employers, assessments provide a way in which they can evaluate the competence of their workforce and direct training or other improvement to their personnel. They also provide a way of ensuring regulatory compliance with rules that require them to ensure competence of their personnel.

For universities, colleges and awarding or certification bodies, assessments are a key way in which they can assess their participants and confirm that they have the learning or skills that the body seeks to impart or confirm. A university degree or a certification of competence would be less valuable and trustable if it had not been properly assessed.

For individuals, the availability of assessments provides an opportunity for all of us to demonstrate competence and achievement and allow others to see it.

Legitimate interests

Organization Name delivers assessments as described in the key information at the front of this DPIA. It’s a required part of the assessment process that information is gathered from participants in order for them to be able to demonstrate competence, and it’s required for the integrity of the assessment process for this information to be retained as evidence and justification of the assessment results. We have a legitimate interest in assessing as follows:

(It’s unlikely that all the below will apply to you. Please adjust, deleting the ones that do not apply and adding or modifying others. You are looking to explain why you have a legitimate interest in delivering assessments and that these reasons are valid and strong and justify the minor privacy invasion of processing their personal data.)

As an employer, we test our personnel and external partners in order to
- Identify skills and knowledge gaps
- Improve our personnel skills
- Ensure that our personnel know our products, services and procedures
- Meet regulatory compliance needs
- Help ensure that our workforce is competent
- Help measure the quality of our training programs

As a learning organization, we test our learners in order to
- To help students learn and to encourage students them to study
- Inform ourselves on areas to improve our teaching
- Provide a basis on which to award qualifications or certificates

As a certification body, we assess our candidates because:
- This is an intrinsic part of what issuing a certification requires
- It allows candidates to demonstrate their competence and knowledge
- It allows stakeholders to be able to trust the value of the certificates we offer

(Please add further information on why your assessments are beneficial and adjust the text above appropriately.)
4. Risks and measures

Risk methodology
This section considers the risk to natural persons, in this case participants in the assessment process. Other risks which apply to the organization, but which do not impact privacy, are out of scope. What is in scope are risks which could lead to physical, material or non-material harm to the data subject, including any discrimination, damage to reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage.

In our analysis, all risks are also associated with a probability:

- **Likely.** Strong (high) chance that the documented scenario could occur. High risks are going to occur from time to time, for example equipment failure in a situation where no redundancy is in place.
- **Possible.** Medium (neutral) chance that the documented scenario could occur. Between low and high.
- **Unlikely.** Scenario is unlikely – should not happen more often than once in a decade, or rarer.

Risks are also associated with a severity.

- **Critical.** There is significant, real damage to a large number of data subjects, for example a large scale data breach.
- **Severe.** There is significant, real damage to one or a small number of data subjects or else more minor damage to a large number of data subjects.
- **Moderate.** Minor or procedural issue that does not lead to significant damage.

*Note – you should review the probability and severity of risks in your environment. For instance, just because the template suggests that a risk is unlikely does not mean that it will be in your environment. For example, if you are storing sensitive data, the risk severity might increase.*

Threats to personal data
Before analyzing risks in detail, we need to consider the likely threats. From the perspective of the data subject, here are the likely threats to privacy:

1. **Disclosure of personal data.** A participant will consider the information given the assessment provider as confidential and could be distressed or suffer damage to reputation if it were leaked inappropriately. For example, a participant would not expect information that he/she had answered an easy or important question wrongly to be publicly disclosed, and would be concerned about assessment results being shared inappropriately.

2. **Integrity of personal data.** A data subject would be concerned if assessment data about them was inaccurate, for example was damaged in transit or misclassified with data about another person or modified incorrectly.

3. **Loss of personal data.** If a participant takes an exam and the results are lost, then he or she has lost important evidence of competence. A data subject would be concerned that assessment results are stored safely for as long as needed.

4. **Someone fails an assessment unfairly.** A serious concern for a data subject is that they should not fail the assessment if they have the competence to pass it. For example, if the system were to mix one person’s results with another, or to have an error in scoring, or if the assessment isn’t fair, valid and reliable, then a data subject who should pass might be failed. And that may have consequences for the data subject.
Passing an assessment when someone should fail is a less serious concern for the data subject, but it is a concern for society and the organization and for other data subjects, as it devalues the results of the assessment for other people. And it’s a legitimate interest of our organization that such mis-classifications should not happen.

5. **Lack of ability to exercise rights under data protection law.** A data subject has many rights under data protection law and could be concerned for example about being unable to obtain copies of their personal data or data being processed inappropriately.

*Please add any other threats that you think your participants will be concerned about, including any genuine ones raised in any consultation you do with your participants.*

The following sections deal with risks relating to these threats, considering separately:
- Breach of confidentiality or integrity threats (1 and 2 above)
- Threats to loss or availability of personal data (3 above)
- Mis-classification threats (4 above)
- Lack of rights under data protection law (5 above)

*The following sections will not likely address all risks and you should include any other risks identified when carrying out your DPIA process. You should assess likelihood, severity and mitigation measures based upon the circumstances of your organization and how it uses Questionmark OnDemand.*

**Risks related to breach of confidentiality or integrity**

The table below shows representative risks related to breach of confidentiality or integrity.

<table>
<thead>
<tr>
<th>ID</th>
<th>Nature of risk</th>
<th>Likelihood</th>
<th>Severity</th>
<th>Mitigations and measures in place</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Interception of data during transmission while assessment being taken or while results being reported (man in the middle attacks or wire sniffing)</td>
<td>Possible</td>
<td>Severe</td>
<td>All transmissions to and from Questionmark OnDemand use well configured, strong encryption via TLS 1.0 or higher.</td>
</tr>
</tbody>
</table>
system is guessed or found or obtained via phishing attack to allow access to results or other data in the Questionmark system or in organizational systems

Adjust to “Possible” if you think there is a larger risk here

attacks, we use a password policy in Questionmark that enforces complex passwords and we use the Questionmark role system to give access to administrators only to the information they need to limit access in the event of a compromise.

Please adjust the above depending on your policies. If you are using SAML to login to Questionmark, replace or supplement above with a statement saying that organization login is used to protect access to Questionmark.

5 Information is retrieved by access to organization systems

Unlikely

Critical

Put in a brief statement explaining how you deal with potential attacks on your own organization infrastructure.

Please add any other risks that you think should be appropriately included here.

Risks related to loss of personal data

The table below shows representative risks related to loss of data or deletion of data. Note that many of the risks above relating to confidentiality could also result in deletion of data.

<table>
<thead>
<tr>
<th>ID</th>
<th>Nature of risk</th>
<th>Likelihood</th>
<th>Severity</th>
<th>Mitigations and measures in place</th>
</tr>
</thead>
</table>
| 6  | Failure of backup means permanent loss of assessment results                    | Unlikely   | Severe   | Questionmark has many mitigations in place to prevent this:
|    |                                                                                 |            |          | • High level of redundancy in cloud setup                                                                                                                      |
|    |                                                                                 |            |          | • Questionmark conducts backups at least daily.                                                                                                               |
|    |                                                                                 |            |          | • Backups are made, encrypted over Internet to a vault company which is ISO 27001 certified                                                                 |
|    |                                                                                 |            |          | • Questionmark conducts restore tests to confirm backup integrity at least quarterly.                                                                           |
|    |                                                                                 |            |          | • Questionmark has a business continuity plan which undergoes regular testing                                                                                   |
| 7  | Disruption during an assessment (e.g. equipment failure, connectivity failure, fire alarm) loses data and requires participant to retake assessment | Likely     | Moderate | Questionmark OnDemand has a “save as you go” capability which means that each answer can be recorded when made and it’s possible to resume/restart an assessment after technical failure, meaning that when issues happen, data should not be lost. |
| 8  | Short term cloud availability issue means temporary unavailability of results     | Likely     | Moderate | Questionmark targets availability of 99.9% and downtime is rare. The short term loss of availability of assessment personal data is unlikely to be a significant concern to data subjects. |

Risks related to mis-classification
<table>
<thead>
<tr>
<th>ID</th>
<th>Nature of risk</th>
<th>Likelihood</th>
<th>Severity</th>
<th>Mitigations and measures in place</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>A data subject fails an assessment due to an error in the assessment authoring process, for example because the assessment is not valid and reliable</td>
<td>Possible</td>
<td>Severe</td>
<td>Our organization puts lots of effort into making sure that our assessments are valid and reliable including the following <em>(adjust as necessary for your organization):</em>&lt;br&gt;• Blueprinting the assessment to ensure it meets needs&lt;br&gt;• Putting questions in an item bank with topic structure to organize them well&lt;br&gt;• Involving subject matter experts in question design and review&lt;br&gt;• Using a professional authoring system (Questionmark) which retains versions of questions during design and otherwise helps us make professional assessments&lt;br&gt;• Careful allocation of pass scores based on objective data&lt;br&gt;• Use of topic scoring to provide a breakdown of competence by topic&lt;br&gt;• Use of item analysis reports to weed out poor quality or ambiguous questions&lt;br&gt;We also provide opportunities for retakes so that if someone does fail, they can retake the assessment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unlikely</td>
<td>Severe</td>
<td>We use the industry leading Questionmark system which is widely used for reliable assessment delivery and errors are unusual. In the event of an IT failure, it’s usually possible to resume the exam and always possible to retake it.</td>
</tr>
<tr>
<td>11</td>
<td>Questions being exposed by one of our authors selling or disclosing them to participants.</td>
<td>Unlikely</td>
<td>Severe</td>
<td>Were this to happen it would devalue the assessment process and we protect against this by <em>(modify as appropriate):</em>&lt;br&gt;• Educating our content authors on the importance of security&lt;br&gt;• Using Questionmark’s role and access system to only give people access to what they need to know&lt;br&gt;• Reviewing results data to spot trends (e.g. hard questions becoming easier)</td>
</tr>
<tr>
<td>12</td>
<td>Cheating via unauthorized help. For example a data subject uses a cheat sheet.</td>
<td>Possible</td>
<td>Moderate</td>
<td>Describe briefly your measures to protect against this.</td>
</tr>
<tr>
<td>13</td>
<td>Cheating by impersonation. For example a data subject pays someone else to take the test for them.</td>
<td>Possible</td>
<td>Moderate</td>
<td>Describe briefly your measures to protect against this.</td>
</tr>
</tbody>
</table>
### Risks related to exercise of data subject rights in data protection law

<table>
<thead>
<tr>
<th>ID</th>
<th>Nature of risk</th>
<th>Likelihood</th>
<th>Severity</th>
<th>Mitigations and measures in place</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>Participants cannot have access to personal data held on them</td>
<td>Unlikely</td>
<td>Moderate</td>
<td>We will respond according to legal requirements to any data subject requesting information. We can provide comprehensive information on assessment attempts and results using Questionmark reports.</td>
</tr>
<tr>
<td>15</td>
<td>Risk that data is processed by a processor not meeting data protection requirements</td>
<td>Unlikely</td>
<td>Moderate</td>
<td>Our contract with Questionmark and other sub-processors is compliant with the GDPR or will be by May 25, 2018.</td>
</tr>
<tr>
<td>16</td>
<td>Personal data is retained longer than it is needed</td>
<td>Unlikely</td>
<td>Moderate</td>
<td>In order to maintain the evidence to justify assessment results, we do keep assessment results for a considerable period. However our organization ensures that we do not keep results longer than necessary and will also respond to appropriate requests from data subjects to remove data.</td>
</tr>
</tbody>
</table>

Clearly as an organization, you will be committed to following the GDPR. Please add to the risk table above any additional items that should be included.
5. Supporting information

Codes of conduct

Article 35(8) of the GDPR says that approved codes of conduct may be taken into account in a DPIA, but at the time of writing there are no such approved codes of conduct. Please adjust the following if your organization does adopt an approved code of conduct.

Article 35(8) of the GDPR states that a DPIA may take into account compliance with approved codes of conduct. Since no relevant codes of conduct are available at present, we have not taken into account any such codes of conduct, however we have taken into account that the processor, Questionmark, the provider of the Questionmark OnDemand system, is ISO 27001 certified.

Views of data subjects

Article 35(9) of the GDPR states that where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing.

Insert here whether you have consulted potential data subjects or their representatives. If you did do so, summarize their responses and how their concerns (if any) are being addressed. If you did not, document the justification for not doing so.

Consultation with data processing officer (DPO)

If a DPO is designated, the DPO does not need to create the DPIA but you must get advice from the DPO when carrying out the DPIA. Put here the date you got advice and a summary of the advice or if you have no DPO, put not applicable for this reason.
6. Conclusion

Summary

In previous parts of this DPIA, we have
- Described the project and given a functional overview
- Described the personal data that has been captured
- Identified the purpose of the processing and the legitimate interests in conducting such processing
- Identified the risks to privacy of data subjects and the mitigations in place for them

We now need to consider whether residual high risk remains and whether there is a need to consult the supervisory authority.

Residual risk

Under the GDPR, it is necessary to consult the supervisory authority prior to processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. Essentially, if the residual risk after mitigations taken remains high, then the supervisory authority needs to be consulted.

The Article 29 Working Party guidance on DPIAs give examples of unacceptable high residual risk:

a) instances where the data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (e.g.: an illegitimate access to data leading to a threat on the life of the data subjects, a layoff, a financial jeopardy)

b) when it seems obvious that the risk will occur (e.g.: by not being able to reduce the number of people accessing the data because of its sharing, use or distribution modes, or when a well-known vulnerability is not patched).

There are no risks within our assessment processes where it seems obvious that the risk will occur. Our organization runs its assessment program professionally and mitigates risks to a high extent. The bullet point (b) does not seem to apply to us. There are two areas where we have considered that the first bullet point (a) might apply.

1. Data breach. There is a small risk of data breach, in the event for instance of a successful cybersecurity attack. The consequences on data subjects could be significant and irreversible depending on the data involved in the breach, however there are a considerable array of mitigations in place against a data breach, in line with and likely in excess of industry standards, and although information on assessment results is highly confidential, it is not as serious as disclosure of some other types of information – for example financial information that could lead to identity theft. It does not seem that residual risk in this area is high.

2. Mis-classification. Were a data subject to fail an assessment unfairly, for example because questions were ambiguous or more broadly the assessment was not valid or reliable, then the data subject could suffer a significant consequence. However, this risk is mitigated by:
   - Substantive measures in place including those described above to ensure the reliability and validity of the assessment;
   - The ability for the data subject to retake the assessment;
   - An appeal process where the data subject can ask for their assessment result to be reviewed.

(Please adjust above to take account of your retake and appeal processes and also how severe a consequence it is to fail an exam in accordance with your particular organization’s procedures.)

(Please review the following sentence carefully.) The data controller has concluded that considering the mitigations in place, there are no residual high risks and that therefore there is no need to consult the supervisory authority.