Draft of May 2020

Template – Basic privacy risk assessment

{{ client }}

# Introduction

This questionnaire is intended to enable {{ client }} to understand privacy risks in connection with the services or processes that you are assessing for the {{ client }}. This questionnaire must be completed before you start processing of personal data and will in some situations require that you complete further risk assessment steps.

This questionnaire does not contain a risk assessment of suppliers, security or high risk situations – this must be done separately if required.

First of all we need some basic information from you:

|  |
| --- |
| Name, title and e-mail of the person filling out this form: |
| {# Question  Give name, title and e-mail of the person filling out this form  Logic  Insert answer  #}  Person filling out this form:  Name: {{ creator }}  Title: {{ creator.position }}  E-mail: {{ creator.email }} |

|  |
| --- |
| Date of filling out this form: |
| {# Question  Give date of filling out this form  Logic  Insert answer #}  {{ creation\_date }} |

|  |
| --- |
| Responsible entity |
| {{ client }}  Company registration number: {{ client.CVR }}  {{ client.address\_block() }}  {#  Question  Insert full name of the {{ client }} legal entity responsible for the processing or activity  Logic  Text to be inserted #} |
| DPO |
| {{ DPO }}  {#  Question  Insert e-mail of DPO to receive notification  Logic  Text to be inserted  #} |

|  |
| --- |
| Project/activity name |
| {{ risk\_project\_name }}  {#  Question  Insert full name of the project  Logic  Text to be inserted  #} |

Thank you.

Now we would ask you some questions in relation to the process, activity or project where we will be focusing on risks.

This questionnaire assess the basic risks when processing personal data and is linked to other relevant assessments if required.

When filling out the questionnaire have in mind the risks {{ client }} wants to avoid is personal data being copied, transmitted, viewed, accessed, stolen or used by an individual unauthorized to do so – **imagine how personal data could likely be misused and what impact it would have on the relevant data subject**.

|  |
| --- |
| *When deciding on the risk both the likelihood and the severity of any impact on the data subjects you are processing personal data about the following should be taken into account, e.g.:*   * *what type of personal data will be used, i.e. sensitive, confidential or ordinary personal data,* * *who are your data subjects and are they vulnerable in the given situation, i.e. consumers, children, elderly etc.,* * *by whom the personal data will be used, i.e. employees of {{ client }}, partners, suppliers etc.,* * *for what purpose the personal data will be used, i.e. marketing, HR, profiling, combining data sets, analysis etc., and* * *where the personal data will be used, i.e. within the EU or outside the EU.* |

And remember! - Involve stakeholder expertise where relevant to answer the questions diligently.

|  |
| --- |
| Key stakeholders |
| {# Question  Identify names and e-mail addresses of   1. Process, activity or project owner 2. Group Legal contact 3. IT- security manager   Logic  Insert answer #}  Process, activity or project owner:  {{ risk\_project\_owner }}  Group Legal contact:  {{ risk\_group\_legal\_contact }}  IT-security manager:  {{ risk\_it\_security\_manager }} |
| Scope of the project and solution description: |
| {# Question  Describe in detail and in your own words the scope of the processing activity, process or project and how personal data is involved.  Logic  Insert answer {{ scope }} #}  {{ risk\_scope }} |
| Purpose of the processing of personal data: |
| {# Question  Select the purpose that describes the processing of personal data:  Logic   User support   Application maintenance   Back-up services   Data analysis   Designing or implementing marketing solutions   Designing or implementing cookie solution   Designing or implementing direct marketing   Designing or implementing HR solutions   Data storage   Hosting   Other please specify below If this box is ticked this needs to trigger a low risk  #}  {{ risk\_purpose }} |
| Types of processing |
| {# Question  Select the types of processing that is relevant to the processing of personal data and the purpose  Logic  If two boxes or more are ticked this needs to trigger a high risk at the end.   The processing involves sensitive data or data of a highly personal nature   The processing involves evaluation or scoring including profiling and predicting behaviour   The processing involves automated-decision making with legal or similar significant effect   The processing involves data processed on a large scale   The processing involves systematic monitoring including processing used to observe, monitor or control data subjects   The processing involves matching or combining dataset   The processing involves personal data concerning vulnerable data subjects   The processing involves innovative use or applying new technological or organisational solutions   The processing in itself “prevents data subjects from exercising a right or using a service or a contract  #}  {{ risk\_types\_of\_processing }} |
| Types of personal data |
| {# Question  Select the types of types of personal data processed  Logic  If one of the red boxes are ticked this needs to trigger a medium risk at the end.   Name   E-mail address   Telephone number   Address   Payment details   CV information   Username   Age   Gender   IP address   Marital status   Next of kin   National identification number   Criminal convictions and offences   Racial or ethnic origin   Political opinions   Religious or philosophical beliefs   Trade union memberships   Genetic data   Biometric data with the purpose of identification   Health data   Data on data subjects sex life or sexual orientation   Other please specify below If this box is ticked this needs to trigger medium risk wih the description at the end.  #}  {{ risk\_types\_of\_personal\_data }} |
| Data sources |
| {# Question  How will personal data be collected?  Logic  If one of the red boxes are ticked this needs to trigger a medium risk and prompt two new questions: describe 1. Who will be delivering the personal data? 2. How will the personal data be delivered? Answers to be filled into the conclusion at the end.   From own existing data   To be collected from data subjects   From third parties  #}  {{ risk\_data\_sources }} |
| Data subjects |
| {# Question  Select the category of data subjects on whom personal data is being processed  Logic  If one of the red boxes are ticked this needs to trigger a medium risk at the end.   Employees   Customers   Suppliers/vendors   Children   Elderly   Patients   Other please specify below  #}  {{ risk\_data\_subjects }} |
| The legal basis for processing the personal data |
| {# Question  In identifying the legal basis for the {{ client }} when processing the personal data, select the situation you think matches the processing of personal data best. There might be more than one legal basis if you have several purposes that you are fulfilling.  Logic  For ordinary personal data:   We will be collecting a consent from the data subject   We will be fulfilling a contract with the data subject   We are required by law to process the personal data   We are processing the personal data in order to protect the vital interests of the data subject or another natural person   We are processing the personal data in the public interest or in the exercise of official authority vested in the {{ client }}   We are pursuing a legitimate interests that overrides the interests or fundamental rights and freedoms of the data subject  For sensitive personal data:   We will be collecting an explicit consent from the data subject   We are processing personal data necessary for the purposes of carrying out the obligations and rights in the field of employment and social security and social protection law   We need to process the personal data to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent   We are a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim where our processing relates solely to our members or to our former members or to persons who have regular contact with us in connection with our purposes and that the personal data are not disclosed outside that our organisation without the consent of the data subjects   We are processing personal information that relates to personal data which are manifestly made public by the data subject   We are processing personal data necessary for the establishment, exercise or defence of legal claims   We are processing personal data necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued   We are processing personal data necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional   We are processing personal data necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law   We are processing personal data necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law  National identification numbers   We are processing national identification numbers  Personal data relating to criminal convictions and offences   We are processing personal data relating to criminal convictions and offences or related security measures based on Union or Member State law  #}  {{ risk\_legal\_basis }} |
| Purpose limitation |
| {# Question  Is it ensured that only personal data strictly necessary for the purpose(s) of the processing will be collected?  Respondent to choose from either option 1 or option 2:  Option 1:  Yes  Logic  No action  Option 2:  No  Logic  This needs to trigger a medium risk at the end.  #}  {{ risk\_purpose\_limitation }} |
| Technology used |
| {# Question  Which types of technology are applied in the processing of personal data?  Logic  Insert answer  *[E.g. databases, web portals, social medias, biometric, RFID or TV-surveillance etc.]*  *#}*  {{ risk\_tech\_used }} |
| Data flow |
| {# Question  Have you done a data flow?  Logic  Respondent to choose from either option 1 or option 2:  Option 1:  Yes  Logic  Upload the data flow  Option 2:  No  Logic  Based on the information provided by you, please draw a data flow overview using the below as an example and upload the flow:  #}  {{ risk\_data\_flow }} |
| Place of storing |
| {# Question  Where is the personal data being stored?  Logic  Insert answer  *[E.g. physical location of servers.]*  *#}*  {{ risk\_storage\_place }} |
| Type of storing |
| {# Question  On which assets is the personal data stored?  Logic  Insert answer  *[E.g. is the personal data recorded, processed, transferred and/or held on hardware, software, networks, people, paper or paper transmission channels]*  *#}*  {{ risk\_storage\_type }} |
| Access to personal data |
| {# Question  Who has access to the personal data?  Logic  Respondent to choose from either option 1 or option 2:  Option 1   {{ client }} employees  Specify department of {{ client }}:  If option 1 is chosen move to the question “Time of storing the personal data”  Option 2   Third parties  Logic  If option 2 is chosen move to the question “Third party access”  #}  {{ risk\_access\_to\_personal\_data }} |
| Third party access |
| {# Question   1. Which third party has access to the personal data - specify details of company name, company reg.no., address and contact person. 2. Why does the third party have access to the personal data?   Logic  Respondent to answer questions.  #}  {{ risk\_third\_party\_access }} |
| Time of storing the personal data |
| {# Question  Will the personal data retained in accordance with {{ client }} guidelines on retention and deletion?  Logic  Respondent to choose from either option 1 or option 2:  Option 1:  Yes  Logic  No action  Option 2:  No  Logic  This needs to trigger a medium risk and prompt one new question: for how long will the personal data be retained? Answers to be filled into the conclusion.  #}  {{ risk\_storage\_time }} |
| Procedure for deleting the stored data |
| {# Question  Will the personal data be deleted in accordance with {{ client }} guidelines on retention and deletion?  Logic  Respondent to choose from either option 1 or option 2:  Option 1:  Yes  Logic  No action  Option 2:  No  Logic  This needs to trigger a medium risk and prompt one new question: how will the personal data be deleted. Answers to be filled into the conclusion at the end.  #}  {{ risk\_procedure\_deleting\_data }} |
| Information to the data subjects |
| {# Question  Have the data subjects been provided with the required information as laid out in the Check List on Information to Data Subjects [Link]]  Logic  Respondent to choose from either option 1 or option 2:  Option 1:  Yes  Logic  No action  Option 2:  No  Logic  If option 2 is chosen this needs to trigger a low risk and prompt two new questions: 1. describe which required information has not been given. 2. How will the information be given to the data subject. Answers to be filled into the conclusion at the end.  #}  {{ risk\_information\_to\_subjects }} |
| Use of third party processors, vendors, suppliers etc. |
| {# Question  Has {{client}} engaged any third party data processors, vendors, suppliers etc. as part of the processing activity or project?  Respondent to choose from either option 1 or option 2:  Option 1:  Yes  Logic  Please state names and company details and prompt next question on “Supplier risk assessment”  Option 2:  No  Logic  No action and skip next question on “Supplier risk assessment” and “Data processor agreement”  #}  {{ risk\_use\_third\_party\_processors\_etc }} |
| Supplier risk assessment |
| {# Question  Has {{client}} done a supplier risk assessment?  If option 2 is chosen this needs to trigger the Supplier risk assessment tool at the end.  Respondent to choose from either option 1 or option 2:  Option 1:  Yes  Logic  Attach the assessment  Option 2:  No  Logic  If option 2 is chosen this needs to trigger the Supplier risk assessment tool at the end.  #}  {%p if risk\_use\_third\_party\_processors\_etc %}  {{ risk\_supplier\_risk\_assessment }}  {%p else %}  N/A  {%p endif %} |
| Data processor agreement |
| {# Question  Has {{client}} entered into a data processor agreement or joint data controller agreement?  Respondent to choose from either option 1 or option 2:  Option 1:  Yes  Logic  Attach the data agreement  Option 2:  No  Logic  If option 2 is chosen this needs to trigger a medium risk at the end and prompt an action to use {{ client }} data processor agreement templates or if the supplier’s data processor agreement is used, please use the check list on data processor agreements available here [insert link] and upload after completion.  #}  {%p if risk\_use\_third\_party\_processors\_etc %}  {{ risk\_dpa }}  {%p else %}  N/A  {%p endif %} |
| Transfer of personal data outside of the EU/EEA |
| {# Question  Will personal data be transferred outside of the EU/EEA as part of the processing activity or project?  If option 1 is chosen it needs to trigger a low risk at the end.  Respondent to choose from either option 1 or option 2:  Option 1:  Yes  Logic  Describe in which country outside the EU/EEA personal data will be processed?  Option 2:  No  Logic  No action  #}  {{ risk\_transfer\_outside\_EUEEA }} |
| Security requirements |
| {# Question  Has security features been planned or is already in place in relation to the project?  Logic  Respondent to choose from either option 1 or option 2:  Option 1:  No  Logic  Trigger medium risk at the end.  Option 2:  Yes  Logic  The check boxes should appear with the following question:  “Please tick the box relevant for the project:”  Organisational security   * The {{client}} has a documented information security policy that addresses how information security is ensured in the {{client}}’s organisation.   Physical Security   * Sites, including data centres, offices and off-site storage facilities, or locations from where the {{client}}’s data can potentially be accessed, have appropriate physical security controls to protect against unauthorised access.   System and Network Security   * Networks and devices on which personal data are processed, are protected from unauthorised access or infiltration, both internally and externally.   Access Management   * The {{client}} ensures that the {{client}}’s personal data is only accessed by authorised persons, through the means of access management procedures that ensure access on a least privilege basis and that access is terminated where and when it is appropriate.   Logging   * All access to personal data are logged and the access log includes the date and time of access, the UserID and the type of access (read, edit, delete, search criteria etc.).   Back-up   * The {{client}} performs back-up of the personal data processed and has procedures in place to ensure the re-establishing of backed-up data in a timely manner to ensure the availability and access to personal data.   If one or more boxes are left unchecked this needs to trigger medium risk at the end.  #}  {{ risk\_security\_requirements }} |

|  |
| --- |
| Based on the data flow mapping and the risk assessments the following risk and mitigating actions have been identified: |
| Triggers and answers to be inserted:   |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |
| Conclusion of risks and need to activate the data protection impact assessment (“DPIA”) process |
| {# Question  Are any of the risks high and/or are two or more of the risks medium?  Logic  Respondent to choose from either option 1 or option 2:  Option 1:  Yes  Logic  E-mail the risk assessment to the technical lead of the project and activate next step  Option 2:  No  Logic  Proceed to legal risk assessment tool  #}  {{ risk\_conclusion\_and\_next\_steps }} |