GDPR Record template

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Summary of Changes** |
| 6.1 | 2020-04 | * Added version control table * Added structure using headings |
| 6.2 | 2020-05-14 | * Indicated whether Template & Phase descriptions are visible to end user * Deleted section ‘Plan Details’ * Adjusted Template description * Adjusted Phase descriptions (distinguish between standalone template, institutional & funder template) * Adjusted Section descriptions * Replaced the term “FAQ” with “guidelines” in Guidance * Removed hyperlinks to Dutch Onderzoektips in Guidance * Made some adjustments in questions/answers/guidance text to streamline this template with the Dutch translation of the template (AVGTemplate v1) |
| 6.3 | 2020-06-8 | * Update guidance in phase 2 ‘DPIA’, question 1 |
| 6.4 | 2020-10-22 | * Correct link to DPIA templates (see Question 1 in DPIA phase, question-specific guidance) |

# Template description

[!This description only applies to the standalone GDPR Record template; not to ‘regular’ DMP templates which contain the GDPR Record & DPIA phases]

Template for researchers who need to **record personal data processing activities** (and, if the latter constitute a probable high risk, also conduct a **Data Privacy Impact Assessment** or DPIA), but who are not writing an extensive Data Management Plan (DMP).

For more information, check the guidelines on [how to register personal data processing activities](https://onderzoektips.ugent.be/en/tips/00001795/).

# Phase 1: GDPR Record

## Phase description

[!Three versions exist. One for the standalone GDPR Record template, one for the GDPR Record phase as part of an institutional DMP template, and one as part of a funder DMP template.]

### Standalone GDPR Record template

This part of the template is for Ghent University and Ghent University Hospital researchers who are collecting or processing personal data, and therefore need to record these personal data processing activities in order to **comply with the General Data Protection Regulation (GDPR)** and the [**Code of Conduct for the processing of personal data and confidential information at Ghent University**](https://www.ugent.be/en/ghentuniv/privacy/code-of-conduct-personal-data.htm).

* As institutions, Ghent University and Ghent University Hospital in principle bear the liability and ultimate responsibility for the lawful and secure processing of personal data and for compliance with the GDPR. However, based on the principle of empowerment, this **responsibility is shared with the person(s) responsible for the research**, i.e. the supervisor and/or leader of the research group and the other participants in the research (possibly also students).
* To demonstrate ongoing compliance with the GDPR and the Code of Conduct of Ghent University, researchers processing personal data need to **maintain a digital record of those processing activities**. Such records should be created before the start of data collection and kept up to date during the research. Afterwards researchers should conduct their research in accordance with the requirements and safeguards documented in this register.

This template presents researchers with an overview of the information they need to provide to comply with the GDPR requirement to record all processing activities, and points them to the possible risks they need to take into consideration before, during or after a research project. The careful and lawful processing of personal data is essential for creating good scientific outcomes.

The **scope** of the GDPR is rather broad; it concerns the protection of individuals when their personal data are processed, in order to safeguard their fundamental rights to privacy and data protection.

### GDPR Record phase as part of an institutional DMP template

The following ‘GDPR’ sections are not part of the [insert template name] template as such, but are included here because you have indicated in the ‘Create Plan’ wizard that you are processing personal data. Therefore, you have to comply with the **General Data Protection Regulation (GDPR)** and the [**Code of Conduct for processing personal data and confidential information at Ghent University**](https://www.ugent.be/en/ghentuniv/privacy/code-of-conduct-personal-data.htm).

Compliance includes **recording your personal data processing activities by completing the questions** in the following ‘GDPR’ sections. Personal data processing activities should be registered before the start of data collection, and this record should be kept up to date during research. Moreover, you should conduct your research in accordance with the requirements and safeguards documented in this record.

See the [guidelines on how to register personal data processing activities](https://researchtips.ugent.be/en/tips/00001795/) for more information.

### GDPR Record phase as part of a funder DMP template

The following ‘GDPR’ sections are not part of the [insert template name] template as such, but are included here because you have indicated in the ‘Create Plan’ wizard that you are processing personal data. Therefore, you have to comply with the **General Data Protection Regulation (GDPR)**.

Compliance includes **recording your personal data processing activities by completing the questions** in the following ‘GDPR’ sections. Personal data processing activities should be registered before the start of data collection, and this record should be kept up to date during research. Moreover, you should conduct your research in accordance with the requirements and safeguards documented in this record.

## SECTION: Collection and processing of personal data

|  |  |  |
| --- | --- | --- |
| **SECTION description:**  When you collect or process personal data in your research, you must take the requirements of the GDPR into account. These requirements apply both when you collect personal data yourself, either directly or indirectly from the data subject and for a specific purpose (primary use), and when you reuse personal data that was previously collected, possibly for another purpose, by yourself or someone else (secondary use).  When processing personal data, it is important to inform the persons concerned (also called the ‘data subjects’) about this processing (principle of ***transparency***), even if it concerns secondary use of personal data. | | |
| **Question** | **Answer Format** | **Question-specific guidance** |
| 1. **Are you collecting or processing personal data?** | Radio buttons (only one option can be selected):  □ Yes (default)  □ No | Personal data are any information relating to an identified or identifiable natural person, i.e. a living individual (also called a 'data subject'). Examples of personal data include but are not limited to name, address, email address, photo, ID number, IP address, employee number, private or professional telephone number (who-is-who), login details, identification cookies, account number, CV, log data (e.g. cafeteria, parking use, web use), camera images, personnel files, wage data, professional expenses, health data, ...  For more information see this [guideline on what are personal data](https://onderzoektips.ugent.be/en/tips/00001781/). |
| 1. **In what format are you collecting or processing the personal data?** | Checkboxes (multiple options can be selected):  □ Digital  □ On paper |  |
| 1. **Are you collecting or processing primary personal data and/or secondary personal data?** | Checkboxes (multiple options can be selected):  □ Primary personal data  □ Secondary personal data | **Primary personal data** implies that you are collecting the personal data directly or indirectly from the data subject for a specific purpose. For example, this is the case when you are collecting personal data via surveys.  **Secondary personal data** means that you reuse personal data that was collected previously, possibly for another (research) purpose, by yourself or by someone else.  In many research projects there will be a combination of primary and secondary personal data.  For more information see this [guideline on secondary processing of personal data](https://onderzoektips.ugent.be/en/tips/00001788/). |
| 1. **If you are processing secondary personal data, will you inform the persons whose personal data are being processed or have they already been informed?** | Radio buttons (only one option can be selected):  □ Yes  □ No | If you are processing secondary personal data, it remains important to be transparent to the data subjects. This means that you should inform the data subjects of this new processing of their data.  In the case of processing secondary personal data, you can be excepted from providing this information if providing this information would require a disproportionate amount of effort, or if it would make impossible or seriously jeopardise the achievement of the purposes of the processing. In this case, you need to explain in the next question why you need to deviate from the data subject’s right to be informed.  For more information see this [guideline on transparency towards data subjects](https://onderzoektips.ugent.be/en/tips/00001791/). |
| 1. **If no, explain why it is impossible or why it would take a disproportionate effort to inform the persons whose personal data are being processed.** | Text area |  |
| 1. **How will the personal data be processed?** | Check boxes (multiple options can be selected):  □ Anonymised (explain below)  □ Pseudonymised (explain below)  □ Raw personal data, i.e. non-pseudonymised or non-anonymised (explain below) | According to the principle of data minimisation and the processing for research purposes, it is advisable to process the data in an anonymised or at least pseudonymised form when possible.  **Pseudonymised** personal data (referred to as 'coded data' in previous Privacy legislation) are personal data (whether sensitive or not) that can only be associated with an identified or identifiable person by means of a non-public (secret) key. Pseudonymised personal data are still personal data protected by the GDPR.  With **anonymised** personal data, the possibilities for identification have been 'irreversibly' removed by means of a processing technique.  Keep in mind that the **handling or process of anonymisation** itself still falls under the scope of the GDPR.  Data that can be traced back to the original individuals with reasonable effort (i.e. by use of additional information or keys) are not anonymous data, but remain personal data and therefore fall under the GDPR.  Use the comment box below to describe why you will process the data in a certain way (anonymised/pseudonymised/other). For example: the data will be pseudonymised for patient safety, the data cannot be anonymised because of follow-up on therapy, necessary quality control, …  For more information see this [guideline on what are personal data](https://onderzoektips.ugent.be/en/tips/00001781/). |
| 1. **If you are going to process personal data in a pseudonymised form, describe the method of pseudonymisation, where you will keep the key, and who has access to it.** | Text area | Pseudonymised personal data are personal data (whether sensitive or not) that can only be associated with an identified or identifiable person by means of a non-public (secret) key.  This non-public (secret) key or additional data or key should be kept separate from the pseudonymised data and should be subject to technical and organisational measures (such as restricted access) to protect the data from re-identification.  Examples of pseudonymisation methods (creating the non-public key) are scrambling, encryption and masking.  Pseudonymised personal data are still personal data protected by the GDPR.  For more information see [this guideline on what are personal data](https://onderzoektips.ugent.be/en/tips/00001781/). |

## SECTION: Categories of personal data & data subjects

|  |  |  |
| --- | --- | --- |
| **SECTION description:**  ***Data minimisation*** is an important principle of the GDPR. It means that you should only process personal information that is necessary for obtaining the objectives of your research.  In the following questions you are asked to document which categories of personal data you are collecting/processing, and who the people are whose personal data you are collecting/processing. | | |
| **Question** | **Answer Format** | **Question-specific guidance** |
| 1. **Are you collecting/processing any of the following special categories of data?** | Check boxes (multiple options can be selected):  □ Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union memberships  □ Data from/ linked to the Electronic Patient File (EPD)  □ Genetic data  □ Biometric data for the purpose of uniquely identifying a natural person, such as audio recordings of voices, fingerprints, facial images, iris scans  □ Data concerning health (physical and mental health), an individual’s sex life, or an individual’s sexual orientation  □ Forensic data  □ Data relating to criminal convictions and offences  □ None of the above | For more information see this [guideline on special categories of personal data](https://onderzoektips.ugent.be/en/tips/00001840/). |
| 1. **Which other categories of personal data are you collecting/processing?** | Check boxes (multiple options can be selected):  □ Identification data (names, titles, addresses, phone numbers, passport numbers, IP addresses, cookies, electronic location data (GPS, mobile phone)…)  □ Financial details (bank account numbers, expenses, loans, …)  □ Personal characteristics (age, gender, date of birth, marital status, nationality…)  □ Physical characteristics (height, weight…)  □ Psychological details (personality, character…)  □ Leisure activities and interests (hobbies, sports…)  □ Consumption patterns  □ Education and training  □ Lifestyle habits  □ Household composition; family membership  □ Home characteristics  □ Occupation and profession  □ National insurance number  □ Audio and video recordings  □ Other (please specify below) |  |
| 1. **Whose personal data are you collecting/processing?** | Check boxes (multiple options can be selected):  □ Children below the age of 13  □ Children between the ages of 13 and 16  □ Children over the age of 16  □ Other vulnerable persons (e.g. pregnant women, elderly persons, people with mental disorders, asylum seekers, disabled persons, ethnic minorities, sick people or patients)  □ Co-workers from UGent / UZ Gent  □ Others (please specify below) | Vulnerable persons often concern persons who are not legally competent, persons who are not able to give their consent, or persons who may suffer very adverse consequences if their personal data become publicly available.  Processing data from children and/or other vulnerable persons may entail further specific requirements (e.g. consent from a parent/legal guardian, a prior Data Protection Impact Assessment…).  Indicate ‘co-workers from UGent or UZ Gent’ if you are processing logging data of co-workers from UZ Gent in the EPD, or data of co-workers from UZ Gent who are involved during a clinical trial (i.e. CV, GCP certification,…).  Indicate ‘others’ if you are processing other persons’ personal data such as participants’ visitors during a clinical trial, administrative information of parents, …  For more information see this [guideline on vulnerable persons](https://ugentbe.sharepoint.com/teams/CA20.DataStewardTeam/RDM%20services%20%20projects/DMP%20support/Templates/For%20more%20information%20see%20this%20FAQ%20on%20vulnerable%20persons.). |
| 1. **Will your research be seriously hampered if the persons whose personal data are being collected/processed exercise their right to access, to rectification, to restriction of processing, to be forgotten, to data portability and/or to object?** | Radio buttons (only one option can be selected):  □ Yes  □ No | As a researcher, you have to take into account that data subjects can exercise different rights with regard to the processing of their personal data:   * **Right of access**: a data subject can ask whether personal data are processed about him/her, which categories of personal data are processed, why they are processed and with whom they are shared. * **Right to rectification**: if the data are not correct, the data subjects can ask to correct or supplement them. * **Right to be forgotten**: in a number of cases and circumstances, the data subjects can have their personal data deleted. * **Right to restriction of processing**: if certain criteria are met, data subjects can ask you to (temporarily) stop processing their personal data. * **Right to data portability**: data subjects can request the transfer of personal data, processed by automated means and on the basis of their consent or the conclusion of a contract with the controller, in a structured, commonly used and machine-readable format. * **Right to object** to certain use of personal data and to automated decision-making and profiling.   Within a research context, some rights of the data subjects may be limited to a greater or lesser extent in specific circumstances, namely when exercising these rights seriously impedes the research objectives or threatens to make them impossible. If this is the case for your research, it is important to clearly explain for each right involved the need to deviate from it (in the next question).  For more information see this [guideline on data subjects' rights](https://onderzoektips.ugent.be/en/tips/00001790/). |
| 1. **If yes, please justify the need to deviate from one or more of the rights mentioned in question 11. A justification is required for each deviation.** | Text area | An example of a need to deviate from one of the rights and of the associated motivation is if you are conducting a clinical trial and you cannot guarantee the right to access because this will jeopardise your methodology or research results. |

## SECTION: Purpose(s) of the processing

|  |  |  |  |
| --- | --- | --- | --- |
| **SECTION description:**  According to the principles of ***lawfulness*** and ***purpose limitation***, personal data should be processed based on an appropriate legal ground and for a specified and explicit purpose.  In the following questions you will be asked to clearly define the purpose and the legal ground of the processing. | | | |
| **Question** | **Answer Format** | | **Question-specific guidance** |
| 1. **What is/are the purpose(s) of the personal data processing?** | Text area | | Describe in detail the purpose(s) for which the personal data are intended.  E.g. the personal data shall be processed in biomedical research, a clinical trial, in a social study, … |
| 1. **What is the legal ground for the processing? If the data are being processed for multiple purposes, you must describe the legal ground for each purpose.** | | Check boxes (multiple options can be selected):  □ The research will be performed in the public interest, which means that it will lead to an increase of knowledge and insight to the direct or indirect benefit of society.  □ The individuals participating in the research have freely given their explicit consent for the processing of their personal data for one or more specific purposes.  □ The research is necessary for the purposes of the legitimate interests of Ghent University and/or Ghent University Hospital, yet results in no high risks for the individuals participating in the research.  □ The processing is necessary for the execution of an agreement with the person whose data are being processed (note that this is not about the processing agreement).  □ The processing is necessary in the context of a legal obligation of Ghent University or Ghent University Hospital.  □ The processing is necessary in order to protect the vital interests of the data subject or of another natural person. | To be lawful, the processing of personal data must be based on any one of the legal grounds mentioned in the GDPR. It is very important to carefully consider and indicate the legal ground for each purpose at the start of your research.  Note that there can **only be one legal ground per purpose** of data processing.  For more information see this [guideline on lawful processing of personal data](https://onderzoektips.ugent.be/en/tips/00001787/). |
| 1. **If you are processing special categories of personal data (see question 8), on which exception is this based?** | | Radio buttons (only one option can be selected):  □ The processing is necessary for scientific or historical research purposes.  □ The data subject has given his or her explicit consent.  □ The personal data are manifestly made public by the data subject.  □ The processing is necessary for reasons of substantial public interest.  □ The processing is necessary for reasons of public interest in the area of public health.  □ The processing is necessary for the purpose of preventive or occupational medicine.  □ The processing is necessary to protect the vital interests of the data subject or of another natural person. | To be lawful, the processing of special categories of personal data must be based on any one of the legal exceptions mentioned in the GDPR.  Note that there can **only be one exception per purpose** of data processing.  For more information see this [guideline on special categories of personal data](https://onderzoektips.ugent.be/en/tips/00001840/). |

## SECTION: GDPR responsibility

|  |  |  |
| --- | --- | --- |
| **SECTION description:**  Within the GDPR different roles are defined in the processing of personal data. The most important roles are those of controller, joint controller and processor.  Since (joint) controllers and processors have different responsibilities and obligations, it is important that you clearly define these roles (together with the other partners in your research) at the start of your research. For more information on the responsibilities and obligations, see this [guideline on the different roles in the GDPR](https://onderzoektips.ugent.be/en/tips/00001789/). | | |
| **Question** | **Answer Format** | **Question-specific guidance** |
| 1. **Which institution(s) is/are involved in the research?** | Radio buttons (only one option can be selected):  □ Ghent University  □ Ghent University Hospital  □ Ghent University and Ghent University Hospital | If the principal investigator or the researcher is affiliated with Ghent University and no patient data or other data collected within Ghent University Hospital will be used or processed within your research, **only** **Ghent University is involved**.  If the principal investigator or the researcher is not affiliated with Ghent University and patient data or other data collected within Ghent University Hospital will be used or processed within your research, **only Ghent University Hospital is involved**.  If the principal investigator or the research is affiliated with Ghent University and patient data or other data collected within Ghent University Hospital will be used or processed within your research, both **Ghent University and Ghent University Hospital are involved**.  Patient data or data collected within Ghent University Hospital include personal data, human body material (MLM), imaging, surveys etc., research projects with volunteers at UZ Gent services, e.g. D.R.U.G., CEVAC, Outpatient services.  **The Data Protection Officer for Ghent University is Hanne Elsen (**[**privacy@ugent.be**](mailto:privacy@ugent.be)**). The Data Protection Officer for Ghent University Hospital is Katya Van Driessche (**[**dpo@uzgent.be**](mailto:dpo@uzgent.be)**).** |
| 1. **Is there another university, hospital, research institute or partner involved in the research (besides Ghent University and/or Ghent University Hospital)?** | Radio buttons (only one option can be selected):  □ Yes  □ No | If there is another university, hospital, research institute or partner involved in the research (besides Ghent University or Ghent University Hospital), please specify this in question 18.  When no other university, research institute or partner is involved in the research, Ghent University or Ghent University Hospital or both of them together define the purposes (‘why’) and the means (‘how’) of the research. Please indicate this in question 18. |
| 1. **Please specify who determines the purposes (‘why’) and the means (‘how’) of the research.** | Radio buttons (only one option can be selected):  □ This is determined within Ghent University: UGent is the data controller**.**  □ This is determined within Ghent University Hospital: UZ Gent is the data controller.  □ This is determined within Ghent University and Ghent University Hospital: UGent and UZ Gent are acting as joint data controllers.  □ This is determined together with a partner outside Ghent University and/or Ghent University Hospital: UGent and/or UZ Gent is/are joint controller(s) together with said partner. Specify its contact details and data protection officer below.  □ This is determined outside Ghent University or Ghent University Hospital: UGent or UZ Gent is a data processor. Specify the contact details of the data controller and its data protection officer below. | By defining who determines the purposes (‘why’) and the means (‘how’) of the research, you will identify the GDPR responsibilities: **data controller, joint controller, data processor or sub processor**.  If **another university, hospital, research institute or partner** (besides Ghent University and/or Ghent University Hospital) is involved in the research, you need to **specify the contact details** of said other university, hospital, research institute or below: this includes name, address, company number, legal status, name and contact details of the data protection officer.  For more information see this [guideline on roles and responsibilities in the GDPR](https://onderzoektips.ugent.be/en/tips/00001789/). |

## SECTION: Data transfers & categories of recipients

|  |  |  |
| --- | --- | --- |
| **SECTION description:**  In the following questions you will be asked if you are disclosing/sharing/transferring your data, and if so, who the recipients are. | | |
| **Question** | **Answer Format** | **Question-specific guidance** |
| 1. **Are you disclosing/sharing/transferring personal data beyond your project team, either with recipients in UGent and/or UZ Gent, or with external recipients during or after your research?** | Radio buttons (only one option can be selected):  □ Yes  □ No | This question relates to the transfer of data both during and after your research. For example: transferring the data to a processor; sharing the data with a researcher from another institution; sharing your data in a data repository after the end of your research, … |
| 1. **If yes, to or with which categories of recipients are the personal data being disclosed/shared/transferred?** | Check boxes (multiple options can be selected):  □ The persons whose personal data are being collected/processed  □ Personal contacts of the data subjects  □ Other researchers within your department  □ Other researchers within UGent or UZ Gent  □ Other researchers outside UGent or UZ Gent  □ Government services/departments (provide contact details below)  □ Justice and police departments (provide contact details below)  □ Social security agencies (provide contact details below)  □ Private companies (e.g. data processors, cloud service providers, …) (provide contact details below)  □ Banks and insurance companies (provide contact details below)  □ Consultants in processing of personal data or direct marketing (provide contact details below)  □ Others (please specify below) | Specify the categories of recipients in the comment box (this includes (company) name, address, company number, legal status, name and contact details of the data protection officer) and motivate why the personal data are being **disclosed/shared/transferred.**  If said recipients are processing the data on behalf of you(**and therefore are acting as data processors**), please also indicate whether you have entered into a **data processing agreement.** |
| 1. **If yes, where are the personal data being disclosed/shared/transferred to?** | Check boxes (multiple options can be selected):  □ Belgium  □ Another country within the European Economic Area (EEA) (please specify the country below)  □ A country outside the European Economic Area (EEA) but on the European Commission’s ‘white list’ (please specify the country below)  □ A country outside the European Economic Area (EEA) and not on the ‘white list’ (please specify the country below)  □ An international organisation (please specify below, including the location of the organisation) | **Within the EEA**, the GDPR guarantees an adequate level of protection of the fundamental rights of data subjects.  For some countries **outside the EEA**, the European Commission has decided that the level of protection is adequate. These countries are on the ‘**white list’**. To see the list of countries offering an adequate level of protection, check the latest version of the [white list](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en) on the website of the EC!  When personal data are being disclosed/shared/transferred to **other countries**, additional measures should be taken.  Also note that when using **cloud services**, personal data may be stored on servers in multiple locations. Therefore, you need to check to which countries personal data are being transferred when using cloud services. If you don’t know, or if personal data are transferred to countries outside the EEA or countries not on the ‘white list’, additional measures must be taken to ensure an adequate level of data protection. |
| 1. **What is/are the purpose(s) of the data transfer?** | Text area | Describe in detail the purpose(s) for which the personal data are intended.  E.g. the personal data shall be processed in biomedical research, a clinical trial, a social study, … |
| 1. **What is the legal ground for the data transfer? If there will be multiple data transfers, you need to indicate the legal ground for each data transfer.** | Check boxes (multiple options can be selected):  □ The transfer will be performed in the public interest, which means that it will lead to an increase of knowledge and insight to the direct or indirect benefit of society.  □ The individuals participating in the research have freely given their explicit consent for the transfer of their personal data for one or more specific purposes.  □ The data transfer is necessary for the purposes of the legitimate interests of Ghent University and/or Ghent University Hospital, yet results in no high risks for the individuals participating in the research.  □ The data transfer is necessary for the execution of an agreement with the person whose data are being processed (note that this is not about the processing agreement).  □ The data transfer is necessary in the context of a legal obligation of Ghent University or Ghent University Hospital.  □ The data transfer is necessary in order to protect the vital interests of the data subject or of another natural person. | There can only be **one legal ground per data transfer**. If there are multiple data transfers, indicate the legal ground for each transfer, using the comment box to clarify which transfer is associated with which legal ground.  For example, if you are processing personal data together with a partner in a consortium for the same purpose (your research project) and the exchange of said data is necessary to obtain your research goals, the legal ground is the same as that of the initial research project you are registering. If you process the personal data on the legal ground of ‘consent’, this cooperation and your partners should be mentioned in your informed consent form or information sheet.  If you collect data within a consortium (a collaboration involving multiple institutions, universities or organisations for a research project) and you are going to transfer this data to another researcher (outside of the consortium and outside of your project) who will use it for another purpose or project, then you have to motivate the legal ground for these other purposes.  For more information see this [guideline on lawful processing of personal data](https://onderzoektips.ugent.be/en/tips/00001787/). |

## SECTION: Retention period

|  |  |  |  |
| --- | --- | --- | --- |
| **SECTION description:**  According to the principle of ***storage limitation***, personal data may not be stored longer than is necessary for the purpose for which they are processed. However, scientific research is one of the exceptions where personal data may be stored for longer periods (e.g. for reuse of data) provided that appropriate security measures are taken to protect the data.  In the next question you will be asked to define the retention period of the personal data you are processing. | | | |
| **Question** | **Answer Format** | **Question-specific guidance** | **Guidance Theme** |
| 1. **What is the envisaged retention period for the different categories of personal data? Please motivate.** | Text area | Indicate how long the data will be retained/preserved, or the criteria that will be used to determine this period for all different categories of personal data.  As a researcher, it is important to ensure that data are preserved in a location or environment with appropriate security measures to protect the confidentiality of the data during this retention period.  For example, if you are working with health data, you have to respect the retention period of the patient file for 30 years after the last patient contact.  For more information see this [guideline on how long to keep personal data](https://onderzoektips.ugent.be/en/tips/00001793/). | **Period of Preservation** |

## SECTION: Risk analysis

|  |  |  |
| --- | --- | --- |
| **SECTION description:**  Risk assessment is an important aspect of the GDPR. The following questions will enable you to evaluate the privacy risks of your processing, and indicate if you will need to take additional measures to protect the privacy of the persons whose data you are processing, as well as whether it is necessary to conduct a data protection impact assessment. | | |
| **Question** | **Answer Format** | **Question-specific guidance** |
| 1. **To analyse the possible risks associated with the processing of personal data, please tick the boxes that apply to this research.** | Check boxes (multiple options can be selected):  □ Special categories of personal data are processed in this research (see question 8).  □ Personal data of children or other vulnerable persons are processed in this research (see question 10).  □ Personal data are processed on a large scale (please consider the number of data subjects concerned, either as a specific number or as a proportion of the relevant population).  □ Aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements are evaluated or scored, profiled or predicted.  □ The data are transferred beyond the borders of the EU or the EEA, or to a country not listed on the ‘white list’ (see question 21).  □ The research involves datasets that have been or will be matched or combined.  □ The processing aims at taking decisions producing legal effects concerning the data subject or similarly significant effects for the data subject. For example, the processing may lead to exclusion of or discrimination against individuals.  □ The processing prevents data subjects from exercising a right or using a service or a contract.  □ The research involves the systematic monitoring of persons in one or more publicly accessible areas.  □ The research involves innovative use or application of technological or organisational solutions, like combining the use of finger print and face recognition for improved physical access control.  □ The research involves the processing of non-pseudonymised personal data. |  |
| 1. **Does the research constitute a probable high-risk processing? If you ticked two or more boxes in question 25, the answer is ‘yes’.** | Radio button (only one option can be selected):  □ Yes  □ No | If you ticked two or more boxes in question 25 (i.e. the data processing planned in your research constitutes a probable high risk), a **Data Protection Impact Assessment** or DPIA must be performed to further identify the privacy risks related to the processing.  You must complete the section on ‘Data Protection Impact Assessment’. You can navigate to it via the ‘DPIA’ tab in this template. |

## SECTION: Security measures

|  |  |  |  |
| --- | --- | --- | --- |
| **SECTION description:**  When you process personal data, you have the ethical and legal obligation to ensure that personal data are adequately protected (principle of ***integrity and confidentiality***). In the following questions, you will be asked to document the technical and organisational security measures that you will take to protect the data. | | | |
| **Question** | **Answer Format** | **Question-specific guidance** | **Guidance theme** |
| 1. **What technical and organisational security measures are in place to protect personal data?** | Check boxes (more than one option can be selected):  □ I hereby confirm that I carry out my research in accordance with the guidelines on information security of UGent and/or UZ Gent.  □ Additional security measures will be or have been taken (please specify below). | The basic level of security must always be in accordance with the guidelines on information security of the institution or organisation.  However, additional measures may be necessary for each processing. The choice of the additional security measures is based on an assessment of the risks of the processing. A more risky processing will have to be accompanied by a more extensive set of security measures.  For more information see the [information security](https://www.ugent.be/en/facilities/ict/information-security) page from Ghent University, and the [guidelines](https://www.ugent.be/en/facilities/ict/information-security) from Ghent University Hospital. | **Data Security** |
| 1. **If you have motivated the need to deviate from one or more of the rights of the persons whose personal data you are collecting/processing in question 11 and 12, please describe which safeguards are put in place to protect their rights and freedoms.** | Text area | An example of a need to deviate from one the rights and of the associated motivation is if you are conducting a clinical trial and you cannot guarantee the right to access because this will jeopardise your methodology or research results. To protect the rights and freedoms of thepersons whose personal data you are collecting/processing, you will need to ensure additional safeguards such as pseudonymisation, restricted access to said data, a trusted third party. |  |

# Phase 2: DPIA

## Phase description

[!Two versions exist. One for the standalone GDPR Record template, and one for the DPIA phase as part of a DMP template.]

### Standalone GDPR Record template

If the personal data processing planned in your research constitutes a **probable high risk** (see questions 25 and 26 of the ‘GDPR record’ component in this template), a **Data Protection Impact Assessment** (DPIA) must be performed to further identify the privacy risks related to the processing.

The following questions (together with template DPIAs) will help you to identify privacy risks and assess the impact your research will or might have on the privacy and fundamental rights of the data subjects.

For more information, see the guideline ‘[When am I processing high-risk personal data and when do I need to conduct a DPIA?](https://researchtips.ugent.be/en/tips/00001853/)’.

### DPIA phase as part of an institutional DMP template

The following ‘DPIA’ section is not part of the [insert template name] template as such, but is included here because you have indicated in the ‘Create plan’ wizard that you are processing personal data.

If the personal data processing planned in your research constitutes a **probable high risk** (see questions 25 and 26 of the ‘GDPR Record’ component in this template), a **Data Protection Impact Assessment** (DPIA) must be performed to further identify the privacy risks related to the processing.

The following questions (together with template DPIAs), will help you to identify privacy risks and assess the impact your research will or might have on the privacy and fundamental rights of the data subjects.

For more information, see the guideline ‘[When am I processing high-risk personal data and when do I need to conduct a DPIA?](https://researchtips.ugent.be/en/tips/00001853/)’.

### DPIA phase as part of a funder DMP template

The following ‘DPIA’ section is not part of the [insert template name] template as such, but is included here because you have indicated in the ‘Create plan’ wizard that you are processing personal data.

If the personal data processing planned in your research constitutes a **probable high risk**, a **Data Protection Impact Assessment** (DPIA) must be performed to further identify the privacy risks related to the processing. The following questions will help you to identify privacy risks and assess the impact your research will or might have on the privacy and fundamental rights of the data subjects.

## SECTION: Data Protection Impact Assessment

|  |  |  |  |
| --- | --- | --- | --- |
| **SECTION description: Data Protection Impact Assessment**  If the data processing planned in your research constitutes a **probable high risk** (see questions 25 and 26 in the ‘GDPR Record’ tab), a **Data Protection Impact Assessment** (DPIA) must be performed to further identify the privacy risks related to the processing. The following questions (together with template DPIAs), will help you to identify privacy risks and assess the impact your research will or might have on the privacy and fundamental rights of the data subjects.  For more information, see the guideline ‘[When am I processing high-risk personal data and when do I need to conduct a DPIA?](https://researchtips.ugent.be/en/tips/00001853/)’. | | | |
| **Question** | **Answer Format** | **Question-specific guidance** | **Themed guidance** |
| 1. **Does your research fall under the scope of a template DPIA?** | Radio button (only one option can be selected):  □ Yes (specify below)  □ No | For **research at/in collaboration with UZ Gent**: since a DPIA can also relate to a series of comparable processing activities (or research projects) that entail comparable high risks, one DPIA can be created/used for this. A DPIA template has already been developed for retrospective and prospective research carried out at Ghent University Hospital.  These [templates](https://intranet.uzgent.be/bad/2017/Paginas/documenten.aspx) can be consulted at the UZ Gent intranet and used as an inspiration to complete the DPIA section in DMPonline.be. |  |
| 1. **Provide more details for any of the risks that you have ticked in question 25 under the ‘GDPR record’ tab, so the overall risks related to your processing are clearly and accurately described.** | Text area | Describe the possible risks or harms to the data subjects, third parties and/or communities associated with the processing of personal data within your research. You can do this by taking into account the risk of discrimination, stigmatisation, data leaks (disclosure of the persons' identity or sensitive data, or damage to their reputation through a breach of confidentiality), threats to the safety of participants, and the possible abuse of the research methodology or findings.  For example: if you have indicated that you will be processing special categories of personal data on a large scale, provide more information on why this can be a risk for the persons whose personal data you are collecting, on what is at stake for them or for their community. In the following questions you will need to describe how you have mitigated or will mitigate this risk.  Another example: if you have indicated that you will be matching or combining special categories of data, describe what data will be matched and combined. The combination of certain data might increase the risk of re-identification for the data-subjects, which might put them at risk. Describe this risk. |  |
| 1. **Explain why the processing of personal data is necessary to achieve the purposes of the research. Include the benefits for individuals and the wider public.** | Text area | Describe the results you will achieve or to which you will contribute with this research, and their added value for the data subjects and society at large.  For example: large-scale processing of special categories of data might be necessary to ensure that all possible participants and outcomes are represented (to avoid bias) and that your research outcome is valid.  Another example: the combination of certain datasets might provide you with more insights than not combining them would. The combination of multiple datasets might also be necessary to ensure that your research outcome is valid. |  |
| 1. **Can the processing or part of the processing reasonably be achieved in a different/alternative way, less detrimental to the privacy of data subjects? Evaluate the possible alternatives.** | Radio button (only one option can be selected):  □ Yes (specify below)  □ No | If the processing can be achieved in a different/alternative way which is less detrimental to the privacy of the data subjects, please describe and evaluate the alternatives (less harmful to those involved). Keep in mind that the data subjects are the persons whose personal data are processed.  For example: you are creating an algorithm and in order to test it, you need to run it on personal data. It might not be necessary to use real personal data; an alternative, less harmful way might be to work with dummy data.  It is also possible that you have already gone through various alternatives before arriving at the present research. If so, describe which alternatives there are and why they are (not) applicable to your research. |  |
| 1. **Describe the steps, measures or controls you are taking to minimise the risk to privacy and safeguard the rights of the persons whose personal data you are collecting.** | Text area | Explain how the rights of the persons whose personal data you are collecting/processing will be safeguarded by describing the (security) measures and steps you have taken. Describe which measure addresses which risk and what the residual risk is after implementation of the measure. If the measure does not completely eliminate the risk, justify why the residual risk is acceptable.  For example:   * Pseudonymisation of personal data * Encryption of stored data at rest * Encryption during transfers * Fellow researchers and partners will receive compliance training on data protection and information security. * Hashing will be used. * Randomisation will be used. * Probalistic risk management * Research participants can opt out at any stage of the research. * Personal data will not leave the EU. * Research will not be used to make decisions directly affecting individuals. * Short retention periods will be used. * Restricted access controls * The risk of stigmatisation is mitigated by working with large population sizes, by adding ‘noise’ to the data; a helpline is provided for data subjects…. * … |  |
| 1. **Describe the steps you have taken to make sure the research is as accurate as possible and there are minimal unintended consequences.** | Text area | For example, you have a data management plan in place which will be kept up to date, your data management plan was reviewed (by peers or other persons), the research builds on a pilot study, … |  |
| 1. **Is the (possible) negative effect or risk for the privacy of the data subjects in reasonable proportion to the processing purposes?** | Radio button (only one option can be selected):  □ Yes  □ No (specify below) |  |  |
| 1. **How would you describe the likelihood of the risk(s) after having completed the previous questions in this DPIA?** | Radio button (only one option can be selected):  □ Negligible  □ Limited  □ Important  □ Maximum | Indicate how likely the risks identified in your research are to happen, after the security, technical and organisational measures you have taken.  By completing the questions in this DPIA, you should be able to estimate the likelihood of the risk(s) in your research, especially in respect of threats, sources of risks, and planned controls. |  |
| 1. **How would you describe the impact of the risk(s) after having completed the previous questions in this DPIA?** | Radio button (only one option can be selected):  □ Negligible  □ Limited  □ Important  □ Maximum | By completing the questions in this DPIA, you should be able to estimate the impact of the risk(s) in your research on the data subjects, their community, your institution, the wider public, … |  |
| 1. **How would you describe the risk(s) after having completed the previous questions in this DPIA?** | Radio button (only one option can be selected):  □ No risk(s) left  □ Acceptable risk(s) left  □ Non-acceptable risk(s) left (specify below) | By completing the questions in this DPIA, you should be able to estimate the impact and the likelihood of the risk(s) in your research. By balancing the impact with the likelihood, you can indicate whether or not there are risk(s) left in your research and whether or not they are acceptable.  If you indicate that there is/are one or more non-acceptable risk(s) left, please contact your Data Protection Officer (DPO):  The Data Protection Officer for Ghent University is Hanne Elsen ([privacy@ugent.be](mailto:privacy@ugent.be)).  The Data Protection Officer for Ghent University Hospital is Katya Van Driessche ([dpo@uzgent.be](mailto:dpo@uzgent.be)). |  |