university of groningen

Starting with a DPIA methodology for human subject research

Starting with a DPIA methodology for human subject research v. 0.1, November 2018

This document is a Deliverable of the Human Subject Research Programme.
Authors: Esther Hoorn and Cristina Montagner
The authors are grateful to Eline Gaspersz for her contribution to the text, and to Marijke Folgering, Christina Elsenga, Francisco Romero Pastrana, Jan-Willem Oordt, Trix Mulder, Ronald Zwaagstra, Tina Kretschmer, and Marije aan het Rot for their comments and suggestions.

Contents

Introduction

This is a guide for support staff and researchers, who already have a general understanding about the General Data Protection Regulation (GDPR). The new GDPR sets a challenge where it introduces the obligation for the data controller to be able to demonstrate compliance. "In the field of data protection, in general terms, accountability not only consists in adopting and implementing the appropriate measures [...] but also in being able to demonstrate – upon request – that such measures have been taken. [...] PIA[1] is a constitutive element of accountability and, a PIA can only be successfully conducted in a sound accountability framework."[2].

In the GDPR there are general requirements regarding records and documentation (Articles 26-31). For instance, the controller should maintain a record of the processing activities under its responsibility (processing register). Another that when there is more than one controller (joint controllers) need to document their responsibilities transparently. The records can be based on a general compliance check and a general description of the processes.

The GDPR introduces in Article 35 the **Data Protection Impact Assessment** (DPIA) as a mandated assessment for specific cases in which there is a high risk to freedom and the rights of data subjects. These specific cases are elaborated by the Data Protection Working Party (WP29)[3] and the National Authority. The Data Protection Working Party identified nine criteria that should consider evaluating if a process is likely to result in a high risk for the rights and the freedom of the data subject[4]. For European research projects, the criteria are specified in the guidance for the ethics self-assessment[5].

The DPIA process aims to ensure that controllers adequately address privacy and data protection risks of 'risky' processing operations. By providing a structured way of thinking about the risks to data subjects and how to mitigate them, DPIAs help organisations to comply with the requirement of 'data protection by design'[6].

In this document, we start with a guidance on doing a DPIA for a research project. We believe that starting to build up experience with DPIA's can – over the coming years- be helpful to get oversight and technical and organizational measures in place. Support staff can fulfil a useful role in identify gaps and raise awareness and, to build legal and ethical aspects into the design of the data management of research projects.

When personal data are processed the first step should assess the lawfulness and the purpose of the processing:

Lawfulness: Do you have a legal ground for processing the data?

Purpose: Which is the purpose of your process and (in case of secondary use) which was the original purpose?

For that reason, in this first version of this guidance, we added a section about the legal grounds that can be relevant for research. For the DPIA method, we follow the steps described in the so-called German model described in Bieker et al.[7] Where possible we refer to examples and lessons learned in supporting DPIA's for research within the university.

1 Paul De Hert, Dariusz Kloza and David Wright (Eds.), PIAF: A Privacy Impact Assessment Framework for data protection and privacy rights. Deliverable D3. Prepared for the European Commission Directorate General Justice. November 2012, pg.16. The authors use the term PIA (Privacy Impact Assessment) and state that "once the GDPR passes into law, a term "data protection impact assessment" should be used to refer to the tool described therein".

2 De Hert et al., 2012, pg. 16.

3 Article 29 Data Protection Working Party, WP248 rev.01" Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679"

4 (1) Use of evaluation or scoring method; (2) automated-decision making; (3) systematic monitoring; (4) sensitive data or data of a highly personal nature; (5) data processed on a large scale; (6) matching or combination of datasets; (7) use of data concerning vulnerable subject; (8) use of new technological or organizational solutions and (9) when the processing prevents the data subject from exercising a right or using a service or a contract.

5 Horizon 2020 Programme Guidance "How to complete your ethics self-assessment" and European Research Council Ethics self-assessment step by step version 1, 26 july 2018.

6 European Data Protection Supervisor, "Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation", February 2018.

7 Felix Bieker, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost, "A Process for Data Protection Impact Assessment under the European General Data Protection Regulation", in K. Rannenberg and D. Ikonomou, Privacy Technologies and Policy, Fourth Annual Privacy Forum, APF 2016 Frankfurt. Heidelberg, New York, Dordrecht, London

We envision that we will need to elaborate this guidance later on with specific assessment situations, specific legal circumstances and particular sets of measures for research- and collaboration scenarios. A protocol for DPIA's in research, based on the university's data protection policy is under development. The protocol will be brought in line with the guidance given in this document. At this stage, the guidance can also be helpful to identify needs for discipline-specific DPIA in the 2019 GDPR working plan of the faculties. We expect that this DPIA approach will help to determine how the researchers can be involved in mitigating risks and which measures should be coordinated at a central level.

1. Why a DPIA in research?

Personal data are often used for scientific research. The protection of personal data is regulated in the General Data Protection Regulation (GDPR), which came into effect on the 25th of May (2018). The GDPR enables a broad range of research scenarios and research collaborations. It takes some effort to identify the technical and organizational measures required for a specific research project. The identification of appropriate safeguards needs to align with methodological and ethical issues in specific fields of research.

How can this be achieved? There is a growing awareness of the responsibilities of research institutes in the discussions about big data, open data and the need for data protection. At the same time, ethical assessment frameworks are not yet adapted to take into account the responsibilities related to the use of personal data. Asking the right questions is crucial.

Create a privacy culture in research - "PIA requires–within an organisation–high-level support, embedding in a governance model, privacy expertise and a privacy culture. […] An organisation is responsible for ensuring that all its employees are sensitive to the privacy implications. Insinuating privacy into daily practice, on-going targeted training and raising awareness". Examples of tools to create a privacy culture are "among others, codes of conduct, general e-learning, blogs and use of an intranet as well as privacy screen-savers and games[8]".
The researchers have a crucial role in the creation of the privacy culture in research. It is essential to stimulate researchers: to identify privacy issues and protection measures related to their specific field of research. A concrete action could encourage researchers to include privacy-related issues in the publication of their discipline (see the example published by European Journal of Human Genetics[9]).

Research takes place at a global scale - The specific requirements of research are recognised in the GDPR. At the same time, however, defining the specific criteria for research is left to the member states of the European Union. The GDPR also introduces an assessment method. DPIA may now be mandatory for a research project. This approach was developed in Canada to support the concept of "privacy by design" and has become increasingly recognised as a holistic method worldwide. The assessment method builds on internationally recognised general principles for data protection.

From protection measures to best-practices - Pseudonymisation and encryption are mentioned as relevant protection measures in the GDPR. However, because the GDPR is technology neutral, a further common range of specific measures needs to be explored (see Section 3). These measures need to ensure that safeguards for the rights of participants are in place and that the essence of data protection law is respected. Building these measures into the research design and data management plans requires the active involvement of researchers. The documentation of the assessment can be helpful for transparency and to fulfil the obligation to demonstrate compliance but not only. In research, a DPIA is also the opportunity to improve the quality of the investigation and to promote the creation of best-practices in research. Examples of best-practices will be presented in relation with transparency in research

A DPIA helps to clarify responsibilities - An example: pseudonymous data is a new subset of personal data introduced in a legal sense in the GDPR. Under the GDPR, pseudonymization means "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and

8 De Hert et al., 2012, pg. 23.
9 M. Shabani, P. Borry, Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation, European Journal of Human Genetics, vol. 26, 149–156 (2018). doi:10.1038/s41431-017-0045-7.

is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person". A researcher will like to know to which extend he can depend on central services, such as a pseudonymization service. Doing a DPIA can help to identify the appropriate measures for a specific research project. Within a Dutch university, the board of a faculty is responsible for research policy. The discussion about shared responsibilities should be organized at discipline-specific level. Moreover, with a DPIA is possible to clarify the responsibilities of the internal and external partners involved in the project (see Section 2).

A DPIA to improve the Research Data Management Plan–"The PIA is a process that should start as early as possible, well before the project becomes operational and when it is possible to influence decision-making and it should be carried out throughout the project's lifetime".[10] In the project proposal the risk analysis is usually focused on the identification of the possible obstacles that researcher may find to achievement of the research goals. On the other hand, the risk assessment carried out in a DPIA is focused on the risks for the freedom and the rights of the data subjects. These two assessments should be considered complementary each other and not in antithesis. The Research Data Management Plan should be an ideal moment for the researcher to combine the results of these two assessments and, to create a concrete plan before to start the project.

Funders may require a DPIA - The guidance from H2020 on ethics self-assessment (version 6.0) request an opinion of the data controller on the need for a DPIA. This applies to processing involving "profiling, systematic monitoring of individuals or processing of large scale of special categories of data, intrusive methods of data processing (such as, tracking, surveillance, audio and video recording, geo-location tracking etc.) or any other data processing operation that may result in high risk to the rights and freedoms of the research participants". The scoping report (see Section 6.1) can be used to substantiate the opinion of the data controller on the need for a DPIA. If the need for a DPIA is foreseen in an early stage this might as well be done as a work-package in the research project.

2. Internal responsibility for personal data in research projects

A DPIA can help to clarify responsibilities. Within a Dutch university, the board of a faculty is responsible for research policy. The report of a DPIA can be useful as a reference within a field of research. For example, reasonable data retention periods should be decided at a discipline-specific level. A documented DPIA report can be shared with other research institutes doing research in the same field to come to discipline specific codes of conduct. In this way, the requirements of the GDPR can be aligned with codes on ethical conduct and research integrity. Clarification of responsibilities will support transparency, the academic debate and a culture of blame-free reporting.

The RUG "General policy on protection of personal data" (June 2018) defines the level of responsibility of all the levels of governance and all staff members of the University[11].

Concerning the DPIA for research projects the General Policy states "Innovative research projects and new processes within the UG, as well as the systems that support these processes, are designed in such a way that the privacy impact is as low as possible while continuing to achieve the legitimate objectives of these processes. Where necessary, a DPIA will be carried out. The UG has a protocol that determines when this is mandatory and that encourages the sharing of insights from the DPIAs." The results from the DPIAs will be used by the Board of the University to establish an annual work programme.

3. Protection goals and measures

The GDPR does not define which method has to be used to perform a DPIA. The minimum requirements for a DPIA are nicely elaborated with the European supervisors (see Annex 1). Moreover, the WP29 states that the "GDPR allows for data controllers to introduce a framework which complements their existing working practices provided it takes account of the components described in Article 35(7)".

10 De Hert et al., 2012, pg. 12.
11 https://www.rug.nl/info/generalpolicy-on-protection-of-personaldataug.pdf

The European Data Protection Supervisor points to the Bieker et al. method as a reference[12]. We started to use the Bieker et al. method because it gives a parsimonious model with privacy- and security protection goals (confidentiality, integrity, availability, unlinkability, intervenability and transparency). These protection goals are aligned with the data protection principles defined in article 5 GDPR (lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality and accountability). Recently, the European Data Protection Supervisor (EDPS)[13] presented a document for doing a DPIA, where a questionnaire is used to guide the assessment related to the data protection principles (see Annex 2).

The interplay between the protection principles and the protection goals is explained in one of the reports of ENISA "Working with protection goals means to balance the requirements derived from the six protection goals concerning data, technical and organizational processes. Considerations on lawfulness, fairness and accountability provide guidance for balancing the requirements and deciding on design choices and appropriate safeguards."[14]

Figure 1 shows the six protection goals, covering the risks of **IT security** (1) availability, (2) integrity (3) confidentiality, and the **data protection** goals (4) unlinkability, (5) transparency, and (6) intervenability.

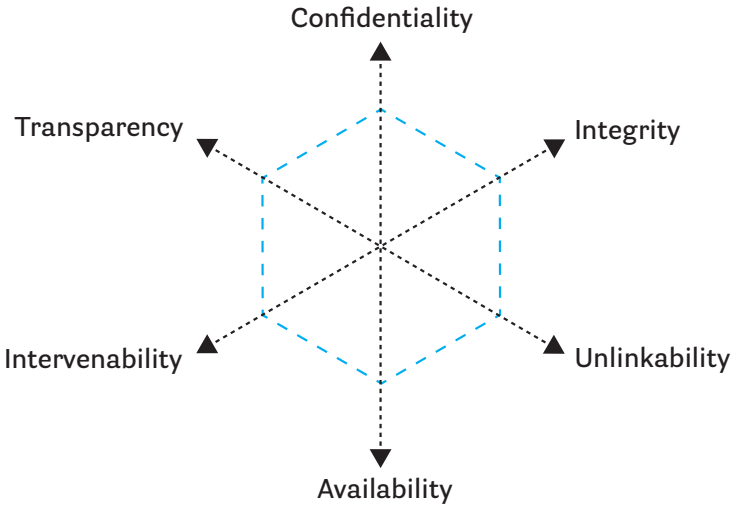

Figure 1. Protection Goals [Bieker et al.]

Data minimisation is an additional protection goal. Data minimisation support the principle of necessity, which requires that any process (collect, process and use) do not involve more personal data than necessary for the achievement of the purpose of the processing. The realization of this protection goal presupposes the appropriateness and legitimacy of the purpose[15].

During the risk assessment it seems to be the common practice to start describing risks and identify possible solutions. To guarantee an objective assessment it is important to take into account the holistic approach of all the protection goals presented in Figure 1. "The protection goals are in a state of dual interplay. This leads to a tension, as usually the strengthening of one protection goal leads to the detriment of its counterpart. The evaluation therefore has to achieve the proper balance between the protection goals. For instance, a system that processes highly confidential data will restrict the access to the data as much as possible, thereby limiting the availability. Still authorized entities should be able to access the data, but depending on the implemented safeguards they may need to undergo a cumbersome process, e. g. applying a four-eye principle

12 European Data Protection Supervisor " Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation", February 2018, p. 26.
13 European Data Protection Supervisor, 2018, p. 26.
14 European Union Agency For Network and Information Security (ENISA) "Privacy and data protection in mobile applications A study on the app development ecosystem and the technical implementation of GDPR", November 2017.
15 The Standard Data Protection Model (SDM), "A concept for inspection and consultation on the basis of unified protection goals" Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016

and demanding necessary paperwork before access is granted, requiring specific hardware for access of the clear text etc.[16]".

Table 1 describes the protection goals and identifies their relation with the GDPR. In the table are presented also some examples of generic measures for the implementation of the protection goals. The information reported in the table are from Standard Data Protection Model developed by the German Conference of Data Protection Authorities[17]. The specific measures to achieve the goals in the research projects will identify during the evaluation stage of the DPIA process. More details in Section 6.2.

The University of Groningen elaborated the "Information security baseline[18]" for the security protection goals in the university systems. The baseline describes the minimum measures needed to ensure a minimum level of information security and applies to all information systems within the University.

Table 1 - The protection goals, their relation with the GDPR and some examples of generic measures for the implementation the goals[19].

PROTECTION GOALS	RELATION WITH GDPR	GENERIC MEASURE FOR THE IMPLEMENTATION OF THE PROTECTION GOALS
Data minimization is the requirement to collect, process and use only personal data than are necessary for the achievement of the purpose of the processing.	Data minimization is explicitly included in Art. 5 (1) (c) "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')".	- Reduction of collected attributes of the data subject, - Preference for automated processing operations (not decision-making processes), which make the use of processed data unnecessary and limit the possibility of interference, compared to dialogue-controlled processes, - Procedures for pseudonymisation and anonymisation.
Availability is the requirement that personal data must be available and can be used properly in the intended process. Thus, the data must be accessible to authorised parties and the methods intended for their processing must be applied.	*Availability* is explicitly included in Art. 32 (1) (b) and (c) in the context of security of data processing. It is also anchored in Art. 5 (1) (e) as a prerequisite for the identification of the data subject. It ensures the availability of the data for the respective purpose as long as this purpose remains valid.	-Preparation of data backups, process states, configurations, data structures, - Protection against external influences, - Implementation of repair strategies and alternative processes.
Integrity refers, (i) to the requirement that information technology processes and systems continuously comply with the specifications that have been determined for the execution of their intended functions. (ii) the data to be processed remain intact, complete, and up-to-date.	*Integrity* is mentioned in Art. 5 (1) (f) as a principle for the processing of data and in Art. 32 (1) (b) as a prerequisite for the security of data processing. It shall ensure protection against unauthorized modifications and deletions.	- Restriction of writing and modification permissions, - Documented assignment of rights and roles, -Specification of the nominal behaviour of workflow or processes and regular testing of the detectability respective determination of the current state of processes.
Confidentiality refers to the requirement that no person is allowed to access personal data without authorisation. It ensures the protection against unauthorized and unlawful processing.	The obligation to maintain *confidentiality* results, in particular, from Art. 5 (1) (f), Art. 32 (1) (b) and Art. 38 (5) (secrecy obligation of the data protection officer) and Art. 28 (3) (b) (secrecy obligation of the data processor) respectively.	- Definition of a rights and role concept according to the principle of necessity on the basis of identity management by the controller, - Implementation of a secure authentication process, - Limitation of authorized personnel to those who are verifiably responsible - Specification and control of organisational procedures (obligation to data secrecy, confidentiality agreements, etc.), - Encryption of stored or transferred data.

16 Bieker et al. 2016.
17 The Standard Data Protection Model (SDM), 2016.
18 https://myuniversity.rug.nl/infonet/medewerkers/ict/beleidenprojecten/security/documenten/rug_baseline_inf_bev_v_1.0.pdf
19 The information in the table are extracted from The Standard Data Protection Model (SDM), 2016.

Unlinkability refers to the requirement that data shall be processed and analysed only for the purpose for which they were collected.	The obligation to process data only for the purposes for which they were collected is to be found, in particular, in the individual legal basis for processing (Art. 6) that make the business purposes, the research purposes, etc. a yardstick. It is included in the in the principle of purpose limitation in Art. 5 (1) (b).	- Restriction of processing, utilization and transfer rights, - Separation in organisational / departmental boundaries, - Approval of user-controlled identity management by the data processor, - Using purpose specific pseudonyms, anonymisation services, anonymous credentials, processing of pseudonymous or anonymous data.
Transparency is necessary for the monitoring and control of data, processes, and systems from their origin to their erasure and is a prerequisite for lawful data processing. Transparency of the entire data processing operation and of the parties involved can help ensure that data subjects and supervisory authorities can identify deficiencies and, if necessary, demand appropriate procedural changes.	*Transparency* is laid down in Art. 5 (1) (a). It is reflected as a fundamental principle of data protection law in numerous regulations of the GDPR. Especially the obligations to information and access take this principle into account (Art. 12-14).	- Documentation of procedures, in particular including the business processes, data stocks, data flows and the IT systems used, operating procedures, description of procedure, interaction with other procedures, - Documentation of the contracts with external service providers and third parties, from which data are collected or transferred to, - Documentation of consents and objections.
Intervenability refers to the requirement that data subjects are effectively granted their rights to notification, information, rectification, blocking and erasure at any time, and that the controller is obliged to implement the appropriate measures.	*Intervenability* are explicitly derived from the provisions on rectification, blocking, erasure, and the right of objection (Arts 16-17 & 22). They may also result from a weighting of interests within the framework of statutory criteria for lawful processing. The controller must, pursuant to Art. 5 (1) (d) GDPR provide the prerequisite for guaranteeing such rights, both at organisational and, where required, at technical level.	- Differentiated options for consent, withdrawal and objection, - Creating necessary data fields, e.g. for blocking indicators, notifications, consents, objections, right of reply, - Disabling options for individual functionalities without affecting the whole system, - Traceability of the activities of the controller for granting the data subject's rights, - Establishing a Single Point of Contact (SPoC) for data subjects, -Operational possibilities to compile, consistently correct, block and erase all data stored with regard to any one person.

4. Data protection and the ethical assessment for scientific research

In the GDPR the special needs of research are recognized. This was also the case under the previous legislation. The main difference is that the new regulation includes as general obligation to demonstrate compliance with the GDPR and specific requirements on transparency. An example of requirements is the need of documented best-practices and building blocks of technical and organizational measures for specific research scenarios. In this the ethics boards have a special role.

For example, there is no definition of what can fall under the derogations for research. Some derogations are solely available to scientific research. The WP29 in a recent guidance document on consent came with this clarification[20]:

> *The term 'scientific research' is not defined in the GDPR. Recital 159 states "(...) For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner. (...)", however, the WP29 considers the notion may not be stretched beyond its common meaning and understands that 'scientific research' in this context means a research project* ***set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice.***

This leads to the conclusion that for research projects that want to use the derogations, e.g. the derogation on storage limitation (Article 5(1)(e) GDPR) in case of longitudinal research infrastructures, a previous ethical assessment should be in place. At this stage a scoping report for a DPIA could be a good method to prepare such an assessment.

20 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051. The full text related to scientific research is provided in Annex 3

At the same time in the Dutch implementation of the derogations for research some derogations are only available for research that is performed by research institutes. On October 2018 the new national VSNU code of conduct on research integrity will take effect. New in this code are duties of care for research institutes e.g. on data management, FAIR data and the principle to be as open as possible. The code of conduct expects the ethical boards to be able to give advice on the principle to be as open as possible. Most likely work has to be done on that field for so far, the main focus of ethical boards has been the approach towards participants and not the responsible handling of their data.

A role for ethics boards and discipline specific networks is also required to develop discipline specific data retention and re-use policies for pseudonymized data. The GDPR opens possibilities for extended data retention for research purposes when that aligns with existing ethics codes. Yet, for many forms of innovative research such ethics codes do not go into detail on these topics. The role of ethics boards in the DPIA process needs further elaboration. For instance the ethical code of the National Ethics Council for Social and Behavioural Sciences state that when personal data are being registered or collected, consent must be obtained in accordance with the law but does not elaborate how that can be assessed. At the institutional level this is clarified in the UG protocol for the DPIA.

5. Legal ground

The lawful base for processing personal data has to be in place before processing the data and the lack of a lawful base cannot be identified in the DPIA process as a risk that can be mitigated. In the following a short overview of the two most common legal grounds is presented. According to a recent guidance document[21] consent is an important legal ground for processing personal data for research. Yet, in some cases the legitimate interest of the researcher or tasks carried out in the public interest can form the legal basis for further processing of personal data of existing data for research.

5.1 Informed consent

Consent is one of the legal bases for processing personal data. The GDPR defines consent as: 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.

The Data Protection Working Party published two useful guidelines one on Consent and, one on transparency[22].

Conditions for consent- The first condition for valid consent is that it should be given by a clear affirmative act, which means it must be given through an active motion or declaration. Examples are ticking a box on a (digital) form, or a written or oral statement, which clearly indicate the data subject's acceptance of the proposed processing of their personal data. This means that pre-ticked boxes, silence or in-activity do not constitute consent.

This clear affirmative act must subsequently indicate the data subject's freely given, specific, informed and unambiguous agreement to the processing of their personal data. Additionally, consent should cover all processing activities carried out for the same purpose. In the case of multiple purposes, consent must be given for each of them.

Additional conditions for valid consent are that the controller must be able to demonstrate the data subject's consent and ensure that given consent can be withdrawn as easily as it was given.[23]

Elements of consent- The elements of valid consent are:

21 WP 248 rev. 01.

22 Article 29 Data Protection Working Party, WP 259 "Guidelines on Consent under Regulation 2016/679" and WP 260 "Guidelines Guidelines on transparency under Regulation 2016/679".

23 More on the conditions for consent in Article 7 GDPR. Article 11 GDPR states that if the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation. Article 17(3)(d) GPDR sets out an exception to the right to be forgotten for scientific research when it likely to render impossible or seriously impair the achievement of the objectives of that processing.

1. Freely given. This element implies choice and control for the data subject. Consent is not valid when the data subject has no real choice, feels compelled or pressured to consent or will endure negative consequences if they refuse or withdraw consent. When the data subject is not allowed to give consent for some processing operations and not for others, their consent is presumed not to be freely given.
2. Specific. The element specific aims to ensure a degree of control and transparency for the data subject and indicates that consent must be given in relation to one or more specific purposes.
3. Informed. This element is based on the principle of transparency: providing information for data subjects is essential to their ability to make informed decisions. In some cases, however, more information may be needed in order to enable the data subject to understand the processing operations and make an informed decision.
4. Unambiguous. The element of an unambiguous indication of the data subjects wishes to agree to the processing of their personal data means that it must be clear to which processing operations the consent was given and there should be no doubt whether consent was given or not.

The Annex 4 presents a checklist for the preparation of a Consent Form and the Participant Information Sheets.

Processing of special categories of personal data is forbidden except when there is explicit consent. Special categories of data are defined in Article 9 GDPR. They are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Based on the GDPR in the Dutch law, it is elaborated that processing of special categories of data is also allowed when it is necessary for the research purpose when it is proportionate to the aim pursued, respecting the essence of the right to data protection and providing for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5.2 Legitimate interest and public interest

A common situation, for the use of the legitimate interest is when researchers want to re-use existing sets of personal data. This is possible when the processing of the data is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

Article 6(1)(f) of the GDPR states that "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

A transparency obligation (Article 13(1)(d)) requires that the legitimate interest of any third party involved in the research is mentioned to the data subject when personal data are collected from the data subject if article 6(1)(f) applies.

A compatibility test must be used to determine the compatibility between the original and the new purpose for the research context. The GDPR defines some criteria that should be evaluated in the compatibility test (Article 6(4)):

I. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

II. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

III. the nature of the personal data, in particular whether special categories of personal data are processed;

IV. the possible consequences of the intended further processing for data subjects;

V. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

A guidance of the WP29[24] on legitimate interests provides two examples of the use of this legal base for scientific research (example 19 and 20). These two examples present also how compatibility should be evaluated when legitimate interests is used as legal ground. Example 20 demonstrates that the interest of the data subjects can override the legitimate interest of the university. Although the examples are based on the previous Directive and not on the GDPR, they still demonstrate how the supervising authorities envision an assessment for scientific research. The examples are presented in Annex 5.

For health research and research in the public interest specific legislation can also form a legal base.

6. Multi-stakeholders approach

At present, there is no method specifically developed to carry out a DPIA for processing personal data in research projects. In the DPIA project (part of the Human Subject Research Programme) the use of the method proposed by Bieker et al. is being assessed. This method is based on a **multi-stakeholders approach**. The team should include members with knowledge on the research project at hand (e.g. principal investigator and eventually other project members such as PhDs, researchers etc.) and members with legal and IT knowledge. The team can also include experts on specific topics related to the research proposal or the protection measures that the team intends to use (e.g. an expert on GPS data or an expert on pseudonymisation techniques).

In case of projects that involve the use of data collected by third parties (e.g. data from a health insurance company), it could be important to involve a representative of those third parties in the team. It should also be considered how participants can give their view. The Recommendations for privacy impact assessment framework includes explicit mechanisms for a stakeholder's consultation in the DPIA policy[25]. "Consultation with key stakeholders is basic to the PIA process. If a PIA is undertaken solely from the viewpoint of the organization itself, it is likely that risks will be overlooked. […] In a complex project applying powerful technologies, many segments of the population are affected. It is intrinsic to the process that members of the public provide input to the assessment, and that the outcomes reflect their concerns. Even if consultation does not increase support for a decision, it may clear up misunderstandings about the project and, at least, gain the respect of stakeholders."[26]

The team should identify a member that organizes the meeting, gathers the conversation and makes notes. In the Bieker method, the documentation of the DPIA process is described in the last stage; we recommend to document of all the steps of the process.

The method includes three stages:

(1) the "preparation stage" that examines whether a DPIA is needed and what the scope and goal of the DPIA are. The results of the preparation stage are documented in the scoping report.

(2) The "evaluation stage" includes the identification of the privacy risks in the project.

(3) The "report and safeguards stage" concerns the identification of appropriate protection measures to eliminate or mitigate the risks identified in stage (2). The results obtained in stage (2) and the measures proposed in stage (3) are described in the DPIA Report. Based on the experience gained so far, we suggest to include the identification of the protection measures in stage (2) instead of stage (3).

24 WP29 "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC".
25 De Hert et al., 2012, pg. 17.
26 De Hert et al., 2012, pg. 18.

6.1 Preparation Stage (A) - the scoping report

The scoping report is the form used to document the "preparation stage". The goal of the scoping report is to document all the information the team needs to perform the risk assessment. The preparation stage may also be used to identify if a DPIA is required. If a DPIA is not mandatory, the scoping report can be used to demonstrate accountability, documenting that the privacy issues have been evaluated before the start of the project.

The scoping report should include the following information[27]:

A1. Description on why the DPIA is necessary;

A2. Section on projecting the assessment: definition of the i) DPIA scope and the ii) the DPIA team;

A3. Target of evaluation: i) description of the system, ii) identification of the data, iii) data flow;

A4. Indication of the actors involved and the person concerned;

A5. Identification of relevant legal requirements.

At the beginning of the DPIA process, it is important to define the reason why a DPIA is needed (A1). The GDPR defines a DPIA mandatory when the processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1)). The WP29[28] provides nine criteria to identify potentially risky processes. The guidance document specifically mentions that a DPIA is mandated for research projects with special categories data when, after a project, there is a shift in the possibility for the participants to use their rights as data subjects. Recently the national authority also issued a list of criteria[29] and the European research funders point at the need to do a DPIA for intrusive research[30].

At the University of Groningen these criteria will be elaborated in a protocol. On the top of that, in the working plan 2019 faculties will be invited to identify the discipline-specific needs to do a DPIA. Doing a DPIA can also be a requirement following from the ethical review process of EU funded projects.

In the Bieker et al. model section A2 should include the definition of the DPIA scope, this section is related to the previous one (A1) but here the goal is to identify which processes, planned in the research project, are to be included in the risk assessment. When the scope is identified, it is also useful to define a team of experts that can help the researcher in the DPIA process.

The detailed description of the data and the data process are included in the section A3. The starting point for the preparation of this section is the project proposal and the RDMP. It is essential to add the following points (if not already available):

- A data flow diagram of the process (flowchart): what do we collect from where/whom, what do we do with, where do we keep it, who do we give it to?
- A detailed description of the purpose(s) of the processing, distinguishing between purposes where necessary.
- A description of the supporting infrastructure: filing systems, ICT etc.

Research project usually involve more than one researcher, for example partners from other universities,

27 Annex 6 provides a template for the Scoping Report.
28 WP 248 rev.01
29 Article 29 Data Protection Working Party, WP 259 "Guidelines on Consent under Regulation 2016/679" and WP 260 "Guidelines Guidelines on transparency under Regulation 2016/679". https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-ap-voor-een-verplichte-dpia-6667
30 Horizon 2020 Programme Guidance "How to complete your ethics self-assessment" and European Research Council Ethics self-assessment step by step version 1, 26 july 2018.

external companies, etc. The GDPR defines various roles for natural persons and organizations that process personal data (controller; join-controllers; processor; sub-processor). For each role, the GDPR defines a set of obligations regarding the protection of the rights and freedoms of the person concerned. This 'division of roles according to the GDPR' is determined in the section A4.

The last section of the scoping report (A5) identifies other relevant legal requirements that should be considered besides the GDPR (e.g. other legislation, codes of conduct, policies, etc.).

6.2 Evaluation Stage (B) - identification of privacy risks and protection measures

The evaluation stage identifies and evaluates potential risks. The evaluation should include the likelihood of the risk and the privacy impact for the data subjects. In the German method the identification of the appropriate safeguards is included in the last stage. Based on our experience with the multi-stakeholders approach, we suggest to include the identification of the measures in the evaluation stage.

For the risk assessment the method suggests to consult the catalogues of typical risks and consequences and the catalogues of typical safeguards. Definitions of the protection goals and a description of the Standard Data Protection Model have also been also proposed by the German Conference of Data Protection Authorities[31]. The Standard Data Protection Model includes a list of generic measures to implement the protection goals. These measures can be used to evaluate existing data processing systems, but also to support the design of new processes.

For research contexts these catalogues have not been defined yet. Considering the multi-tier structure of the UG we can identify some classes of operational practice that can be considered in the evaluation stage:

- Protection mechanisms: access control, pseudonymization, virus protection, ...
- Organizational measures: training; implementation best-practices, ...
- Legal measures (accountability): processing register, process agreements, privacy policies, ...

The earlier mentioned guidance of the WP29 on consent also suggests specific best practices for scientific research, like the identification of a single point of contact for participants to exercise their rights.

Based on so-called 'reference DPIAs' building blocks of technical and organizational measures and specific ethical codes can be elaborated in the future. At this stage an important recommendation is that in the DPIA process researchers document and apply their awareness of discipline specific best practices.

6.3 Documentation

It is suggested to document all the steps of the DPIA process. The DPIA report is a crucial element of the DPIA process, but it is important to remember that it is not its ultimate objective. The DPIA report should be considered as a "**living instrument**" that should be updated if necessary. Projects may change before the completion and the definition of the need to revisit and update a DPIA when, a project changes and this change has privacy implication, is a function of the DPIA process[32].

The Privacy Impact Assessment Framework (PIAF) support the **publication** of the DPIA report "the organization should make the it [PIA report] publicly available, e.g. publish it on its website. Ones a PIA is revised, a new version should be made equally available, with a reference to the previous one[33]". The PIAF also recognizes that "state secrets and commercially sensitive information should not be made public" and proposes two solutions: (i) the possibility to place confidential information in an annex and publish only the main body of the report. (ii) The creation of a summary of the report understandable also by individuals who without technical or legal knowledge[34].

31 The Standard Data Protection Model (SDM), 2016.
32 De Hert et al., 2012, pgs. 31-32.
33 De Hert et al., 2012, pg. 19.
34 De Hert et al., 2012, pg. 20.

It is desirable to create a repository for DPIAs. To comply with the GDPR, the DPIA report and related documentation must be accessible by the DPO. Moreover, doing a DPIA is a learning process and the results of a DPIA, the so-called reference DPIA, may be used for other DPIAs if the other processes share the same nature, scope, context and purposes. The PIAF refers to the creation of a "public register of PIAs that helps to create a body of knowledge and example of good practice[35]". The publication of the DPIA report is not legally required but it is suggested as good practice to improve the transparency and accountability of the institution[36].

Reference documents

- Felix Bieker, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost, "A Process for Data Protection Impact Assessment under the European General Data Protection Regulation", in K. Rannenberg and D. Ikonomou, Privacy Technologies and Policy, Fourth Annual Privacy Forum, APF 2016 Frankfurt. Heidelberg, New York, Dordrecht, London. Link
- The Standard Data Protection Model (SDM), "A concept for inspection and consultation on the basis of unified protection goals" Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016
- Article 29 Data Protection Working Party, WP 248 rev.01, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679".
- Article 29 Data Protection Working Party, WP 259 "Guidelines on Consent under Regulation 2016/679".
- Article 29 Data Protection Working Party, WP 260 "Guidelines Guidelines on transparency under Regulation 2016/679".
- Article 29 Data Protection Working Party, WP 217 "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC".
- European Data Protection Supervisor " Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation", February 2018.
- European Union Agency For Network and Information Security (ENISA) "Privacy and data protection in mobile applications A study on the app development ecosystem and the technical implementation of GDPR", November 2017.
- European Commission "Horizon 2020 Programme Guidance How to complete your ethics self-assessment", Version 6.0, July 2018. Link
- European Research Council Ethics self-assessment step by step version 1, 26 july 2018. Link
- Paul De Hert, Dariusz Kloza and David Wright (Eds.), PIAF: A Privacy Impact Assessment Framework for data protection and privacy rights. Deliverable D3. Prepared for the European Commission Directorate General Justice. November 2012. Link

Further reading

- Handbook on European data protection law (2018 edition), European Union Agency for Fundamental Rights and Council of Europe, European Court of Human Rights, European Data Protection supervisor.
- David Wright and Emilio Mordini "Privacy and Ethical Impact Assessment" in Privacy Impact Assessment, Editors David Wright and Paul De Hert, Pages 397-418, Springer 2012.
- Felix Bieker, Nicholas Martin, Michael Friedewald, Marit Hansen, "Data Protection Impact Assessment A Hands-On Tour of the GDPR's Most Practical Tool", in Marit Hansen, Eleni Kosta, Igor Nai-Fovino, and Simone Fischer-Hübner (eds.), Privacy and Identity Management. The Smart Revolution. 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Ispra, Italy, September 2017, Revised Selected Papers, Springer, Cham, 2018, pp. 207-220. https://doi.org/10.1007/978-3-319-92925-5_13

35 De Hert et al., 2012, pg. 20.
36 Article 29 Data Protection Working Party WP248.

- Trix Mulder, Raj R. Jagesar, Aline M. Klingenberg, Jeanne P. Mifsud Bonnici, Martien J. Kas, “New European privacy regulation: Assessing the impact for digital medicine innovations”, European Psychiatry 54 (2018) 57–58.
- Gabe Maldoff, “How GDPR changes the rules for research”, IAPP (International Association of Privacy Professionals). Link.

Annex 1 - Criteria for a DPIA

The WP29[37] proposes the following criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR:

A systematic description of the processing is provided (Article 35(7)(a)):

- nature, scope, context and purposes of the processing are taken into account (recital 90);
- personal data, recipients and period for which the personal data will be stored are recorded;
- a functional description of the processing operation is provided;
- the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
- compliance with approved codes of conduct is taken into account (Article 35(8));

Necessity and proportionality are assessed (Article 35(7)(b)):

- measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:
  - ◊ measures contributing to the proportionality and the necessity of the processing on the basis of:
    - specified, explicit and legitimate purpose(s) (Article 5(1)(b));
    - lawfulness of processing (Article 6);
    - adequate, relevant and limited to what is necessary data (Article 5(1)(c));
    - limited storage duration (Article 5(1)(e));
  - ◊ measures contributing to the rights of the data subjects:
    - information provided to the data subject (Articles 12, 13 and 14);
    - right of access and to data portability (Articles 15 and 20);
    - right to rectification and to erasure (Articles 16, 17 and 19);
    - right to object and to restriction of processing (Article 18, 19 and 21);
    - relationships with processors (Article 28);
    - safeguards surrounding international transfer(s) (Chapter V);
    - prior consultation (Article 36).

Risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):

- origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
  - ◊ risks sources are taken into account (recital 90);
  - ◊ potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
  - ◊ threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
  - ◊ likelihood and severity are estimated (recital 90);
- measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);

Interested parties are involved:

- the advice of the DPO is sought (Article 35(2));
- the views of data subjects or their representatives are sought, where appropriate (Article 35(9)).

37 Article 29 WP, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679', Rev 0.1, 4 oct. 2017. http://ec.europa.eu/newsroom/document.cfm?-doc_id=47711.

Annex 2 - Catalogue of guiding questions on data protection principles[38]

Guiding Questions on fairness

1. Can people expect this to happen, also if they don't read the information you provide them with?
2. In case you rely on consent, is it really free? How do you document that people gave it? How can they revoke their consent?
3. Could this generate chilling effects?
4. Could this lead to discrimination?
5. Is it easy for people to exercise their rights to access, rectification, erasure etc.?

Guiding Questions on transparency

1. How do you make sure that the information you provide actually reaches the individuals concerned?
2. Is the information you provide complete and easy to understand?
3. Is it targeted to the audience? E.g. children may require tailored information
4. In case you defer informing people, how do you justify this?

Guiding Questions on purpose limitation

1. Have you identified all purposes of your process?
2. Are all purposes compatible with the initial purpose?
3. Is there a risk that the data could be reused for other purposes (function creep)?
4. How can you ensure that data are only used for their defined purposes?
5. In case you want to make available / re-use data for scientific research, statistical or historical purposes, what safeguards do you apply to protect the individuals concerned?

Guiding Questions on data minimisation

1. Are the data of sufficient quality for the purpose?
2. Do the data you collect measure what you intend to measure?
3. Are there data items you could remove (or mask/hide) without compromising the purpose of the process?
4. Do you clearly distinguish between mandatory and optional items in forms?
5. In case you want to keep information for statistical purposes, how do you manage the risk of re-identification?

Guiding Questions on accuracy

1. What could be the consequences for the persons affected of acting on inaccurate information in this process?
2. How do you ensure that the data you collect yourself are accurate?
3. How do you ensure that data you obtain from third parties are accurate?
4. Do your tools allow updating / correcting data where necessary?
5. Do your tools allow consistency checks?

Guiding Questions on storage limitation

1. Does EU legislation define storage periods for your process?
2. How long do you need to keep which data? For which purpose(s)?
3. Can you distinguish storage periods for different parts of the data?

38 European Data Protection Supervisor "Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation", February 2018.

4. If you cannot delete the data just yet, can you restrict access to it?
5. Will your tools allow automated permanent erasure at the end of the storage period?

Guiding Questions on security

1. Do you have a procedure to perform an identification, analysis and evaluation of the information security risks possibly affecting personal data and the IT systems supporting their processing?
2. Do you target the impact on people's fundamental rights, freedoms and interests and not only the risks to the organisation?
3. Do you take into consideration the nature, scope, context and purposes of processing when assessing the risks?
4. Do you manage your system vulnerabilities and threats for your data and systems?
5. Do you have resources and staff with assigned roles to perform the risk assessment?
6. Do you systematically review and update the security measures in relation to the context of the processing and the risks?

Annex 3 - Guidelines on Consent in research[39]

Scientific research

The definition of scientific research purposes has substantial ramifications for the range of data processing activities a controller may undertake. The term 'scientific research' is not defined in the GDPR. Recital 159 states "(...) For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner. (...)", however the WP29 considers the notion may not be stretched beyond its common meaning and understands that 'scientific research' in this context means a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice.

When consent is the legal basis for conducting research in accordance with the GDPR, this consent for the use of personal data should be distinguished from other consent requirements that serve as an ethical standard or procedural obligation. An example of such a procedural obligation, where the processing is based not on consent but on another legal basis, is to be found in the Clinical Trials Regulation. In the context of data protection law, the latter form of consent could be considered as an additional safeguard. At the same time, the GDPR does not restrict the application of Article 6 to consent alone, with regard to processing data for research purposes. As long as appropriate safeguards are in place, such as the requirements under Article 89(1), and the processing is fair, lawful, transparent and accords with data minimisation standards and individual rights, other lawful bases such as Article 6(1)(e) or (f) may be available.69 This also applies to special categories of data pursuant to the derogation of Article 9(2)(j).

Recital 33 seems to bring some flexibility to the degree of specification and granularity of consent in the context of scientific research. Recital 33 states: "It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose."

First, it should be noted that Recital 33 does not disapply the obligations with regard to the requirement of specific consent. This means that, in principle, scientific research projects can only include personal data on the basis of consent if they have a well-described purpose. For the cases where purposes for data processing within a scientific research project cannot be specified at the outset, Recital 33 allows as an exception that the purpose may be described at a more general level.

Considering the strict conditions stated by Article 9 GDPR regarding the processing of special categories of data, WP29 notes that when special categories of data are processed on the basis of explicit consent, applying the flexible approach of Recital 33 will be subject to a stricter interpretation and requires a high degree of scrutiny.

When regarded as a whole, the GDPR cannot be interpreted to allow for a controller to navigate around the key principle of specifying purposes for which consent of the data subject is asked. When research purposes cannot be fully specified, a controller must seek other ways to ensure the essence of the consent requirements are served best, for example, to allow data subjects to consent for a research purpose in more general terms and for specific stages of a research project that are already known to take place at the outset. As the research advances, consent for subsequent steps in the project can be obtained before that next stage begins. Yet, such a consent should still be in line with the applicable ethical standards for scientific research.

Moreover, the controller may apply further safeguards in such cases. Article 89(1), for example, highlights the need for safeguards in data processing activities for scientific or historical or statistical purposes. These purposes "shall be subject to appropriate safeguards, in accordance with this regulation, for the rights and freedoms of data subject." Data minimization, anonymisation and data security are mentioned as possible safeguards. Anonymisation is the preferred solution as soon as the purpose of the research can be achieved without the processing of personal data.

39 wp259rev.01, Guidelines on consent under Regulation 2016/679 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

Transparency is an additional safeguard when the circumstances of the research do not allow for a specific consent. A lack of purpose specification may be offset by information on the development of the purpose being provided regularly by controllers as the research project progresses so that, over time, the consent will be as specific as possible. When doing so, the data subject has at least a basic understanding of the state of play, allowing him/her to assess whether or not to use, for example, the right to withdraw consent pursuant to Article 7(3). Also, having a comprehensive research plan available for data subjects to take note of, before they consent could help to compensate a lack of purpose specification. This research plan should specify the research questions and working methods envisaged as clearly as possible. The research plan could also contribute to compliance with Article 7(1), as controllers need to show what information was available to data subjects at the time of consent in order to be able to demonstrate that consent is valid.

It is important to recall that where consent is being used as the lawful basis for processing there must be a possibility for a data subject to withdraw that consent. WP29 notes that withdrawal of consent could undermine types scientific research that require data that can be linked to individuals, however the GDPR is clear that consent can be withdrawn and controllers must act upon this – there is no exemption to this requirement for scientific research. If a controller receives a withdrawal request, it must in principle delete the personal data straight away if it wishes to continue to use the data for the purposes of the research.

Annex 4 – Consent Form & Participant Information Sheet

This document provides information and context for preparing the Consent Form and the Participant Information Sheet. This guidance applies when the consent is the legal ground for processing the data and the personal data[40] are collected directly from the data subjects (participants).

Please be aware that when the personal data are used to develop apps or algorithms other further requirements may be requested by the GDPR.

When a **Data Protection Impact Assessment (DPIA)** is required, it is recommended to complete the DPIA and design a tailor-made consent form and information sheet before to start the collection of the data.

The signed consent form gives the authorization to the controller (researcher) to collect and process the data in the terms described in the Participant Information Sheets. The consent form does relieve the controller to the obligation to take all the **necessary measures** to protect the **rights and the freedoms of the participants**[41].

Consent in scientific research

Consent as legal ground - Consent is one of the legal grounds for processing personal data for scientific research. "The definition of scientific research purposes has substantial ramifications for the range of data processing activities a controller may undertake. The term *'scientific research'* is not defined in the GDPR. Recital 159 states "(...) *For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner.* (...)", however the Data Protection Working Party (WP29) considers the notion may not be stretched beyond its common meaning and understands that '*scientific research'* in this context means a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice."[42]

Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing of his/her personal data (Article 7 GDPR) and that consent requirements defined by GDPR are meet. All the information that the controller provides to the participants must be presented in a concise, transparent, intelligible and easily accessible way, using clear and understandable language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the participants, the information may be provided orally. However, the controller needs to demonstrate that the data subjects were properly informed about the processing of their personal data (Participation Information Sheet).

To facilitate the communication with the data subjects the Data Protection Working Party suggests the use of a ***layered approach***. The *layered approach* means that the controller may provide information to the data subjects using a combination of methods (privacy statements/notices, information on the project's web page, etc.). In any case, it is recommended that the "first "layer" (the primary way in which the controller first engages with the data subject) should generally convey the most important information, namely the details of the purposes of processing, the identity of controller and the existence of the rights of the data subject, together with information on the greatest impact of processing or processing which could surprise the data subject"[43]

Special categories of personal data- GDPR forbids the processing of special categories of personal data except when data subjects give their explicit consent. Special categories of data are defined in Article 9 GDPR. They are personal data revealing racial or ethnic origin, political opinions, religious or philosophical

40 Personal data includes any information that can be used to directly or indirectly identify a specific individual.

41 "The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data" (Rec. 75 GDPR).

42 Article 29 Data Protection Working Party, WP259 "Guidelines on Consent under Regulation 2016/679".

43 Article 29 Data Protection Working Party, WP260 rev 0.1 "Guidelines on transparency under Regulation 2016/679", pg.19.

beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Based on the GDPR, the Dutch law (in the Uitvoeringswet Algemene Verordening Gegevensbescherming - UAVG), elaborates that the processing of special categories of data is also allowed when it is necessary for research purposes. In this case, the use of the data needs to be proportionate to the aim pursued and respect the essence of data protection. The controller also has to provide appropriate measures to safeguard the fundamental rights and the interests of the data subjects.

Vulnerable categories of data subject - "Vulnerable persons are those with whom there is a disbalance in power, between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his/her data. [...] This also concerns vulnerable segment of the population requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly, a patient, or in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified"[44].
In case of participation of vulnerable subjects an assessment of specific best practices to involve them[45] is requested. The information shall be understandable to the audience addressed by the controller, paying particular attention to the position of children[46].

Conditions for a valid consent
The condition for valid consent is that it should be given by a clear affirmative act, which means it must be given through an active motion or declaration[47]. This clear affirmative act must subsequently indicate the data subject's freely given, specific, informed and unambiguous agreement to the processing of their personal data.
For the principle of transparency, it is essential that the participants determine in advance what the **scope** and **consequences** of the processing entail. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller needs to obtain an authorization from the data subjects. Moreover, the controller needs to ensure that the given consent can be withdrawn as easily as it was given[48].

General elements of consent

1. Freely given. This element implies choice and control for the data subject. Consent is not valid when the data subject has no real choice, feels compelled or pressured to consent or will endure negative consequences if they refuse or withdraw consent. When the data subject is not allowed to give consent for some processing operations and not for others, their consent is presumed not to be freely given.
2. Specific. The element "specific" aims to ensure a degree of control and transparency for the data subject and indicates that consent must be given in relation to one or more specific purposes.
3. Informed. This element is based on the principle of transparency: providing information for data subjects is essential to their ability to make informed decisions. In some cases, however, more information may be needed in order to enable the data subject to understand the processing operations and make an informed decision.
4. Unambiguous. The element of an unambiguous indication of the data subjects wishes to agree to the processing of their personal data means that it must be clear to which processing operations the consent was given and there should be no doubt whether consent was given or not.

44 Article 29 Data Protection Working Party, WP248 "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", pg. 9
45 It is difficult to provide a comprehensive list of best practices on how address consent with vulnerable data subjects. We recommend as example the *Alzheimer Europe Report, The ethics of dementia research* on how approach and inform people with dementia.
46 On children's consent and parental responsibility please see, Article 29 Data Protection Working Party, WP259 "Guidelines on Consent under Regulation 2016/679", pgs. 24-27.
47 A good practice in case of a person unable to sign or to mark a document to indicate his/her consent, the consent may give orally in the presence of at least one witness, and it should be recorded. [D. Wright and E. Mordini, 2012].
48 Please see, *What if somebody withdraws their consent?* by the European Commission https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en#example

Checklist for the Participant Information Sheets (PIS)

This checklist was designed to give advice in the context of a research project in the field of spatial sciences. The research involves the participation of people in an early stage of dementia. The checklist intends to help to integrate the requirement based on the GDPR and ethical guidelines. Similar checklists, with specific best-practices related to disciplines or research scenarios, can be developed by support staff (RDO, Library and P&S coordinators) in collaboration with the researchers.

The Participant Information Sheet aims to provide to the potential participants a description of the nature of their involvement and, the scope(s) of the processing of their personal data. The potential participants should be informed about their rights and the risks associated with their participation. The researcher should also provide to the potential participants the possibility to receive answers on further questions that they might have.

The content and form of each PIS will depend on the nature of, and the level of risk posed by, the specific research project for which they have been designed. While each PIS is likely to be different, some core pieces of information will generally be included.

Following is, a check-list with the information that needs to be provided to the participants. The reference to the related articles of the GDPR literature and/or the guidance documents made by the Data Protection Working Party (WP) are also included. Extra questions or comments, e.g. based on the ethical guidelines of the Faculty of Spatial Sciences, are presented to contextualize and clarify the meaning of the requested information.

Information about the purpose(s), the data and the data processing:

- A clear statement of the purpose(s) of the research project and the purpose(s) of the processing the data. [GDPR Art. 13(1)(c) and Rec. 42, 33]

  → *Is the purpose(s) of the personal data processing presented in a non-technical language intelligible to the participants? For answer to this question, take into consideration the different stages of the data lifecycle. Process the data with the purpose of answer to a research question(s) is different from the purpose of making the data available to other researchers. If at the end of your project you want making the data opens you need to ask the consent to the participants.*

  → *The GDPR contemplates some flexibility to the degree of specification of consent in the context of scientific research. Recital 33 states: "It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research". However, in case of special categories of personal data, the Data Protection Working Party gives a restricted interpretation of the Rec. 33 and, points at the need to ensure the essence of the consent requirements in others ways, such as in line with ethical standard in scientific research.49*

  → *To compensate for the lack of purpose specification, you may provide to the participants a comprehensive version of your research plan. This research plan should specify the research questions and the working methods envisaged as clearly as possible. The research plan could also contribute to compliance with Article 7(1) GDPR. As controllers you need to show what information was available to data subjects at the time of consent to be able to demonstrate that consent is valid.*

- What (type of) data will be collected and used. [WP259 rev.01 pg 13]

  → *Will the project ensure that persons involved in the project give their informed consent, not only in relation to the aims of the project, but also in relation to the process of the research, i.e. how data will be collected and by whom, where it will be collected, and how the results are to be used? [DW]*

- How the data collected will be handled and protected (e.g. include detail/protocol on the pseudonymization technique) [GDPR Rec. 33]

  → *How has the methodology addressed ways in which sensitive information, data or sources will be handled (e.g. personal data, data protection, tracking of people)? [EC-FSS]*

49 Article 29 Data Protection Working Party, WP259 "Guidelines on Consent under Regulation 2016/679", pgs. 28-29.

→ *What arrangements have been made to preserve confidentiality for the participants or those potentially affected? [EC-FSS]*

→ *Please explain the mechanisms in place to ensure the confidentiality of private information, and compliance with data protection law. [EC-FSS]*

→ *What concerns have been taken into account with regard to the preparation and design of the research project? If agencies, communities or individuals are to be directly affected by the research (e.g. participants, service users, vulnerable communities or relations), what means have you devised to ensure that any harm or distress is minimized and/or that the research is sensitive to the particular needs and perspectives of those so affected? [EC-FSS]*

- The risks of the participation [GDPR Rec. 33]

→ *Will the person be informed of the nature, significance, implications and risks of the project technology?[DW]*

→ *Will the person have an interview with a project representative in which he(s) will be informed of objectives, risks and inconveniences of the project or research activity and the conditions under which the project is to be conducted? [DW]*

→ *Particular attention must be paid to vulnerable categories of individuals such as children, patients, people subject to discrimination, minorities, people unable to give consent, people of dissenting opinion, immigrant or minority communities, sex workers, etc. If your research involves children or other individuals unable to make decisions for themselves, you must maintain an active relationship with their legal guardians and/or carers; you must not only seek their consent, but also allow them to monitor the research. [H2020]*

→ *If the individual is not able to give informed consent (because, for example the person suffer from dementia) to participate in a project or to use of technology, will the project representatives consult with close relatives, a guardian with powers over the person's welfare or professional cares? Will written consent be obtained from the patient's legal representative and his doctor? [DW]*

- If the case, mention of possible commercial revenues from the research, especially when the revenues lead to the conclusion that the data is not processed solely for scientific research.

→ *Please see the case of the use of personal data for commercial purpose recently appeared in the newspaper.*
https://www.dutchnews.nl/news/2018/10/vu-professor-reprimanded-for-using-patient-dna-for-commercial-purposes/

The rights of the participant:

- The existence of the rights of the data subjects (access, rectification, erasure). [GDPR Art. 13(2)(b)]

→ *Does the consent outline the use for which data is to be collected, how the data are to be collected, instructions on how to obtain a copy of the data, a description of the mechanism to correct any erroneous data, and details of who will have access to the data?*

→ *Specific derogations may apply in research project* [GDPR Arts. 85, 89 and UAVG]

- The right to lodge a complaint with a supervisory authority. [GDPR Art. 13(2)(b)]
- A clear statement that participation is entirely voluntary and that participants can withdraw from the project at any time without prejudice, now or in future.

→ *Is consent given truly voluntary? For example, does the person need to give consent in order to get a service to which there is no alternative? [DW]*

- A description of the easy procedures for withdrawal [GDPR Art. 7(3) and WP259 rev.01 pg. 10-11]

→ *Are person involved in or affected by the project able to withdraw from the project and to withdraw their data at any time right up until publication? [DW]*

Plans at the end of the project:

- Plans for storage or archiving the data after the end of the project. The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period [GDPR Art. 13(2)(a)]
  - → *Please take in consideration the institutional and discipline specific guidelines and, if possible add the URL.*
  - → *The period for which the personal data will be stored based on the discipline specific guidelines.*
- Plan for made the data reusable after the end of the project [GDPR Art. 13(3), Rec. 32 and WP259 rev.01 pg. 10]
  - → *The participant needs to give explicit consent on made the his/her data reusable at the end of the project.*

Information on the person that will have access to the data:

- In case of joint-controllers the names of all the controllers and clarification of responsibilities in a transparent way [WP259 rev.01 pg. 13]
  - → *Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. An organization is a joint controller when together with one or more organizations it jointly determines 'why' and 'how' personal data should be processed. In research that could be the case when more than one University are participating in the same project or in case of collaboration with an external party.*
  - → *An alternative would be an elaborated annex to the Data Management Plan available to the participants.*
  - → *Take into account that in case of joint controllers the University of Groningen may have to sign, with the other controller, a cooperation agreement on processing the data (in Dutch "Samenwerkingsovereenkomst verwerking persoonsgegevens").*
- If the case, a full list (no names) of recipients or categories of recipients and processors [GDPR Art.13(1)(e) WP259 rev.01 pg 13]
  - → *Recipients or categories of recipients means internal and external people who will have access to the data.*
  - → *The data processor means a third party which processes personal data on behalf of the controller. The duties of the processor towards the controller must be specified in a contract or another legal act. A typical activity of processors is offering IT solutions, including cloud storage. In research a processor could be a company or a person that process the data during the project: such as, collect the data, transcribe interviews, analyze the data, etc.*
- Where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission. [WP259 rev.01 pg. 18, GDPR Art 46, 47, 49(1)(a)]
  - → *The participant needs to give explicit consent on transfer his/her data.*
- Where applicable, the fact that the controller intends use of automated individual decision-making, including profiling. [GDPR Art. 22(1)]
  - → *"The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." (GDPR Art. 22(1)).*
  - → *The participant needs to give explicit consent to be subject to this process (GDPR Art. 22(2)(c)).*

Contact details:

- Contact details of the University of Groningen and, where applicable, of the controller's representative. [GDPR Art. 13(1)(a)]
- Details of who to contact for further information and complaints
  - → *This information should allow for easy identification of the controller and preferably allow for different forms of communications with the data controller (e.g. phone number, email, postal address etc.).*
  - → *As a further measure on transparency for scientific purposes: while full information cannot be provided at the outset, it could designate a specific contact person for data subjects to address with questions.*
  - → *Data Protection Working Party suggests the use of single point of contact.*
- The contact details of the Data Protection Officer (DPO) and right to complain with the officer. [GDPR Art. 13(1)(b)]
  - → *The DPO of RUG is Arjen Deenen*

Checklist for the Consent form

The consent form should be a short document that concisely covers the core statements to which the participant is being asked to agree.
Separate 'yes/no' tick boxes allow the researcher to make sure that the participant is actively affirming their consent. If the participant wants to tick the no box this allows the researcher to clarify any points the participant is unsure about.
The consent should at least cover the following statements:

- The participant has read and understood the information about the research project and the purpose of the data processing.
- The participant had the opportunity to ask questions.
- The participant voluntarily agrees to participate.
- The participant has been informed of his/her rights.
- The participant understands that he/she can withdraw at any time without giving a reason.
- The participant understands how his/her data will be processed and protected.

The controller may need to obtain from the participant the explicit consent to some specific processes (here some examples):

- Whether the participant agrees or not with the reuse of his/her data at the end of the research project.
- Whether the participant agrees or not with the transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission.
- Whether the participant agrees or not with the use of automated individual decision-making, including profiling.

The form should include the signatures of the participant and dates. It is a good practice include the signature of the person that collect the form.

The participant should receive a copy of the form and, the researcher should retain the signed original.

Reference documents

[WP259] Article 29 Data Protection Working Party, WP259 "Guidelines on Consent under Regulation 2016/679".

[WP260] Article 29 Data Protection Working Party, WP260 rev 0.1 "Guidelines on transparency under Regulation

2016/679".

[WP248] Article 29 Data Protection Working Party, WP248 "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679"

[DW] David Wright and Emilio Mordini "Privacy and Ethical Impact Assessment" in Privacy Impact Assessment, Editors David Wright and Paul De Hert, Pages 397-418, Springer 2012.

[H2020] European Commission "Horizon 2020 Programme Guidance How to complete your ethics self-assessment", Version 6.0, July 2018

[EC-FSS] Ethics guidelines Faculty of Spatial Sciences, University of Groningen.

Annex 5 – Examples use of legitimate interest in research[50]

Example 19: Research on effects of divorce and parental unemployment on children's education attainment Under a research programme adopted by the government, and authorised by a competent ethics committee, research is performed into the relationship between divorce, parental unemployment and children's educational attainment. While not classified as 'special categories of data', the research is nevertheless focusing on issues that for many families, would be considered very intimate personal information. The research will allow special educational assistance to be targeted at children who may otherwise fall into absenteeism, poor educational attainment, adult unemployment and criminality. The law of the Member State concerned explicitly allows processing of personal data (other than special categories of data) for research purposes, provided the research is necessary for important public interests, and carried out subject to adequate safeguards, which are then further detailed in implementing legislation. This legal framework includes specific requirements but also an accountability framework that allows for assessment on a case-by-case basis of the permissibility of the research (if carried out without the consent of the individuals concerned) and the specific measures to be applied to protect the data subjects. The researcher runs a secure research facility and, under secure conditions, the relevant information is provided to it by the population registry, courts, unemployment agencies, and schools. The research centre then 'hashes' individuals' identities so that divorce, unemployment and education records can be linked, but without revealing individuals' 'civic' identities – e.g. their names and addresses. All the original data is then irretrievably deleted. Further measures are also taken to ensure functional separation (i.e. that data will only be used for research purposes) and reduce any further risk of re-identification. Staff members working at the research centre receive rigorous security training and are personally - possibly even criminally - liable for any security breach they are responsible for. Technical and organisational measures are taken, for example, to ensure that staff using USB sticks could not remove personal data from the facility. It is in the legitimate interests of the research centre to carry out the research, in which there is a strong public interest. It is also in the legitimate interests of the employment, educational and other bodies involved in the scheme, because it will help them to plan and deliver services to those that most need them. The privacy aspects of the scheme have been well designed and the safeguards that are in place mean that the legitimate interests of the organisations involved in carrying out the research are not overridden by either the interests or privacy rights of the parents or children whose records formed the basis of the research.

Example 20: Research study on obesity A university wants to carry out research into levels of childhood obesity in several cities and rural communities. Despite generally having difficulties gaining access to the relevant data from schools and other institutions, it does manage to persuade a few dozens of school teachers to monitor for a period of time children in their classes who appear obese and to ask them questions about their diet, levels of physical activity, computer-game use and so forth. These school teachers also record the names and addresses of the children interviewed so that an online music voucher can be sent to them as a reward for taking part in the research. The researchers then compile a database of children, correlating levels of obesity with physical activity and other factors. The paper copies of the completed interview questionnaires – still in a form that identifies particular children – are kept in the university archives for an indefinite period of time and without adequate security measures. Photocopies of all questionnaires are shared on request with any MD or PhD student of the same and of partner universities across the world who show interest in further use of the research data. Although it is in the legitimate interests of the university to carry out research, there are several aspects of the research design that mean these interests are overridden by the interests and rights to privacy of the children. Besides the research methodology, which is lacking in scientific rigour, the problem emanates in particular from the lack of privacy enhancing approaches in the research design and the broad access to the personal data collected. At no point are children's records coded or anonymised and no other measures are taken to ensure either security of the data or functional separation. Valid Article 7(a) and Article 8(2)(a) consent is not obtained, either, and it is not clear that it has been explained to either the children or their parents what their personal data will be used for or with whom it will be shared.

50 WP29 "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" http://www.dataprotection.ro/servlet/ViewDocument?id=1086

Annex 6 –Scoping Report template

DPIA Scoping report <Project Title>

The DPIA is carried out within the framework of:

Project title:

Project leader:

Project code:

Version and archiving data:

Why a DPIA:

A Data Protection Impact Assessment (DPIA, in Dutch "Gegevensbeschermingseffectbeoordeling") is a method to:

1. Map the data privacy risk in a process or project;
2. Assess these risks; and
3. Define measures to avoid or mitigate the risks.

Summary

DPIA Method:

This DPIA is carried out on the basis of a method drawn up by Bieker et al.[51]. The method includes three phases. The first phase (A) is a preparation phase that examines whether a DPIA is needed and what the scope and objects of the DPIA are. On this basis, a "scoping report" is prepared. The second phase (B) concerns the identification of risks for the protection of the privacy of data subjects. The third phase (C) concerns the formulation and application of appropriate protection measures with which these risks are eliminated or mitigated. The phases and the information to be collected, the analysis and the measures that have to be performed are described in detail in the method and are therefore not explicitly quoted in this report. The layout of the report is based on the steps taken during the phases described in the method.

The DPIA will have to comply with the requirements set by the GDPR (Article 35 of the GDPR). The article 29 Working group, European joint venture of the national privacy supervisors (WP29), has published a number of guidelines for the execution of a DPIA[52]. These guidelines are followed as much as possible.

Phase A – Preparation Stage (scoping report)

A1. Explanation on the choice for performing the DPIA:

A.1.1 Identification of issues in the research project *<Description of the privacy issues identified in the project.>*

A.1.2 Clarify responsibilities *<This section may include responsibilities internal/external to the project (collaboration with other university or companies) and in the university organization (Deans, director of research units, etc.)>*

A2. Scope of the DPIA and DPIA team:

Short description of the project:

Scope of the DPIA: < which processing of personal data falls within the scope?>

51 Felix Bieker, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost, "A Process for Data Protection Impact Assessment under the European General Data Protection Regulation", in K. Rannenberg and D. Ikonomou, Privacy Technologies and Policy, Fourth Annual Privacy Forum, APF 2016 Frankfurt. Heidelberg, New York, Dordrecht, London.

52 Article 29 WP, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679', Rev 0.1, 4 oct. 2017.

Person responsible for the DPIA:

DPIA team: *(A DPIA has the best result in a multidisciplinary team. Examples of team members are: project leaders, project participants, IT experts, Information Security experts, IT lawyers, Data Protection officers.)*

Support: *<persons who support the execution of the DPIA>*

Advice Data Protection Officer/Privacy professional: <>

Persons concerned: asking for the opinion of the parties involved or their representatives about the processing is required in 'appropriate cases' (Article 35, paragraph 9 GDPR)[53].

A3. Target of evaluation: description of the system, identification of data and data flow.

Data flow: *<Insert an overview of these data flow with the route of the data and the type of data>*

Intended processing: *<indicate here the intended processing with regard to personal data. Processing concerns all actions relating to personal data, such as collecting, recording, organizing, structuring, storing, updating or modifying, retrieving, consulting, using, providing by means of forwarding, distributing or otherwise making available, aligning or combining, shield, erase or destroy.>*

Purpose processing: *<description of one or more purposes>*

Types of personal data: personal data are all the information about an identified or identifiable natural person. The identification can be direct or indirect. The latter means that the identification becomes possible only through the combination of the data with other data that an organization has.

Some technical aspect of the process may affect the rights and freedoms of the data subject. The method mentions the following:

File formats: <...>

Data transport protocols: <...>

IT systems used: <...>

Procedures: <...>

Configuration of authorities within a system based on roles and functions: <arranged yes / no>

A4. Actors and role in the project:

The GDPR defines various roles for natural persons and organizations that process personal data. For each role the GDPR defines a set of obligations regarding the protection of the rights and freedoms of the person concerned. This 'division of roles according to the GDPR' is determined in the DPIA process.

a. <...> is / are controller(s)

b. <...> is / are the processor of <controller>

c. <...> is / are subprocessor of <processor>

d. <...> is / are the person(s) concerned

A5. Identification relevant legal issues:

a. **Other legislation relating to the protection of personal data:** <..>.

b. **Other legislation:** <...> (e.g. sector-specific legislation for the protection of personal data or custody obligations)

c. **Code of conduct:** <...>

d. **Policy:** <...> (the privacy policy, information security policy and the other standards to which the parties involved in the project are bound are included where necessary).

53 See note 2.