



Pitch: Linking privacy risks and preventive action to research scenarios
Name: Fieke Schoots and Raymond van Erkel (LEI)
Date: May 2019
Contact: f.schoots@library.leidenuniv.nl and r.van.erkel@fsw.leidenuniv.nl

1. Goal (problem definition, solution approach) and demarcation of the subject.

On April 10, the national Disciplineoverleg Sociale Wetenschappen (Consultative Body for Social Sciences) (DSW) discussed a proposal that would make it easier for researchers to comply with AVG. The proposal foresees in the forming of a task group that will pave the way for the sharing of Data Protection Impact Assessments (DPIA's) at a national level for frequently used research scenarios in Social Sciences.

The researcher is expected to protect a research subject's privacy against risks posed by scientific research. Taking extra precautions when dealing with personal data is part of this. The General Data Protection Regulation (GDPR) lists the applicable rules. The GDPR obliges a researcher to do his/her utmost to minimize risks for research subjects by taking the necessary organizational and technical measures. A researcher should make a prior inventory of privacy risks a research subject could face by using a Data Protection Impact Assessment (DPIA). A DPIA indicates which measures are appropriate to properly safeguard the processing of (special) personal data. A DPIA is compulsory when data processing prompts a high privacy risk. In the social science domain this is often the case. Since the introduction of GDPR, social science researchers who often work with personal data, are experienced in carrying out risk assessments.

An institute is obliged to facilitate a researcher in safeguarding the privacy of research subjects and must offer the necessary amenities and support. A researcher is assisted by various research support staff for the ethical and legally justifiable execution of research according to the applicable rules and legislation: a privacy officer, a functionary for data protection, an ethical committee and a research data support officer. A collective (multi-stakeholder) implementation of a DPIA by interested parties leads to a better mutual understanding of which actions, measures, roles and responsibilities result in a proper degree of data protection.

Expectations are that sharing "DPIA reports can lead to better insights that make it easier to take the correct technical and organizational measures when controlling research" and that "institutes will quickly be able to link lists of basic measures for data protection to specific research scenarios, so that DPIAs can be carried out relatively quickly" (quoted in the consultation version of the VSNU [Association of Universities in the Netherlands] code of conduct for use of personal data in scientific research, version 0.9, October 2017).

The task group will give form to this learning process by bringing together insights gleaned from DPIAs of regularly undertaken research in social sciences. It is possible to conduct one DPIA that covers a series of comparable processes with risks of a similar magnitude. The idea is to carry out and sustain one DPIA per research scenario, so that for a large part of new research, only the right scenario need be selected. A DPIA need only be drawn up if a research project with personal data does not fall within one of the pre-determined scenarios.

The task group will submit an advisory report to the initiator of the proposal, the Disciplineoverleg Sociale Wetenschappen (Consultative Body for Social Sciences). Due to practicalities, the task group will limit itself to scenarios in Social Sciences.

2. Why is this of institute-transcending importance?

DPIAs are carried out at the faculty of Social Sciences. The task group will pool all resulting insights on a national level to create a reference frame for DPIAs of frequently undertaken research. From this good practices can be distilled which in turn are shared with the various Social Science faculties. A researcher can choose the scenario that is best suited to the research he/she is undertaking. This also supports the researcher in substantiating choices made regarding the progress of his/her research and the privacy of a research subject. The choice of scenario, the corresponding DPIA and any measures taken are recorded in a process register. As a result DPIA support will become more advisory in nature and focus less on the actual filling out of a DPIA. How measures instigated by a DPIA are put into practice may differ from one institute to the next. Every institute has a privacy and information protection policy and own facilities to implement procedures.

3. Deliverable/output, what is the expected yield? (the “product”) + rough outline.

The product consists of an advisory report submitted to the DSW which is made up of:

- An inventORIZATION of the scenarios and the corresponding assumptions
- A framework for classification of research according to certain scenarios with the aim of carrying out DPIAs
 - o Based on criteria like: type of research method, type of data, nature of personal data, research location, type of research subject (vulnerability), source of data, and collaboration with third parties.
- An elaboration of the scenarios that have a privacy and security DPIA classification
 - o This depends on which basic procedures are followed for research that involves personal data.
- Recommendations about implementation, managing and maintenance of the devised scenarios.

As a follow-up to the work of this task group, the scenarios may be broadened to include other research fields. Another possibility is to develop an itinerary for a legally binding advice with the Autoriteit Persoonsgegevens (Data Protection Authority).

4. Which expertise/competencies are necessary to form a task group? And what resources do you think you need?

To form a task group we are looking for colleagues with research know-how and experience with carrying out Privacy Impact Assessments in Social Sciences. Ideally we would like a broad set of representatives from all over the country who are active as either researcher, research data support officer, privacy officer, data protection functionary or security officer. Taking into account the interest that exists for this topic, we also expect to set up a sounding board group. The following is a list of persons who have agreed to collaborate on behalf of the institute they work for. We invite institutes that are not yet represented to make their interest known. The ultimate composition of the task group and sounding board group will take place in consultation with the LCRDM.

- Annemiek van der Kuil (UU, consultant RDM)
- Cristina Montagner (RUG, data consultant)

- Fieke Schoots (LEI, RDM support functionary CDS)
- Jessica Hrudey (VU, research data officer FGB; sounding board group)
- Marco Teunisse (UvA, information manager FMG)
- Marlon Domingus (EUR, data protection functionary)
- Mijke Jetten (RU, open science support & data steward Management Sciences)
- Raoul Winkens (UM, data protection functionary)
- Raymond van Erkel (LEI, information manager & privacy officer FSW)

The sounding board group will include representatives of DSW and Nethics (Nationaal Ethiek Overleg Sociale en Gedragwetenschappen or National Consultative Body for Ethics in Social and Behavioural Sciences)

- DSW sub-committee Scientific integrity, data storage and reproducibility: Sander Nieuwenhuis (LEI)
- Nethics: still to be determined

Results will be nationally coordinated with:

- LCRDM: RDM support staff
- SCIPR: data protection functionaries
- SCIRT: security officers

We will make use of existing communication channels and besides the commitment of the task group members, we have no need of extra resources.

5. Estimated duration (2 months maximum) and desired planning (desired start – date of completion)

June 2019 – October 2019. We will do our best to start before the summer holidays.

6. What is already known/has already been done and why does this information not suffice?

There have been various initiatives that have not yet been weighed against each other. There are different frameworks for classifying scenarios. A uniform selection of scenarios does not exist nor is there agreement about the underlying assumptions. The corresponding DPIAs cannot be used in an institute transcending way.

- At the beginning of 2018 UM developed a set of scenarios that was used at the Psychology faculty.
- Towards the end of 2018 UvA issued a document that serves as a point of departure for carrying out an IB&P risk analysis for research.
- EUR recently drew up a document about DPIAs and scenarios.
- At the RUG, a plan has been devised for scenarios with reference DPIAs and procedures in the form of building blocks for the benefit of the Faculty of Behavioural and Social Sciences.
- In the consultation version of the code of conduct for use of personal data in scientific research, the VSNU has given a broad description of several scenarios.
- A code of conduct exists for statistic and data- analytical study of market research (has not yet been made public).
- In March 2019, the NFU established quality assurance guidelines for human research.