Privacy and GDPR Compliance Checklist for Doing Research

This checklist enables you to assess in a few steps whether you process personal data during your research and what measures you should take to process the personal data in accordance with the GDPR. You need to assess this when you are designing the research, so in the phase in which the research plan is written, so you will not be taken by surprise on this point during the research.

The plan of approach is based on the metro map which Marlon Domingus of the EUR has developed for academic research.

1 Do you process personal data?

(Please note that the use of personal data to approach respondents also falls under cases in which the GDPR is applicable).

a. No > the GDPR is not applicable

b. Yes > go to question 2

Personal data: data that can identify a natural, living person directly or indirectly

(Article 4 of the GDPR)

2 What is the aim of processing data?

Personal data such as data used in surveys is often collected and processed for a specific purpose (e.g. in the context of a research). Personal data collected for another purpose is also made use of sometimes.

- Has permission been granted for further use or is the use of data compatible with the purpose for which this data has been collected?

There should be purpose limitation. In principle, you are only allowed to process collected personal data for the purpose you have acquired them for or the new purpose is compatible with the original purpose the data have been collected for.

3 What is the basis for processing?

- Do respondents give consent?
- Is there a general interest or a legitimate interest for processing during the research?

Without any basis, processing is unlawful and fines can be imposed by the AP.

4 How do you estimate the risk of processing personal data?

- Is there a significant risk or a low risk?

So, it really concerns the processing of personal data during the research; when respondents fill in data anonymously and this data cannot be traced back to individuals, this is not considered a high risk. In fact, then you only process data for inviting people to take part in the research).

There is a significant risk when very sensitive data are processed (e.g. think of medical data), when data is processed on a very large scale, data of vulnerable groups (e.g. minors, the disabled).

- Do you doubt the risk level?

In that case, you could contact the Data Protection Officer to make an estimate of and assess the risk. If there is a significant risk, extra safeguards might be required to be able to carry out the research in accordance with the GDPR.

5 Describe in your research proposal how you process personal data in accordance with the GDPR.

a. Fill in a DPIA and discuss it with the DPO. On the basis of this document, the DPO can estimate the risk and fill in the obligatory records of processing activities. The DPIA is an obligatory part of the research plan.

b. Describe who might receive any personal data. If you process all input of respondents anonymously, state it.

c. Make sure that the personal data you process are processed safely, and take the following into account:

- Informing the parties involved (the people whose data you are processing). They should be well informed.
- How is the data stored? And where? Make sure that the data stays in the EU and make use of the applications made available by BUas. Do not use, for example Google Drive or We Transfer!
- Who has access and how is this access determined and given? Is, for example two-factor authentication used?
- Are partners cooperated with, and have any agreements been made (are any agreements made) about how to deal with personal data (Please note: both partners are probably responsible). You do not need any processing agreements, but, for instance a cooperation agreement, in which you make agreements about how to deal with personal data.

Any questions? Please contact the Data Protection Officer of BUas => FG@BUas.nl