Privacy in Research

Auteur	Sander van Acht
Team	SURF Privacy Awareness
Laatst gewijzigd	4 februari 2019
Licentie	CC Naamsvermelding 4.0 Internationale licentie
Webadres	https://maken.wikiwijs.nl/125518/

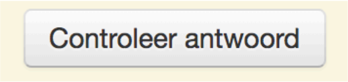
Inhoudsopgave

Welcome

Welcome to 'Privacy in Research'

What does the GDPR mean for your work as a researcher?

This course contains some Dutch-language buttons. You'll find the English translation below:

← Vorige	- previous
Volgende →	- next
 Controleer antwoord	- check answer
Goed	- right
Fout	- wrong
Keuzemogelijkheden	- options
Combineer met de keuzemogelijkheden	- combine with the options

Questions?

If you have questions about this course, please contact **info@cybersaveyourself.nl**.

Purpose and summary

From 25 May 2018, the General Data Protection Regulation (**GDPR**) applies. This means that from this date the same privacy legislation applies in the entire European Union. The Dutch Data Protection Act (Wbp) will no longer apply from this date.

What has changed?

The GDPR ensures amongst other things:

- reinforcement and extension of privacy rights;
- more responsibilities for organisations;
- the same, robust powers for all European privacy supervisors, such as the authority to impose fines of up to €20 million.

The GDPR has significant consequences for the work of researchers as well. This online module and the follow-up session at your university or university of applied sciences will help you to know exactly which changes it entails for your specific type of research, but above all which opportunities the GDPR offers.

Purpose

The purpose of this module is threefold:

- You learn what the GDPR entails;
- You know which aspects of the GDPR are important for your research project;
- You are aware of the steps you can take to comply with the GDPR.

Target group

This module is developed for researchers who are associated with a university or university of applied sciences.

Summary

This online module consists of three sections:

- You will work through three research cases, each with a short quiz to test your current knowledge of the GDPR;
- You will get to know various aspects of the GDPR, such as the DPIA, 'Privacy by Design' and the six rules of thumb;
- Using three scenarios, you will learn which criteria determine an important part of the measures within a study.

Duration

The entire module will take approx. 45 minutes.

Three cases

What is your current knowledge of the GDPR? How effective can you choose adequate technical and organisational measures to be taken in the context of a certain research project? In order to test yourself, we offer you three introductory cases. Please read each case carefully before trying to answer the questions.

Go straight to:

Case ❶: Bullying among young people. What interventions are effective to reduce bullying?

Case ❷: Are the rich more selfish than the poor, or do they just have more money?

Case ❸: Can big data demonstrate efficiency in healthcare in the EU?

Case 1: Bullying among young people

This case focusses on bullying among young people and possible interventions. Please take your time to read the information about the case before trying to answer the questions. In this way you will discover your current knowledge of processing personal data in this type of research.

Title of the study:

"Bullying among young people aged 12 - 18"

Purpose of the study

This study researched the extent to which bullying at school among young people aged 12 - 18 occurs and which interventions can contribute to the reduction of bullying behaviour.

Set-up of the study

COLLABORATION	GEOGRAPHY	DATA
This study was carried out in the sociology department of one university.	This study was carried out in the Netherlands.	This study did not use existing data sets.

Performance of the study

In this case, the researcher wanted to build up a data set using video recordings in the classroom and interviews with young people. In broad lines, the study included the following steps:

1. The researcher asks teachers in schools if they are interested in participating and explains the study.
2. The researcher uses forms to ask teachers and parents which (minor) students are allowed take part.
3. Students that are not allowed to take part are given a red sticker, the other students get a green sticker.
4. The researcher makes the recordings and ensures the 'red stickers' are out of shot. The interviews are conducted.
5. The researcher transports the data by public transport to the university for processing in the study.
6. The researcher publishes the study and archives the data. At conferences, he shows parts of the video recordings.

This gives you a general impression of the set-up and performance of this study. Now, use the exercise below to check the extent of your current knowledge of handling personal data processing in this type of study:

Oefening

Bullying among young people
https://maken.wikiwijs.nl/p/questionnaire/standalone/4392025

Algemene Informatie

Titel	Bullying among young people
Aantal Vragen	3

Which measures must the researcher in this case take to ensure proper processing of personal data? Do the test to find out your current knowledge of the GDPR. Good luck!

MAIN_SECTION

Step 1: The researcher asks teachers in schools if they are interested in participating and explains the study.

Does the researcher process personal data in this first step?

○ No

○ He probably does

Step 2: The researcher uses forms to ask teachers and parents which (minor) students can take part.

For what must the researcher ask permission in the forms?

□ From the parents: for filming their minor children

□ From the parents: for interviewing their minor children

□ From the school principal and teacher: for filming the teacher in the school and for the fact that filming is taking place in his/her classroom

□ From the young people aged 16 and over: for filming and conducting the interviews

---

Step 6: The researcher publishes the study and archives the data. At conferences he shows parts of the video recordings.

Can you show parts of video recordings from a study at a conference or during your classes?

○ Yes, if permission is obtained for this

○ Yes, because it gives good insight in the theory

○ Yes, if the conference or class is not open to the general public

○ Yes, if the research subjects are present themselves

After finishing the exercise, click 'Volgende' in the bottom righthand corner to go to the next page.

Case 2: Wealth and selfishness

In this case, possible egoistic behaviour of wealthy people is central. Please take your time to read through all of the information about the case before trying to answer the questions. In this way you will discover your current knowledge of handling personal data in this type of study.

Title of the study:

"Are rich people more selfish than poor people? "

Purpose of the study

This study researched the extent to which wealthy people show selfish behaviour compared to less wealthy people.

Set-up of the study

COLLABORATION	GEOGRAPHY	DATA
This study was performed in the department of one university.	This study was performed in the Netherlands.	This study used a CBS data set.

Performance of the study

In this case, the researcher sent so-called incorrectly addressed mail containing cash to wealthy and less wealthy people. The data about the wealth of the persons involved was derived from the CBS. In broad lines, the study included the following steps:

1. The researcher divides two areas in a city into 'poor' and 'rich' based on CBS data.
2. The researcher sends without prior permission ('covert research') a letter with cash to all addresses.
3. The researcher registers which percentage from both areas returns the 'incorrectly addressed' mail.
4. The researcher processes the data at the university.
5. The researcher publishes the study and archives the data. Afterwards, he informs the persons involved.

This gives you a general impression of the set-up and performance of this study. Now, use the exercise below to check the extent of your current knowledge of handling personal data processing in this type of study:

Oefening

Wealth and selfishness
https://maken.wikiwijs.nl/p/questionnaire/standalone/4392029

Algemene Informatie	
Titel	Wealth and selfishness
Aantal Vragen	3

Which measures must the researcher in this case take to ensure proper processing of personal data? Do the test to find out your current knowledge of the GDPR. Good luck!

MAIN_SECTION

Step 2: The researcher sends without prior permission (‘covert research’) a letter with cash to all addresses.

Is 'covert research' permitted by the GDPR?

○ No, it is never permitted

○ It is only permitted on specific conditions

Step 2: Adequate measures

Which measures would be 'appropriate' in covert research and in this study?

○ Strong de-identification of personal data, informing the persons involved about the study at the end.

○ Not publishing data in the country in which the study was performed.

○ Using fictitious names for the persons involved.

Step 4: The researcher processes the data at the university.

Are you only allowed to process personal data at the university according to the GDPR?

○ No

○ Yes

After finishing the exercise, click 'Volgende' in the bottom righthand corner to go to the next page.

Case 3: Healthcare efficiency

This case focusses on the possible increase in efficiency in healthcare by using big data. Please take your time to read through all of the information about the case before trying to answer the questions. In this way you will discover your current knowledge of handling personal data in this type of study.

Title of the study:

"More efficient healthcare in the EU by using big data?"

Purpose of the study:

This study researches the extent to which linking large data sets from healthcare insurers, hospitals and private clinics may lead to faster diagnoses, more effective logistics, shorter waiting times and less impact on patients.

Set-up of the study:

COLLABORATION	GEOGRAPHY	DATA
This study was performed in collaboration with various European public and private parties.	This study was performed in EU and non-EU countries (Norway, Israel).	The study is solely based on existing data sets.

Performance of the study:

This case focussed on the creation of contracts between all of the participating parties. Who would have access to which data sets, both prior to and after delivery of the publication? In broad lines, the study included the following steps:

1 All parties involved drafted a joint proposal for a European grant which was awarded.

2 All parties involved have created contracts regarding the processing, access, storage and publication of the data.

3 In order to be able to measure efficiency gains, measurements are performed in various work packages.

4 The measurements are cause for supplementary interventions to enhance efficiency.

5 In addition to the research data, 'lessons learned' and preconditions from this study are published.

6 The study is published and the data is archived.

This gives you a general impression of the set-up and performance of this study. Now, use the exercise below to check the extent of your current knowledge of handling personal data processing in this type of study:

Oefening

Healthcare efficiency
https://maken.wikiwijs.nl/p/questionnaire/standalone/4392033

Algemene Informatie

Titel	Healthcare efficiency
Aantal Vragen	2

Which measures must the researcher in this case take to ensure proper processing of personal data? Do the test to find out your current knowledge of the GDPR. Good luck!

MAIN_SECTION

Step 2: All of the parties have created contracts regarding the processing, access, storage and publication of any of the data.

Can you start a study in collaboration with a private party without a contract setting out the arrangements with regard to data?

○ No

○ Yes

tep 3: In order to be able to measure efficiency gains, measurements are performed in various work packages.

A hospital and a healthcare insurer are collaborating here. Do they need access to the same data?

○ Yes

○ No

After finishing the exercise, click 'Volgende' in the bottom righthand corner to go to the next page.

Quick wins

You see from the three cases that specific measures are required for each study to ensure correct handling of personal data. However, there are also general 'quick wins' for researchers: simple adjustments in your working method that ensure considerable extra security. This page contains a brief overview.

What can you do already?

Below you see seven relatively simple actions that ensure a significant reduction of the risk of data leaks in your study. We recommend every researcher to implement them wherever possible.

Privacy filter: A special type of foil that can be applied to every laptop or desktop screen. It ensures that the viewing angle is significantly reduced to make it more difficult for other people to view your screen. Useful when you are working a lot on the go. Search for 'privacy filter laptop' to find a suitable type.

Webcam cover: Without you noticing it, malicious people can view through your webcam. A webcam cover is a 'small lock' that is simple to apply and can fully cover the webcam when required. This makes viewing by others a thing of the past. Search for 'webcam cover' to find a suitable type.

Encryption of the hard drive: With encryption the data on the drive is secured against unauthorised access, as this drive can be easily removed from your laptop and be read effortlessly by a pc. For Windows computers, BitLocker Drive Encryption is a good option, for Macs this is FileVault.

Terms of service reader: Many online services have included provisions in their 'terms of service' on what they can do with your data. There are add-ons available for your browser to make it easier to asses these often lengthy 'terms of service' documents. These add-ons give a quick insight into the risks you run by using the service.

Anti virus software: To prevent malicious people from getting access to your computer or laptop, quality anti-virus software and regular installing of updates are important. This software keeps your computer clean and safe.

Anti-tracking and anti-cookie software: For web browsers, software is available that analyses cookies for you, indicates what these cookies do and already eliminate harmful cookies. This software also checks whether a party is 'tracking' you and thus is gathering information about you which it may forward to third parties.

Privacy in research

Personal data. Why would you handle it with care? It only takes extra time and trouble to properly arrange it all. No... It can even offer you a lot of benefits. Really. Here are four reasons why careful handling of personal data may be important.

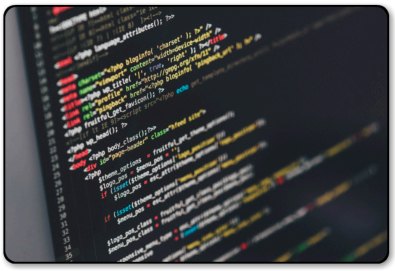
1. Code of conduct

In the 'Netherlands Code of Conduct for Scientific Practice' (2014) safeguarding the privacy of persons involved in the research is explicitly referred to as a further interpretation of the principle of 'honesty and scrupulousness'. This code of conduct sets out the principles that Dutch scientific practitioners should adhere to for the correct performance of their task and to which they can be held accountable where appropriate. It reads:

"Every academic practitioner demonstrates respect for the people and animals involved in scientific teaching and research. Research on human subjects is exclusively permitted if the persons concerned have freely given informed consent, the risks are minimal and their privacy is sufficiently safeguarded."

2. Accountability

The new privacy legislation GDPR offers instruments such as the DPIA (Data Protection Impact Assessment) to help you to review your study even more proactively. These instruments give you an exact insight into the challenges with regard to privacy that apply to your study, enable you to anticipate quicker and ensure that you are more 'in control' during the study. This provides a clear overview, prior to the research project, to safeguard privacy in the different stages of your research, in terms of compliance to the GDPR.



3. Impact

Researchers do not only seek scientific impact, but also aim to have impact on society. Demonstrably safeguarding the privacy of all persons involved, and transparency about how you do this, contributes to confidence in research in general and in the reliability of the institution you are associated with. Data leaks harm the trust in research, the institution and the researcher.

4. Collaboration

Safeguarding privacy is also important for your attractiveness as a reliable (international) research partner, so that in addition to your substantive contribution you also distinguish yourself in a preconditional sense. In this way it is easier for you to participate in research consortiums and compete for research funding.

The GDPR

The new privacy law which takes effect on 25 May 2018, is called the General Data Protection Regulation or GDPR. This regulation applies to all persons in organisations that process personal data of European citizens, therefore including staff from the university or university of applied sciences. This page provides a brief introduction to the GDPR and sets out what is specifically relevant for researchers.

The GDPR in a nutshell

If you do not use any personal data in your research, the GDPR does not apply. However, if you do, the GDPR is important to you.

Feel like totally immersing yourself in the GDPR? Please follow **this link** to the full wording of the regulation. No time to read all 88 pages? The six key issues from the GDPR that every researcher should know are:

1. Focus on the **privacy rights** of the **persons involved**, not on your research results.
2. The GDPR is based on **principles** and only states **that** you have to organise matters regarding privacy.
3. **What** exactly you should do depends of the **research context**. As soon as you know this, the measures are clear.
4. Before you start your study and in the event of significant changes, perform a **DPIA**.
5. **Privacy by Design**: When you set up your study, build in measures to promote privacy.
6. **Privacy by Default**: Ensure that the default settings of all of your systems promote the privacy of the research subjects.

Preparing for the GDPR?

The Dutch Data Protection Authority (DPA) supervises compliance with the legal rules for the protection of personal data. This supervision covers various activities including research.

Another important task of the DPA is giving advice on new regulations. In this latter role, the DPA has described ten steps you can take to properly prepare for the GDPR. The video below clearly explains these steps. If you prefer to read the steps, you can download them as a text document underneath the video. We do recommend that you review these steps carefully.

https://www.youtube.com/embed/afyxuxHK1Xc?rel=0&showinfo=0

Video produced by Karel Roos, ICT- and ICT&O advisor/coordinator, Leiden University

Preparation for the GDPR in ten steps

Need more help?

This module discusses in more detail what you, as a researcher, have to (and can) do with the GDPR. If you already want to study the GDPR in more detail, we recommend you start with the site **hulpbijprivacy.nl**. This website from the Dutch Data Protection Authority offers clear general information about the GDPR.

Via **this SURF website** you can find a Wiki explaining the regulation and its interpretation, plus a comparison with the Dutch Data Protection Act.

Six rules of thumb

The GDPR is based on six principles, also referred to as rules of thumb. It is important for researchers to keep these rules of thumb in mind in every phase of the study. Applying these rules of thumb consistently, reduces the risk of errors while dealing with personal data.

Six questions

Below are the six rules of thumb each with an associated question. If during the study the answer to one of these questions is 'no' you will have to adjust your study. For instance, informing the persons involved ('Transparency'), destroying the personal data ('Storage limitation') or asking for an age range instead of a year of birth ('Data minimisation').

Purpose & purpose limitation

Am I using the personal data only for the purpose of my study?

Basis

Is there at least a legal basis for processing the data?

Data minimisation

Am I only using the data required for the realisation of the established purpose?

Transparency

Have I informed the persons involved clearly in advance about the purpose of the data processing?

Data integrity

Is the personal data I use still accurate?

Storage limitation

Do I really need the data after a certain period?

Read through the six rules of thumb before trying to answer the questions below correctly:

Oefening

Six rules of thumb
https://maken.wikiwijs.nl/p/questionnaire/standalone/4392043

Algemene Informatie

Titel	Six rules of thumb
Aantal Vragen	6

Start each time by reading the descriptive summary before answering the question. Good luck!

MAIN_SECTION

Transparency

In the context of transparency, do you always have to inform the person(s) involved in advance of the study?

○ Yes

○ No

Data integrity

Data integrity means maintaining and safeguarding the accuracy and consistency of the personal data.

○ Yes

○ No

Storage limitation

Can you use data for a longer period than the 'standard' period of 10 years (as set out in the Netherlands Code of Conduct for Scientific Practice of the Association of Universities in the Netherlands)?

○ Yes

○ No

Basis

The two bases on which you may process personal data as a researcher are:

1. processing personal data on the basis of informed consent

2. processing personal data on the basis of scientific research

○ Correct

○ Incorrect

Purpose and purpose limitation

You are researching the effects of smartphone use on the sleep pattern. Can you use this research data also for a study of addiction to smartphone use?

○ Yes, you can if you comply with the conditions provided in the law

○ No, never

Data minimisation

You are researching drug use among young people to establish the extent to which young people over 16 years of age use certain drugs. What data do you need at least?

○ Date of birth

○ Age range

Privacy by Design

Privacy by Design. One of the key starting points for proper handling of personal data. It means that you do not only describe clearly in your research plan how you will safeguard privacy, but also that you take the correct technical and organisational measures for every step in the research process. This exercise will show you which they are.

Exercise 'Privacy by Design'

Every study is different, so the exact measures to be taken for every step in your study differ as well. What is important is the 'mindset' that you focus on privacy throughout your study.

Below shows a study divided in six steps. Try to discover the technical and organisational measures that you could take with every step.

Exercise

Drag the correct measures to the correct step in the study:

□	Drawing up a research plan	**a**	Ensure you have 'informed consent'; your research subjects must know what they agree to and must be able to withdraw.
□	Data collection	**b**	Archive the data for which you have permission for follow-up research and actually destroy data that can be destroyed.
□	Data processing	**c**	Publish and share data only in the way in which the research subjects have authorised.
□	Data storage	**d**	Only edit data at moments when nobody else can view your screen.
□	Collaboration	**e**	Perform a DPIA and where necessary adjust your plan.
□	Publication	**f**	Make sure you have an encrypted and, where necessary, anonymised location

		to store your data.
□ Archiving / destruction	g	If you collaborate with other parties/ persons, make clear agreements about who can access which type of data.

Context

The specific organisational and technological measures you have to take in every step of your study depends on the context in which you perform the study. This involves questions such as:

- Does the study involve collaboration of **public** or **private** parties?
- Are multiple **countries** involved in the research and if so, which?
- Does the study assume existing **data sets** or does the study only create a new data set?
- Do the researchers use **new** technologies or very **extensive** data sets in the study?

To know which measures apply in your situation, you may perform a DPIA prior to your study. The Dutch name for this is a 'gegevensbeschermings- effectbeoordeling'. We will discuss this in more detail on the next page.

DPIA

How do you, as a researcher, know you have taken all possible measures to protect the personal data in your study? You use a Data Protection Impact Assessment (DPIA). In Dutch: a 'gegevensbeschermings-effectbeoordeling'.

A DPIA can best be compared to a traffic light. It contains a series of questions that show for which points in your study the light is green, yellow or red in respect of handling personal data. On this page we explain how it works.

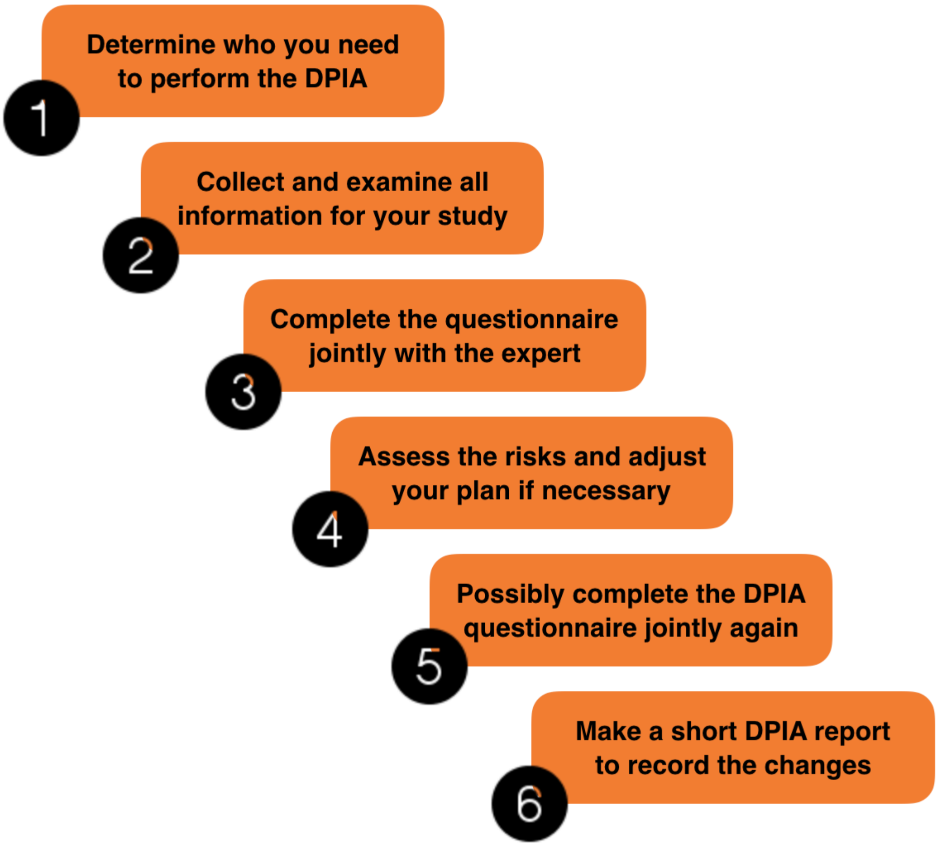
Why?

In the GDPR, a DPIA serves as a risk assessment. It is a structured way to identify risks with regard to the handling of personal data in a study. Answering all of the questions in the DPIA together with a privacy expert in your organisation will give you an overview of the potential risks, so that you can take relevant measures in an early stage. This will save you a lot of time, and in particular prevents risks of data leaks, later on in your study.

How?

You always carry out a DPIA when the design of your study has been outlined. Together with a privacy expert (often a 'data steward') in the organisation, you go through the questionnaire. This will mostly take an hour to ninety minutes. The questionnaire will result in a risk analysis that may be the basis of adjustments of parts of your research plan. Subsequently another DPIA may be performed to check your adjusted research proposal for risks.

The framework of the process is as follows:


1
Determine who you need to perform the DPIA
2
Collect and examine all information for your study
3
Complete the questionnaire jointly with the expert
4
Assess the risks and adjust your plan if necessary
5
Possibly complete the DPIA questionnaire jointly again
6
Make a short DPIA report to record the changes

Example

As mentioned, a DPIA is a questionnaire. If you already want to have a look at the questions covered in a DPIA, view an example **here**. Please note: the questionnaire used by your organisation may differ from this one. Ask your internal privacy expert (often the 'data steward') about the DPIA used by your organisation.

Scenarios

Every study is unique, that much is certain. Fortunately, that does not mean that for each separate study you have to determine the measures required to safeguard the privacy of the research subjects all over again. Three criteria offer you a handle here: **collaboration**, **geography** and type **data**.

Purpose

The purpose for every researcher with regard to the correct handling of personal data is clear:

100%
insight in the measures to be taken

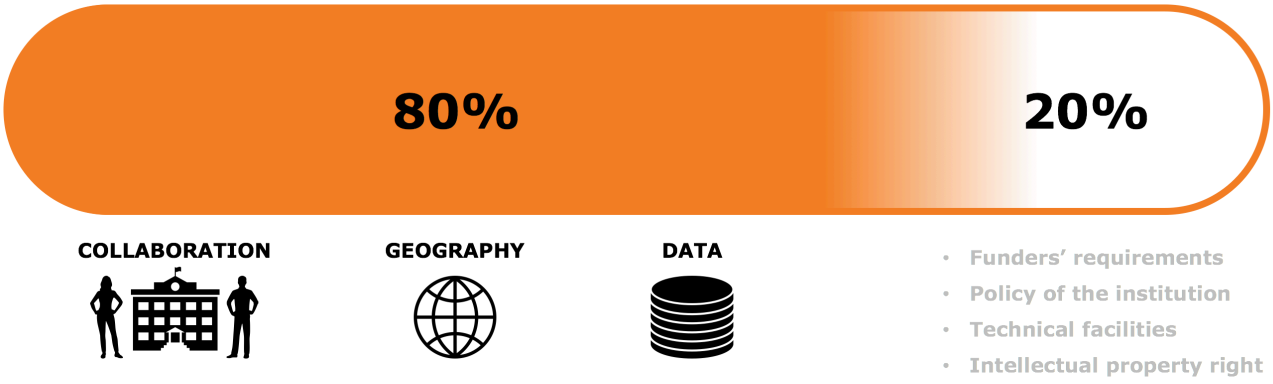
But how do you achieve the 100% insight? In practice, it appears that approx. 80% of the technical and organisational measures that you have to take can be derived from three aspects:

1. The type of **collaboration** involved in the study. Public, public-public or public-private?

2. **Geography**: The countries that participate in the study. Only countries in the EU, countries outside of the EU and the United States in particular?

3. The type of **data** you use in the study. Do you create e new data set, do you use a publicly accessible data set, a private data set or a combination of data sets?

As soon as the privacy expert in your organisation knows these three aspects, the questions in the DPIA can be completed for approx. 80%. The other 20% result from the specific context in which you conduct the research. For instance, the available technical facilities, the requirements of a possible funder etc.:



80%

20%

COLLABORATION

GEOGRAPHY

DATA

- Funders' requirements
- Policy of the institution
- Technical facilities
- Intellectual property right

By performing a DPIA more frequently, you will become familiar with the fixed measures based on the three aspects of collaboration, geography and data. In this chapter we briefly go through these three aspects.

Collaboration

The way in which you collaborate with other parties in your study may have consequences for the measures you have to take in the GDPR. For instance, entering into contracts governing access to certain data. The privacy expert in your organisation can tell you the exact measures based on your situation.

Three scenarios

Broadly, three scenarios can be distinguished in relation to collaboration:

Within the institution
1
Public – public
2
Public – private
3

1. Within the institution. You are conducting the research in the actual institution. Any data will only be available to employees of this institution. This scenario requires the least drastic measures.

2. Public - public. You are conducting the study in collaboration with another public institution, such as another university or university of applied sciences. In this scenario you have to make arrangements about who has access to which data and when, and coordination is required regarding the technologies to be used for the storage and analysis of the data among other things.

3. Public - private. This scenario entails the most drastic measures. You are collaborating with a private institution, which may have other (commercial) interests in the data apart from the study. This collaboration is also very well possible within the GDPR, but requires contractual arrangements about data handling in every research phase.

Be aware that in virtually every study you 'collaborate' with others. Even in the first scenario you may share data with parties outside of the institution anyway, without it involving a formal collaboration!

Actions

The specification of the measures you have to take in your study comprises three steps:

1. DPIA. Together with the privacy expert in your institution you perform a DPIA to identify possible risks.

2. Arrangements. Subsequently (in any case in scenarios 2 and 3) contractual agreements are required about access to (parts of) the data, the technology you will use, the location of the servers etc. These agreements are made in collaboration with legal and IT experts in your organisation.

3. Registration and verification. To be fully 'GDPR compliant' in your work, you will have to draw up a process for the registration of all data and the verification of the contractual agreements. This is also done in collaboration with the necessary experts in your organisation. If you do not know who they are, ask the IT department, the lawyer of the institution and/or the planning and control department.

Geography

Also, the geographical delineation of your study has consequences for the measures you have to take. Not only the countries that are involved in the study, but for instance also the countries where servers are located storing the data of your study. The privacy expert in your organisation can tell you the exact measures based on your situation.

Three scenarios

Broadly, three scenarios can be distinguished regarding geography:

1. Within the institution. You are conducting the research in the actual institution. Any data will only be available to employees of this institution. This scenario requires the least drastic measures.

2. Within the EU. You are conducting the study in collaboration with organisations in the EU, which may be both public and private organisations. In this scenario you will have to make arrangements about access to data and coordination will be required regarding the technologies to be used for data storage and analysis among others.

3. Outside the EU. This scenario entails the most drastic measures. You are collaborating with organisations outside the EU, where other agreements regarding the handling of personal data apply. This collaboration is also very well possible within the GDPR, but requires contractual agreements about data handling in every research phase.

Actions

The specification of the measures you have to take in your study based on the scenario that is relevant to you is comparable with the steps in the 'collaboration scenarios'. By performing a DPIA you will get insight in the measures to be taken.

Data

If you do not use personal data in your study, the GDPR does not apply. If (part of) your data does consist of personal data, you have to take measures. The type of data you use shall determine the kind of measures. The privacy expert in your organisation can tell you the exact measures based on your situation.

Three scenarios

Broadly, three scenarios can be distinguished with regard to the type of data in research:

1. Automatically generated. This includes data originating from sources that make data available continuously, such as Wi-Fi networks, fitness watches, smart electricity meters etc. The communication of and access to these large volumes of automated data must be suitably secured (encryption, storage, https).

2. Own creation. This includes data originated through the efforts of the researcher, for instance: interviews, recordings, photographs taken etc. This often involves multiple data collection moments. Each moment and each process must be well considered with regard to security.

3. Re-use. This includes mostly multiple existing data sets that are linked together, or that are enriched by the researcher's own data. Linking data sets may lead data to individuals. To prevent this, you have to ensure that access to the data is properly secured and that you immediately start using pseudonyms wherever possible.

Special personal data

A special category of personal data is the special personal data. These are data that refer directly to a certain person, such as DNA, photographs and video recordings, biometrical data etc. It often concerns data that can not or not easily be anonymised. For instance, in an interview you can leave out the name of the interviewee, so that the text is not traceable, but with DNA this is not possible.

If you are working with this type of data, you will have to take additional measures.

Actions

The specification of the measures you have to take in your study based on the scenario that is relevant to you is comparable with the steps in the 'collaboration scenarios'. Performing a DPIA will give you insight in the measures to be taken.

Congratulations!

You have reached the end of this online module on 'Privacy in research'! We hope it has given you a good idea of the sections in the GDPR and the role the GDPR plays in your study.

If you have questions or comments after this online module, we would love to hear from you. Please contact the privacy expert in your organisation or contact Cybersave Yourself via **info@cybersaveyourself.nl**.

Other/Dutch modules

SURF also offers e-learning courses about privacy for various other target groups. On this page you will find an overview of all Dutch and English modules in the series.

Ook voor diverse andere doelgroepen biedt SURF een e-learning over privacy aan. Op deze pagina vind je een overzicht van alle Nederlands- en Engelstalige modules in de reeks.

English e-learning modules:

Privacy in Research
target group: English speaking researchers in research and education in The Netherlands
duration: approx. 45 minutes

Privacy in Research Light
target group: English speaking researchers in research and education in The Netherlands
duration: approx. 20 minutes

Privacy in Education
target group: English speaking teachers in research and education in The Netherlands
duration: approx. 45 minutes

Nederlandstalige e-learning modules:

Privacy in Onderzoek
doelgroep: onderzoekers in onderwijs en onderzoek in Nederland
duur: ca. 45 minuten

Privacy in Onderzoek Light
doelgroep: onderzoekers in onderwijs en onderzoek in Nederland
duur: ca. 20 minuten

Privacy in Onderwijs
doelgroep: docenten in onderwijs en onderzoek in Nederland
duur: ca. 45 minuten

Privacy voor Onderwijsondersteuners
doelgroep: onderwijsondersteuners werkzaam op onderwijsinstellingen in Nederland
duur: ca. 30 minuten

Over dit lesmateriaal

Colofon

Auteurs	Sander van Acht
Team	SURF Privacy Awareness
Laatst gewijzigd	4 februari 2019 om 13:06
Licentie	De Internationale Creative Commons 4.0 licentie waarbij de gebruiker het werk mag kopiëren, verspreiden en doorgeven en afgeleide werken mag maken onder de voorwaarde: Naamsvermelding, zie http://creativecommons.org/licenses/by/4.0/. Meer informatie over de CC Naamsvermelding 4.0 Internationale licentie licentie.

Aanvullende informatie over dit lesmateriaal

Van dit lesmateriaal is de volgende aanvullende informatie beschikbaar:

Eindgebruiker	leerling/student

Gebruikte Wikiwijs Arrangementen

Privacy in Onderzoek (2018)

Link:	https://maken.wikiwijs.nl/117199/