

Personal data – a guide for assessing if your data can be shared with RoDL

1 Introduction

RoDL is short for Road Data Lab. RoDL is run by RISE, Lindholmen Science Park, Zenseact, Stiftelsen Chalmers industriteknik och Lund universitet. The purpose of the data lab is to collect and make available data related to roads to support open innovation and improve traffic safety. To achieve this goal, different stakeholders need to share their data with RoDL. Some of this data will contain personal data.

General Data Protection regulation¹ (GDPR) regulates how you can use personal data. This short PM is intended to be used as a check list for you who work with personal data and is thinking about exporting data to RoDL. Go through the checklist and think about the different questions. Some questions are more important than others and they are highlighted. After completing the check list, you are well prepared for a first meeting with the data protection officer and have more knowledge about if it is possible to share data with RoDL.

2 General questions

2.1 Does your data contain personal information?

Personal data means any information relating to an identified or identifiable natural living person (data subject). An identifiable natural person is one who can be identified, directly or indirectly. Example of personal data can be photos where individuals are identifiable, license plates of cars (if linked to a natural car owner), location data, behaviour etc.

2.2 Does your data contain sensitive personal data?

Sensitive personal data is data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Example of sensitive data is filming a person going into a church or a hospital.

It is appropriate to consult with a data protection officer regarding this matter!

2.3 Does your personal data contain information about a crime?

Do you collect data about a person's crime i.e., speeding?

It is appropriate to consult with a data protection officer regarding this matter!

2.4 Do you intend to use pseudonymization and does a copy exist somewhere?

Is it possible and relevant to pseudonymize the data? Pseudonymisation is the processing of personal data in such a way that it is not possible to attribute them to a specific person without the use of additional information. The additional information is kept separately and is secured through organizational or technical measure. This is still personal data.

¹ Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data.

It is appropriate to consult with a data protection officer regarding this matter!

2.5 What is not personal data?

Data that has not originally related to an identified or identifiable natural person i.e., solar storm.

Is it possible and relevant to anonymize the data? Data which were initially personal data but were later made anonymous is not personal data. But how will you make sure that your anonymized data do not again turn into personal data?

It is appropriate to consult with a data protection officer regarding this matter!

2.6 What is your purpose?

Purpose is very important, and you need to think it through. The purpose cannot be too open i.e., my purpose is to do research (not good enough). You must make your purpose much more detailed i.e., my purpose is to do research about traffic safety in order to save lives (good enough).

Can you justify your purpose (ethics etc)?

Very important, remember you can't change the purpose later on. For example, you collect personal data for the purpose of traffic safety and then you realise two years later that your data could be used for traffic planning. If traffic planning is not one of your original purpose you can't do it. Again – you must think of all kinds of possible purpose before you start collecting data.

Very important – if you export/import personal data the purpose must be the same through the whole chain. RoDL is about traffic safety research. If you don't have research as a purpose when you are collecting your data, you can't export the data to RoDL.

It is appropriate to consult with a data protection officer regarding this matter!

2.7 Data processing of personal data – every second counts

Note what every processing of personal data counts (collect, save, delete, copy etc). Even if it is just for one micro second.

2.8 How will you protect your data (technic and organisation)?

You need to protect your data i.e., fire, misuse, hackers. You must work with technical safety (i.e., firewalls) but also safety within your organisation (i.e., who can access the data).

What levels of security do you need?

Who will you share your personal data with?

It is appropriate to consult with a data protection officer regarding this matter.

2.9 Who will be personal data controller?

Personal data controller is responsible for the processing of personal data. This is normally a company and not a natural person. Personal data controller decides the purpose and how to protect the data technical and organisation. If somethings go wrong – personal data controller has to pay penalty fee.

2.10 Will you use personal data assistant?

This is a subcontractor and your agreement with the subcontractor must handle how to deal with your personal data.

2.11 Who is data protection officer?

Personal data controller decides who will be data protection officer.

2.12 Who will you share the personal data with?

You must know if you share the personal data with a 3rd party.

2.13 For how long time do you need the data?

For how long time can you justify that you need the data? If you don't need the data anymore you must delete it.

2.14 How much personal data do you intend to work with?

Less is more. You can't collect everything. Instead, you need to justify the amount of data you collect.

2.15 Where is your server located?

You can only store personal data within EU/EES (with a few exceptions). Do you know where your data is stored?

If you don't know where your server is located, it is appropriate to consult with a data protection officer regarding this matter.

2.16 Can you work with consent?

You need to have a legal ground to work with personal data. One legal ground is consent. Can you ask a person if it is okay to collect his/her personal data? This is the best legal ground if you can use it. But sometimes it is impossible to work with consent i.e., an autonomous vehicle films persons on the streets. You can't stop the car and ask every person if it is okay to take photos of them.

If you are collecting data in an employment relationship, is it appropriate to consult with a data protection officer regarding this matter! It is tricky to work with consent and employees.

2.17 Can you work with agreement?

You need to have a legal ground to work with personal data. One legal ground is agreement between you and the person i.e., to send a bill to someone you need his/her personal data. But again, sometimes it is impossible to ask people about entering into an agreement.

2.18 Can you work with legitimate interest?

You need to have a legal ground to work with personal data. One legal ground is legitimate interest (balancing of interest). If you can't use any other legal grounds this is your last resort (but agencies can't use this legal ground).

To use this legal ground, you must think of the principle of proportionality. Think of a scale. Is your interest of collecting personal data more important compared to a person's right to privacy?

It is appropriate to consult with a data protection officer regarding this matter.

2.19 How will you work with quality of your data?

Personal data must be correct, and you must be able to correct the personal data if it is wrong. Can you update your data?

2.20 Is your data searchable?

The person, what you have collected personal data about, has certain rights. How will you live up to whose rights? Data subjects can i.e., ask for the data to be erased, to be corrected, to have access

Your data could for example be searchable through time and geolocation.

2.21 Can you deliver a portable copy of the data?

Data subjects have the right to request a portable copy of the data collected.

3 Next step

When you have finished this checklist, it is time to book a meeting with your data protection officer to discuss your conclusions. The data protection officer may suggest that you do a Data Protection Impact Assessment (DPIA). DPIA describes a process designed to identify risk arising out of the processing of personal data and to minimize these risk. DPIA demonstrates to authorities that your organization complies with GDPR. The DPIA must be done before beginning any data processing activity.

4 Do you need to know more?

Here are some useful links.

A short article that explains GDPR in Swedish:

[Sjyst data - Vägledning 2019-2.pdf](#)

Ledendal. J. *Vägledning om dataskydd. God integritet vid digital tjänste- och affärsutveckling* (revision 2019:2)

Integritetsskyddsmyndigheten has lots of information on their homepage:

[Lagar och regler - Integritetsskyddsmyndigheten \(imy.se\)](#)