Data Management
Personal Data and GDPR

Dr Emma Murphy

OLLSCOIL TEICNEOLAÍOCHTA
BHAILE ÁTHA CLIATH
DUBLIN
TECHNOLOGICAL
UNIVERSITY DUBLIN

Recap

- Ethical Theories
- Data Lifecycle
- Data Management Strategies
- Data Governance
- History of Data Protection

Overview

Data Protection and Privacy

- History of data privacy
- GDPR
- ePR

Personal Data

Handling personal data – controllers and processers

So what is personal data?

- According to GDPR:
- ‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’).
- “An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”

Personal Data - Context

- That's a lot of information! In certain circumstances, someone's IP address, hair colour, job or political opinions could be considered personal data.
- "The qualifier 'certain circumstances' is worth highlighting, because whether information is considered personal data often comes down to the context in which data is collected."

https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data

Personal data - Context

- Organisations usually collect many different types of information on people, and even if one piece of data doesn't individuate someone, it could become relevant alongside other data.
- For example, an organisation that collects information on people who download products from their website might ask them to state their occupation.
- This doesn't fall under the GDPR's scope of personal data, because, in all likelihood, a job title isn't unique to one person. Similarly, an organisation might ask what company they work for, which, again, couldn't be used to identify someone unless they were the only employee.

https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-

Personal data - Context

- However, in many instances these pieces of information could be used together to narrow down the number of people to such an extent that you could reasonably establish someone's identity.
- In other words, if you refer to someone with a specific job title at a specific organisation, there may only be one person who fits that description.
- Of course, that's not always the case. Knowing that someone is a barista at Starbucks doesn't narrow things down much, for example.
- In these cases, those two pieces of information together wouldn't be considered personal data. However, it's highly unlikely that this information would be stored without a specific identifier, such as the person's name or payroll number.

https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data

Personal data - Context

- You might think that someone's name is as clear an example of personal data as it gets; it is literally what defines you as *you*. But it's not always that simple, as the UK's Information Commissioner's Office explains:
- "By itself the name John Smith may not always be personal data because there are many individuals with that name.
- "However, where the name is combined with other information (such as an address, a place of work, or a telephone number) this will usually be sufficient to clearly identify one individual."

https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data

Personal data - Names

- However, the ICO also notes that names aren't necessarily required to identify someone:
- "Simply because you do not know the name of an individual does not mean you cannot identify [them]. Many of us do not know the names of all our neighbours, but we are still able to identify them."
-

https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data

Personal Data - Identifiers

- An individual is 'identified' or 'identifiable' if you can distinguish them from other individuals.
- A name is perhaps the most common means of identifying someone. However whether any potential identifier actually identifies an individual depends on the context.
- A combination of identifiers may be needed to identify an individual.
- The GDPR provides a non-exhaustive list of identifiers, including:
    - name;
    - identification number;
    - location data; and
    - an online identifier. ('Online identifiers' includes IP addresses and cookie identifiers which may be personal data.)
- .

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

Personal data

- In most circumstances, it will be relatively straightforward to determine whether the information you process ‘relates to’ an ‘identified’ or an ‘identifiable’ individual. In others, it may be less clear and you will need to carefully consider the information you hold to determine whether it is personal data and whether the GDPR applies.

Special categories of PD

- Race;
- ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where this is used for identification purposes);
- health data;
- sex life; or
- sexual orientation.
- Personal data can include information relating to criminal convictions and offences. This also requires a higher level of protection.

Sensitive Personal Data

- Sensitive personal data should be held separately from other personal data, preferably in a locked drawer or filing cabinet.
- As with personal data generally, it should only be kept on laptops or portable devices if the file has been encrypted and/or pseudonymised.

Pseudonymisation

- Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual.
- The GDPR defines pseudonymisation as:
- "…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 is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

Pseudonymisation

- Pseudonymisation may involve replacing names or other identifiers which are easily attributed to individuals with, for example, a reference number.
- Whilst you can tie that reference number back to the individual if you have access to the relevant information, you put technical and organisational measures in place to ensure that this additional information is held separately.

Pseudonymisation

- Pseudonymising personal data can reduce the risks to the data subjects and help you meet your data protection obligations.
- However, pseudonymisation is effectively only a security measure. It does not change the status of the data as personal data. GDPR makes it clear that pseudonymised personal data remains personal data:
- "…Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person…"

Anonymisation

- The GDPR does not apply to personal data that has been anonymised. :
- "…The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/#pd1

Anonymisation

- This means that personal data that has been anonymised is not subject to the GDPR. Anonymisation can therefore be a method of limiting your risk and a benefit to data subjects too. Anonymising data wherever possible is therefore encouraged.
- However, you should exercise caution when attempting to anonymise personal data. Organisations frequently refer to personal data sets as having been 'anonymised' when, in fact, this is not the case. You should therefore ensure that any treatments or approaches you take truly anonymise personal data. There is a clear risk that you may disregard the terms of the GDPR in the mistaken belief that you are not processing personal data.

Anonymisation

- In order to be truly anonymised under the GDPR, you must strip personal data of sufficient elements that mean the individual can no longer be identified.
- However, if you could at any point use any reasonably available means to re-identify the individuals to which the data refers, that data will not have been effectively anonymised but will have merely been pseudonymised. This means that despite your attempt at anonymisation you will continue to be processing personal data.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Question….

- For your Masters thesis you want to interview 20 people to elicit user requirements for a piece of software that you are designing
- In addition to your interview questions you will record some important demographic information that will be useful for your analysis and contact details so that you can get in touch with them again.
- You want to record their name, address, date of birth, gender, occupation, education experience, number of devices that they own
- Thinking of data privacy and data protection how are you going to manage this data?

Lawful bases for processing personal information

- (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose
- (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- (d) Vital interests: the processing is necessary to protect someone's life.
- (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

What are the lawful bases for processing?

- (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose
- (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- (d) Vital interests: the processing is necessary to protect someone's life.
- (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

GDPR - Subject Access

- Individuals have the right to access their personal data.
- This is commonly referred to as subject access.
- Individuals can make a subject access request verbally or in writing.
- Organisations have one month to respond to a request.
- Organisations cannot charge a fee to deal with a request in most circumstances.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

GDPR – Subject Access

Individuals have the right to obtain the following from you:

- confirmation that you are processing their personal data;
- a copy of their personal data; and
- other supplementary information – this largely corresponds to the information that you should provide in a privacy notice

Subject Access – Other Information

In addition to a copy of their personal data, you also have to provide individuals with the following information:

- the purposes of your processing;
- the categories of personal data concerned;
- the recipients or categories of recipient you disclose the personal data to;
- your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with a data supervisory authority (i.e. Data Protection Commission);
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards you provide if you transfer personal data to a third country or international organisation.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

Controllers and Processors

- Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data.
- If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes.
- Processors act on behalf of, and only on the instructions of, the relevant controller.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Who is the controller?

- To determine whether you are a controller or processor, you will need to consider your role and responsibilities in relation to your data processing activities.
- If you exercise overall control of the purpose and means of the processing of personal data – ie, you decide what data to process and why – you are a controller.
- If you don't have any purpose of your own for processing the data and you only act on a client's instructions, you are likely to be a processor – even if you make some technical decisions about how you process the data.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Roles

- Controllers shoulder the highest level of compliance responsibility – you must comply with, and demonstrate compliance with, all the data protection principles as well as the other GDPR requirements. You are also responsible for the compliance of your processor(s).
- Processors do not have the same obligations as controllers under the GDPR and do not have to pay a data protection fee. However, if you are a processor, you do have a number of direct obligations of your own under the GDPR.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Checklists

- The following checklists set out indicators as to whether you are a controller, a processor or a joint controller. The more boxes you tick, the more likely you are to fall within the relevant category.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

Are we a controller?

□ We decided to collect or process the personal data.

□ We decided what the purpose or outcome of the processing was to be.

□ We decided what personal data should be collected.

□ We decided which individuals to collect personal data about.

□ We obtain a commercial gain or other benefit from the processing, except for any payment for services from another controller.

□ We are processing the personal data as a result of a contract between us and the data subject.

□ The data subjects are our employees.

□ We make decisions about the individuals concerned as part of or as a result of the processing.

□ We exercise professional judgement in the processing of the personal data.

□ We have a direct relationship with the data subjects.

□ We have complete autonomy as to how the personal data is processed.

□ We have appointed the processors to process the personal data on our behalf.

https://ico.org.uk/

Are we a joint controller?

- □ We have a common objective with others regarding the processing.
- □ We are processing the personal data for the same purpose as another controller.
- □ We are using the same set of personal data (eg one database) for this processing as another controller.
- □ We have designed this process with another controller.
- □ We have common information management rules with another controller.

https://ico.org.uk/

Are we a processor?

□ We are following instructions from someone else regarding the processing of personal data.

□ We were given the personal data by a customer or similar third party, or told what data to collect.

□ We do not decide to collect personal data from individuals.

□ We do not decide what personal data should be collected from individuals.

□ We do not decide the lawful basis for the use of that data.

□ We do not decide what purpose or purposes the data will be used for.

□ We do not decide whether to disclose the data, or to whom.

□ We do not decide how long to retain the data.

□ We may make some decisions on how data is processed, but implement these decisions under a contract with someone else.

□ We are not interested in the end result of the processing.

https://ico.org.uk/

Ethics of data handling and privacy

- Impact on people: Because data represents characteristics of individuals and is used to make decisions that affect people's lives, there is an imperative to manage its quality and reliability.
- Potential for misuse: Misusing data can negatively affect people and organizations, so there is an ethical imperative to prevent the misuse of data.
- Economic value of data: Data has economic value. Ethics of data ownership should determine how that value can be accessed and by whom.

(DAMA, 2017)

References

DAMA International (2017) DAMA DMBOK, DAMA DMBOK – Data Management Body of Knowledge, Technics Publications, New Jersey, pp 381–85

O'Keefe, K. and O'Brien, D. (2018) Ethical Data and Information Management: Concepts, Tools and Methods (1st. ed.). Kogan Page Ltd., GBR.

Hasselbach, G and Tranberg, P (2017) Data Ethics: The new competitive advantage, PubliShare, Copenhagen.

OECD (2011) Thirty Years After: The OECD Privacy Guidelines. Available: http://www.oecd.org/sti/ieconomy/49710223.pdf