Data Management
Data Protection and Data Privacy

Dr Emma Murphy

OLLSCOIL TEICNEOLAÍOCHTA
BHAILE ÁTHA CLIATH
TU DUBLIN
TECHNOLOGICAL
UNIVERSITY DUBLIN

Recap

- Ethical Theories
- Data Lifecycle
- Data Management Strategies
- Data Governance

Overview

Data Protection and Privacy

- History of data privacy
- GDPR
- ePR

Personal Data

Handling personal data – controllers and processers

Data Protection vs Data Privacy

- “Data protection is focused on protecting assets from unauthorized use, while data privacy defines who has authorized access. One can say that data protection is mostly a technical control, while data privacy is more of a process or legal matter. One doesn’t ensure the other, and we need both to work together as a proper control mechanism”- Sameer Shelke, aujas.com

https://www.forbes.com/sites/forbestechcouncil/2018/12/19/data-privacy-vs-data-protection-understanding-the-distinction-in-defending-your-data/#3edce80150c9

Data Protection vs Data Privacy

- “The important distinction people should know about data privacy and data protection is who controls which part. Data privacy controls are mostly given to users. Users can usually control which data is shared with whom. Data protection is mostly a company’s responsibility. Companies basically need to make sure that the level of privacy their users have set is implemented and data is protected”. - Vikram Joshi, pulsd

https://www.forbes.com/sites/forbestechcouncil/2018/12/19/data-privacy-vs-data-protection-understanding-the-distinction-in-defending-your-data/#3edce80150c9

Data Privacy

- Privacy law is not new. Privacy and information privacy as concepts are firmly linked to the ethical imperative to respect human rights.

(DAMA, 2017)

Data Privacy history US

- In 1890, American legal scholars Samuel Warren and Louis Brandeis described privacy and information privacy as human rights with protections in common law that underpin several rights in the US constitution.
- In 1973, a code of Fair Information Practice was proposed, and the concept of information privacy as a fundamental right was reaffirmed in the US Privacy Act of 1974, which states that “the right to privacy is a personal and fundamental right protected by the Constitution of the United States”.

(DAMA, 2017)

European Convention of Human Rights

- In the wake of human rights violations during the Second World War, the European Convention of Human Rights (1950) established both the general right to privacy and the specific right to information privacy (or the right to protection of one's personal data) as human rights which are fundamental to upholding the right to Human Dignity

Computers and data

- Privacy became an issue in the late 1960s because of the convergence of two trends: the post-industrial information revolution and the growing government use of personal data.
- The advantages of using computers to more efficiently process data were increasingly apparent yet at the same time so too were growing concerns about the possible loss of dignity or the erosion of rights that could result from the misuse of personal data.
- There was recognition too of the growing awareness in certain circles of the need to empower citizens in claiming their rights. Governments in many OECD member states responded to these concerns by creating task forces, commissions and committees to study the issue.

(OECD, 2011)

OECD expert group

- In 1977an Expert Group was formed by the OECD chaired by Honourable Justice Michael Kirby of Australia, was created to begin work on guidelines.
- [The Organisation for Economic Co-operation and Development (OECD); is an intergovernmental economic organisation with 36 member countries, founded in 1961 to stimulate economic progress and world trade.]

(OECD, 2011)

OECD Data expert group

- The creation of the 1977 Expert Group and the decision to work on guidelines were in response to the concerns that had surfaced over the previous decade about the growing use of personal data and the increasing reliance on computerised processing that prompted several countries to pass legislation.
- Given its mandate to foster economic growth and contribute to the expansion of world trade, the OECD was also concerned about the possibility that national laws would create barriers to the free flow of information that would impede growth.

(OECD, 2011)

OECD

- In 1980, the Organization for Economic Co-operation and Development (OECD) established Guidelines and Principles for Fair Information Processing that became the basis for the European Union's data protection laws.

(OECD, 2011)

OECD Fair Information Processing Standards

- OECD's eight core principles, the Fair Information Processing Standards, are intended to ensure that personal data is processed in a manner that respects individuals' right to privacy.

(OECD, 2011)

OECD Principles (1980)

- Although there was a broad consensus about the OECD principles and the need to take action, reaching agreement was not easy.
- One of the key challenges facing the Expert Group is described in the Explanatory Memorandum:
- "…*there is an inherent conflict between the protection and the free transborder flow of personal data. Emphasis may be placed on one or the other, and interests in privacy protection may be difficult to distinguish from other interests relating to trade, culture, national sovereignty, and so forth.*" (OECD, 2011)

OECD Principles (1980)

- Collection Limitation Principle There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- Data Quality Principle Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

(OECD, 2011)

OECD Principles (1980)

- Purpose Specification Principle The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- Use Limitation Principle Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [those above] except: a) with the consent of the data subject; or b) by the authority of law.

(OECD, 2011)

OECD Principles (1980)

- Security Safeguards Principle Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
- Openness Principle There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

OECD Principles (1980)

- Individual Participation Principle An individual should have the right:
- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him
- c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
- Accountability Principle A data controller should be accountable for complying with measures which give effect to the principles stated above

Irish Legislation

Data Protection Act 1988:

…. to regulate in accordance with its provisions the collection, processing, keeping, use and disclosure of certain information relating to individuals that is processed automatically. [13th July, 1988]

which led to the establishment of the Office of the Data Protection Commissioner (ODPC) in 1989.

http://www.dataprotection.ie/docs/EU-Directive-95-46-EC/89.htm

Data Protection (Amendment) Act 2003.

- The 1995 Data Protection Directive (Directive 95/46/EC) was transposed into Irish domestic law in 2003 with the Data Protection (Amendment) Act 2003.

2003 Data Protection Act

- Among other stipulations, this Act set out eight data protection principles:
- Obtain and process the information fairly
- Keep it only for one or more specified and lawful purposes
- Process it only in ways compatible with the purpose or purposes for which it was given to you initially
- Keep it safe and secure
- Keep it accurate and up to date
- Ensure that it is adequate, relevant and not excessive
- Retain it no longer than is necessary for the specified purpose or purposes
- Upon their request, give individuals a copy of their personal data

https://www.itgovernance.eu/en-ie/data-protection-ie

2003 Data Protection Act

- Organisations found to be in breach of the DPA 2003 could be fined up to €100,000 by the ODPC.
- The Data Protection Directive 1995 and all local laws derived from it, including the Act of 2003, have now been superseded by the GDPR.

2018 GDPR

- Originally proposed by the European Commission in January 2012, the GDPR (Regulation (EU) 2016/679) was adopted by the European Parliament in April 2016 and published in the Official Journal of the European Union on 4 May 2016. Following a two-year transition period, it was enforced in all 28 EU member states on 25 May 2018.

https://www.itgovernance.eu/en-ie/data-protection-ie

2018 Data Protection Act

- In Ireland, a new Data Protection Act was also enacted in May 2018 to supplement the GDPR by filling in sections of the Regulation that are left to individual member states to interpret and implement, and applying its provisions – or at least a "broadly similar regime" – to certain areas outside the GDPR's scope.

GDPR SCOPE

- Under the GDPR, data subjects have the right to lodge a complaint with the supervisory authority, the DPC (Data Protection Commission (formerly the ODPC)), if they consider that the processing of their personal data infringes the Regulation, and the right to an effective judicial remedy against data controllers and processors if they consider their rights to have been infringed by processing that does not comply with the Regulation.

GDPR SCOPE

- On top of this, the DPC has the power to "impose a temporary or definitive limitation including a ban on processing" – in other words, effectively shut organisations down altogether.
- Both the GDPR and the DPA 2018 are backed by a regime of considerably higher penalties than the Data Protection Acts of 1998 and 2003, with administrative fines of up to €20 million or 4% of global annual turnover – whichever is greater.

OECD Principles to GDPR

GDPR Principle	Description of Principle
Fairness, Lawfulness, Transparency	Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
Purpose Limitation	Personal data must be collected for specified, explicit, and legitimate purposes, and not processed in a manner that is incompatible with those purposes.
Data Minimization	Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
Accuracy	Personal data must be accurate, and where necessary, kept up-to-date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay.
Storage Limitation	Data must be kept in a form that permits identification of data subjects [individuals] for no longer than is necessary for the purposes for which the personal data are processed.
Integrity and Confidentiality	Data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.
Accountability	Data Controllers shall be responsible for, and be able to demonstrate compliance with [these principles].

GDPR principles

- These principles are balanced by and support certain qualified rights individuals have to their data, including the rights to access, rectification of inaccurate data, portability, the right to object to processing of personal data that may cause damage or distress, and erasure.

(DAMA, 2017)

Data privacy in the EU

- Broadly speaking, data privacy in the EU is covered under the General Data Protection Regulation and but there are also the ePrivacy Regulations.

ePrivacy Regulations

- The Irish ePrivacy Regulations 2011, derived from the EU ePrivacy Directive 2002/58/EC deals with data protection for phone, email, SMS and Internet usage (the 'cookies law').
- The 2011 Regulations set out the rules on electronic communications, including marketing emails, faxes, texts and phone calls; the use of cookies that track website visitors' information; the security of public electronic communications services; and the privacy of end users. If you market by phone, email, text or fax, use cookies or compile public directories, you must comply with the Irish ePrivacy Regulations 2011.

https://www.itgovernance.eu/en-ie/data-protection-ie

ePR

- In January 2017, the European Commission proposed a new Regulation on Privacy and Electronic Communications (ePR) as part of its digital single market strategy.
- The ePR will replace the 2002 ePrivacy Directive (the 'cookies law') and all member state laws that implemented it – including Ireland's ePrivacy Regulations 2011.

https://www.itgovernance.eu/en-ie/eprivacy-regulation-epr-ie

ePR

- While the current ePrivacy Regulations only apply to traditional telecoms providers, the ePR is broader in scope, and aims to ensure stronger privacy in all electronic communications – including over-the-top (OTT) service providers such as instant messaging apps and Voice over Internet Protocol (VoIP) platforms, and machine-to-machine communications such as the Internet of Things (IoT). The ePR also extends to inter personal communication services that are ancillary to another service.

ePR

- The ePR has the same territorial scope as the EU's General Data Protection Regulation (GDPR), carries an identical penalty regime for non-compliance and it was intended to come into effect on 25 May 2018.

ePR Timeline

- However, the Council of the European Union is yet to confirm its position so the Regulation's final text is far from being agreed.
- With further delays caused by the 2019 EU elections, and the latest draft specifying a 24-month transition period, the ePrivacy Regulation might not take effect until 2022 at the earliest.

ePR and GDPR

- The GDPR – and the new Irish Data Protection Act 2018 – apply to the processing of personal information.
- The ePR has been designed to complement the GDPR by providing specific rules regarding the protection of the fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services.

GDPR vs ePR

- Each regulation was drawn up to reflect a different segment of EU law. The GDPR was created to enshrine Article 8 of the European Charter of Human Rights in terms of protecting personal data, while the ePrivacy regulation was created to enshrine Article 7 of the charter in respect to a person's private life.
- The private sphere of the end user is covered under the ePrivacy regulations, making it a requirement for a user's privacy to be protected at every stage of every online interaction.

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.

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?

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.)

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