Ethics and Data Governance

Dr Emma Murphy

OLLSCOIL TEICNEOLAÍOCHTA
BHAILE ÁTHA CLIATH
DUBLIN
TECHNOLOGICAL
UNIVERSITY DUBLIN

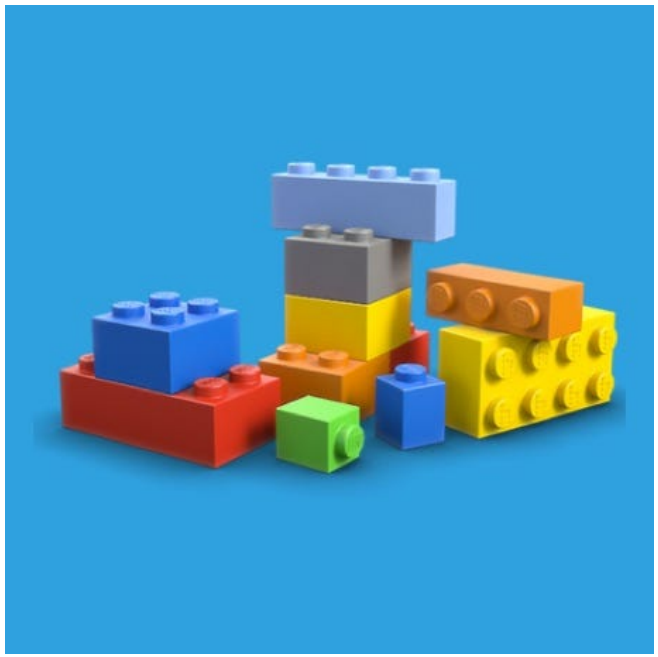
Ethics and Data Governance

- An ethically based framework for data governance decisions, particularly in scenarios where codified standards or laws lag behind the technological capabilities available, supports a wider ethics-based approach to information management as it enables and coordinates the definition and communication of ethical values in setting and enforcing data-related policies, standards and processes.
- It will ensure a clear escalation and remediation path to raise any ethical issues regarding data access, quality, ownership, standards, security, usage and management.

(O'Keefe and O'Brien, 2018)

Case study - Apple

Case Studies - Lego



Towards ethical principles for DG

- Looking at these two case studies, and considering the various ethical frameworks we have considered we can start to formulate some candidate ethical principles for data governance

(O'Keefe and O'Brien, 2018)

Ethical principles for DG

Ethical Principle	Description
People are an end in and of themselves, not a means to an end	The processing of data about people in the organization is done in a way that respects them and their privacy
The arbiter of our ethics is the customer, through the outcomes they experience	The information and process outcomes that our stakeholders experience, and the degree to which those experiences match expectations, is the benchmark for our ethical standards
The customer owns their data. We use it on trust	Data that is obtained from or about our customers is their data. We use it on trust and must ensure we are transparent and truthful about what we will do with that information
The only mode of expression for ethics is action	It is not enough to talk about information ethics, we must design our information handling processes in an ethical manner, and design ethics in
The processing of data should be designed to serve mankind	We need to design our processes for acquiring, analysing and using data in a way that serves mankind, delivering utility, equality and supporting dignity, while avoiding unnecessary invasion of privacy or infringement of other fundamental rights

Ethical principles for DG

First, do no harm	When engaging in any processing of information, we must aim to avoid information or process outcomes that cause harm or loss to people
Accountability follows the data life cycle	Everyone in the organization is accountable for how they obtain and use data, and have an obligation to ensure the effective stewardship of information to ensure the appropriate information and process outcomes are consistently delivered

Individual beliefs vs Organizational ethic

- The ethic of the individual represents the bundle of beliefs, perceptions and values that we each bring to the organization and constitutes the lens through which we view and interpret the ethic of the organization and the various policies, standards and guidance that might exist in relation to ensuring the consistent delivery of appropriate information and process outcomes.

(O'Keefe and O'Brien, 2018)

Individual vs. Society

- You will often see conflict between the ethic of the individual and the ethic of the organization, and even the ethic of society. This conflict needs to be managed through agreed-upon models for decision making.
- Handled well, conflicts of this kind can improve the alignment between the ethic of the organization and the ethic of society – after all, the individuals in your organization are also members of society.
- Handled badly, this may result in the development of groupthink in the organization, in which individual concerns are not given due consideration. In such cases, your organization may find itself facing whistleblowing, brand damage or other impacts.

(O'Keefe and O'Brien, 2018)

Activity

- Facebook Case study

Individual vs. Society

- The Facebook ‘fake news’ example is a good example of where the ethic of the individual can run into problems with the ethic of the organization.
- In that case, an individual engineer identified something that looked unusual in the data about content sharing. This was raised through a discussion forum.
- But in the absence of agreed-upon models and methods for escalating issues like this (such as agreed models for root cause analysis and upwards reporting for guidance or action), the signal that there was a potential problem in the news feeds was missed.

(O’Keefe and O’Brien, 2018)

Need to align ethics

- Appropriate structures and frameworks are therefore needed, and must be planned for to ensure appropriate alignment of the ethic of the individual with the ethic of the organization, and ultimately with the ethic of society
- Where the culture diffuses responsibility for actions or ethical outcomes to others, this can lead to people claiming they were ‘acting under orders’ or seeking some other entity to remedy the situation (such as Facebook staff looking to governments to regulate the ‘fake news’ issues

(O’Keefe and O’Brien, 2018)

Ethics and Stewardship

- In designing your information stewardship model for ethics, it is essential therefore that: Individuals are given a chance to engage and be involved in role taking as democratic leaders. Supports should be in place to give people a normative structure for discussing ethical issues in information management.
- Ethics should be made relevant and relatable to the immediate context of the individual's job. There should be clear mechanisms for consequences to be identified and understood, both in terms of consequences for the external stakeholders affected by actions, but also in the context of consequences within the overall governance structure of the organization.

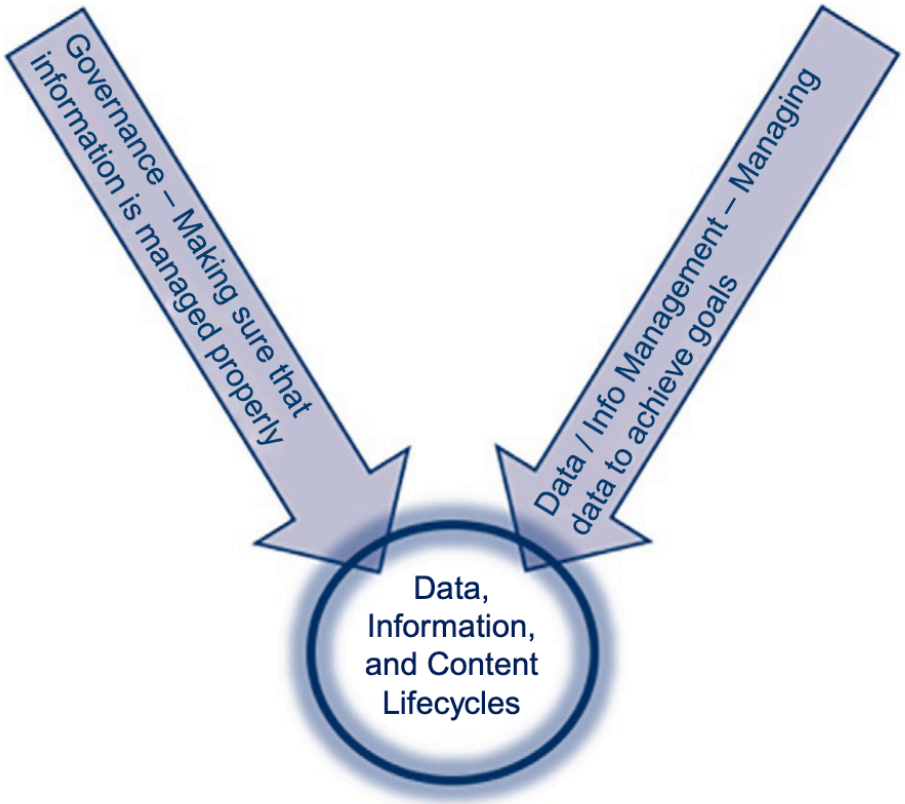
(O'Keefe and O'Brien, 2018)

Separation of Duties

- Another key aspect of effective data governance is the development of an effective separation of duties between oversight and execution in the context of information management processes.
- While generally considered an accounting concept (also auditing, quality control), segregation of duties is also a prudent risk-management concept. In the context of information management, it means that no part of the organization should be defining what 'right' is in relation to the required information and process outcomes as well as being accountable for the management of data to achieve goals.
    - EU's General Data Protection Regulation, which explicitly requires that data protection officers are independent of influence in the performance of their oversight and monitoring tasks.

(O'Keefe and O'Brien, 2018)

Governance V model



(Ladley, 2020)

Risk management and governance

- It is essential that the organization's risk management and governance approach for information and data consider the impacts on external stakeholders as a result of the information and process outcomes that are delivered.
    - an explicit feature of legislation such as the EU's General Data Protection Regulation (GDPR), which requires the risk to the data privacy of individuals and the risks to the rights and freedoms enabled by data privacy rights to be considered when conducting or designing any information-processing activity.
- This means risks to both the individual and the organization need to be considered, and formal structures and processes are required to ensure that those decisions are taken objectively and are recorded.

(O'Keefe and O'Brien, 2018)

DG – Key Factors

- You need to consider several key factors as you architect the structures for your governance model.
- Cultural norms (about data): are there potential barriers or cultural obstacles to implementing or improving governance structures and processes in the organization?
- Cultural norms (about ethics): what is the dominant ethical culture or bias in the organization? What is the ethic of the organization?

(O'Keefe and O'Brien, 2018)

DG – Key Factors

- Data governance practices: how and by whom are decisions about data made currently in your organization? What are the rules for deciding how to decide? How is work organized and executed: what is the relationship between governance and project/operational execution? What committee structures or forums are in place to manage the oversight and execution of ethical principles?
- (O'Keefe and O'Brien, 2018)

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.

Ladley, J. (2020) Data Governance. 2nd edition, 2020.

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.