Engaging Content
Engaging People

TEU0031: What's the Internet Doing to Me?

Data Protection Organisation Obligations

Dave Lewis, dave.lewis@scss.tcd.ie

Thanks to: Harsh Pandit, Kaniz Fatema

@ethicscanvas
ethicscanvas.org
hello@ethicscanvas.org

Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union
European Union
European Regional Development Fund
SFI Science Foundation Ireland

The ADAPT Centre is funded under the SFI Research Centres Programme (Grant 13/RC/2106) and is co-funded under the European Regional Development Fund.

Principles of Data Protection – Data Controllers

GDPR sets out seven key principles related to the processing of personal data,

- Lawfulness, fairness, and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality; and
- Accountability.

Controllers need to be **aware of and comply with** these principles when collecting and otherwise processing personal data:

Accountability Obligation

Organisations, and not data protection authorities, must **demonstrate** that they are compliant with the law.

Relevant measures include:

- Adequate **documentation** on what personal data is processed;
- How, to what purpose, and how long data will be processed for;
- Documented processes and procedures aiming at tackling data protection issues at an **early stage** when building information systems or **responding to a data breach**; and
- The presence of a **Data Protection Officer** (if required) who is integrated in the organisation planning and operations etc.

Make **an inventory of all personal data** you hold and examine it under the following headings:

- Why are you holding it?
- How did you obtain it?
- Why was it originally gathered?
- How long will you retain it?
- How secure is it, both in terms of encryption and accessibility?
- Do you ever share it with third parties and on what basis might you do so?

Transparency Obligations

Businesses and organisations that process personal data must **provide individuals with information** on the type of processing that is taking place and who is carrying it out.

At a minimum, this information must clearly state:

- Who you (the organisation) are.
- Why you are processing the data.
- What legal basis you rely on to legitimise the processing.
- Whether or not the data will be transferred on to other organisations or individuals.
- How long the data will be stored.
- The existence of the individual's rights under data protection, including the rights to access, correction, erasure, restriction, objection and portability.

Personal Data Breach Obligations

A **personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data

Personal data breaches can be the result of both

- **accidents** (such as sending an email to the wrong recipient) as well as
- **deliberate acts** (such as phishing attacks to gain access to customer data).

A personal data breach negatively impacts the **confidentiality, integrity, or availability** of personal data;

It means that the controller is **unable to ensure compliance** with the principles relating to the processing of personal data under GDPR.

There are two primary obligations on controllers under GDPR:

- **notification of any personal data breach to the DPC**, unless they can demonstrate it is unlikely to result in a risk to data subjects; and
- **communication of that breach to data subjects**, where the breach is likely to result in a high risk to data subjects.

Data Subject Identification

- In general terms, a natural person can be considered as **“identified”** when, within a group of persons, he or she is "distinguished" from all other members of the group.
- Accordingly, the natural person is **“identifiable”** when, although the person has not been identified yet, it is possible to do it…
- “Singling out” is when it is possible to distinguish the data relating to one individual from all other information in a dataset.
  - For example, there might be only one individual in a dataset who is 160cm tall and was born in 1990, even though there are many others who share either the height or year of birth.

Anonymisation and Pseudoanonymisation: What?

Data can be considered **“anonymised”** from a data protection perspective when data subjects are not identified or identifiable, having regard to all methods reasonably likely to be used by the data controller or any other person to identify the data subject, directly or indirectly.

Irreversibly and effectively anonymised data is not “personal data” and not subject to GDPR

If the source data is not deleted at the same time that the ‘anonymised’ data is prepared, where the source data could be used to identify an individual from the ‘anonymised’ data, the data may be considered only ‘**pseudonymised**’ and thus still ‘personal data’, therefore still subject to.

N.B. It is **not** normally possible to **quantify the likelihood of re-identification** of individuals from anonymised data

Anonymisation and Pseudoanonymisation: Why?

Anonymisation and Pseudoanonymisation can be used

1. To improve protection for data subjects.
2. As part of a risk minimisation strategy when sharing data with data processers or other data controllers.
3. To avoid inadvertent data breaches occurring when your staff is accessing personal data.
4. As part of a “data minimisation” strategy aimed at minimising the risks of a data breach for data subjects.

Data Linking

Any linking of identifiers in a data set will make it more likely that an individual is identifiable.

For example, taken individually the first and second name “John” and “Smith” might not be capable of distinguishing one of a large company’s customers from all other customers, but if the two pieces of information are linked, it is far more likely that “John Smith” will refer to a unique, identifiable individual.

Re-identification from Data Linking

A major risk factor which may lead to the identification of individuals from anonymised data is the **risk of data from one or more other sources being combined or matched** with the anonymised data.

Source of matching data

- **Public registers**, such as the Land Registry, Register of Electors, or publicly accessible registries of the members of professions.
- **Searchable information** contained on the internet or in online databases. e.g. newspaper stories, blog posts or online directories, or data published in previous data breaches.
- **Statistical data** published in an anonymised format, which might be combined with certain anonymised data to identify a data subject. This is a particular concern in the case of research or statistical publications concerning the same data subjects. Information available to the particular organisation or individual that is being given access to anonymised data, e.g Yahoo search log dataset
- **Personal knowledge**

Data minimisation and collection techniques, which are also part of the principles of data protection are helpful in reducing the risk of data matching being successful

Privacy by Design and by Default

Data Protection by design means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This will help to ensure better and more cost-effective protection for individual data privacy.

Data Protection by default means that the user service settings (e.g. no automatic opt-ins on customer account pages) must be automatically data protection friendly, and that only data which is necessary for each specific purpose of the processing should be gathered at all.

Ethics Canvas Project Title: Date:

Individuals affected- 1:
Who uses the application? Who is affected by its use? What are their gender, age etc?

Behaviour - 3:
How might people's behavior change due to the application, e.g. in habits, time-schedule, choice of activities?

Relations - 4:
How do relations between individuals and groups change, e.g. between friends, family, co-workers etc?

What can we do? 9 :
What are the most important ethical impacts and how can you mitigate these?

Worldviews - 5:
How might people's worldview be affected by the application, e.g. o consumption, religion, work etc?

Group Conflicts - 6:
How might group conflicts arise or be affected by the application. E.g. in discrimination, loss of work etc?

Groups affected – 2:
Which groups are affected by the application, e.g. work-related, interest or advocacy groups?

Product or Service Failure – 7:
What types of failures could the application experience and what would the impact of these?

Use of Resources – 8:
What resources does the application consume and what is the impact of that consumption?

Ethics Canvas v1.8 - ethicscanvas.org © ADAPT Centre
The ADAPT Centre for Digital Content Technology is funded under the SFI Research Centres Programme (Grant 13/RC/2106) and is co-funded under the European Regional Development Fund. .

Data Protection Canvas Project Title: Date:

Data Subjects- 1:
What type of people do you hold personal data on? Employees/ Customers Adults/ Children Etc?

Purpose - 3: For what purposes are data being collected?

Consent - 4: Has consent been asked for data collection or will it be asked? Is it presented clearly? Is consent revocable?

Risk Mitigation? 9 : What measures need to be put in place to reduce the risks of GDPR non-compliance?

Transparency - 5: Is there transparency in the processing and use of the data? I.e: Info notices, paper trails etc

Rights- 6: Can data subjects access their data on request? Can the data be erased? Can data subjects object to certain types of use of the data eg: direct marketing? Will data subjects be notified on a data breach?

Data Types – 2:
What type of data do you hold? Children data? Sensitive data? Biometric data(data that could identify a person)?

Storage – 7: Is there a storage time limitation? What technical measures have been taken to protect personal data from un-authorised access? What level of security is needed?

Breach – 8: What happens after a data breach? Who is notified? Do you maintain an internal breach register? Possibility of administration fines