dcm THE LEARNING EXPERTS

CPD-accredited Data Protection and EU GDPR Refresher Webinar

Kara Ovington

HELLO!

I am **Kara Ovington**

I am a Data Protection trainer since 2013.

Housekeeping

- Days, start and finish times
- Breaks
- Resources available
- Using zoom/teams

Data Protection Legislation

Key Data Protection legislative frameworks applicable from 25 May 2018

The Data Protection Commission (DPC) is governed by a number of legislative frameworks. Details of the key legislation and guidance about how the laws are applied is outlined below.

From 25 May 2018 the key legislative frameworks are:

- General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- the "Law Enforcement Directive" (Directive (EU) 2016/680) which has been transposed into Irish law by way of the Data Protection Act 2018
- the Data Protection Acts 1988 and 2003
- the 2011 "ePrivacy Regulations" (S.I. No. 336 of 2011 – the European Communities (Electronic Communications Networks and Services) (Privacy And Electronic Communications) Regulations 2011)

Learning Outcomes

By the end of this session you will be able to understand the following areas

- GDPR and data Protection holistic view
- Principles and User rights
- Special category Data
- What is processing?
- Consequences of failure

What is PII?

Personally Identifiable Information (PII)

GDPR Art.4(1) defines Personal Data as:

> *"Any information relating to an identified or identifiable natural person ("data subject"); an identifiable 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, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."*

NOTE: these are examples but NOT a definitive list

If you can identify an individual from the data held, then the data is "Personal Information" and it therefore falls within the scope of the GDPR

However, the GDPR does **NOT** apply to processing "by a natural person in the course of a purely personal or household activity" (Article 2)

Lawful Processing- standard PII

Special Category Data

Personal data relating to **criminal convictions and offences** are not included, but similar extra safeguards apply t it’s processing (see Article 10 EU-GDPR)

Lawful Processing- Special Category PII

Who has PII?

Living People (aka Natural Person)

- The GDPR protects the PII of "natural persons whatever their nationality or place of residence"
- Referred to as a "Data Subject"
- This includes your employees/co-workers

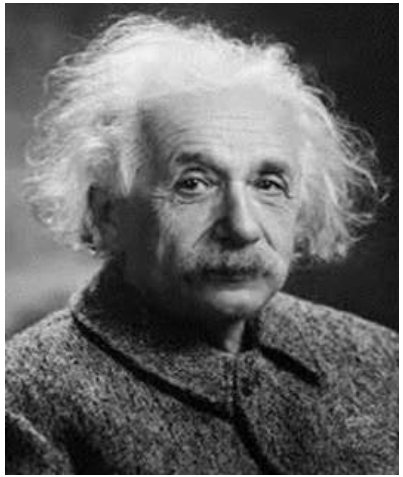
Can't be deceased

Can't be a corporate person (aka Legal Person)

Class question

Which of the following would be protected under the GDPR?

Michael Phelps
American Swimmer



Albert Einstein
German Physicist

Phoebe who lives in England

dcm

The Learning Experts

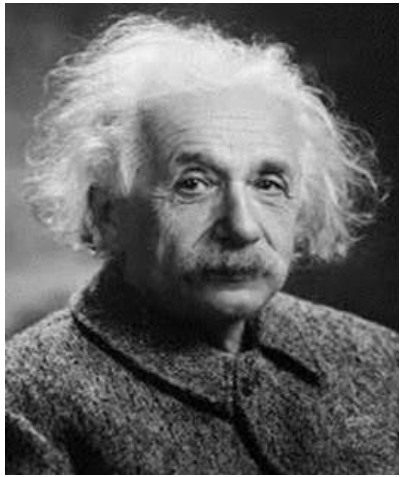
DCM Learning, an Irish based Training Company

Class question

Which of the following would be protected under the GDPR?

Michael Phelps
American Swimmer

✅



Albert Einstein
German Physicist

Phoebe who
lives in England

Legal entity

The Learning Experts

DCM Learning, an
Irish based Training
Company

Processing GDPR Definition

“Processing”, in relation to information or data means **“obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data”**, including: Manipulating data in some way:

- Organising and retrieving data
- Adaptation, alteration, or modification of the data
- Use of the information or data
- Transmitting the data and making the data available
- Destroying, blocking, or erasing data

Who Processes PII?

Data Controllers

"A natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by EU or Member State laws, the controller (or the criteria for nominating the controller) may be designated by those laws" (Art.4(7))

Data Processors

"A natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller" (Art.4(8))

Personal Data Breach

"Data Breach" means a breach of security leading to the…

- Accidental
- Unlawful destruction
- Loss
- Alteration
- Unauthorised disclosure of
- Or access to

…personal data transmitted, stored, or otherwise processed

Notification Obligations

Three data breach notifications are required under the GDPR, including:

1. Obligation for the Data Processor to notify Data Controllers

2. Obligation for the Data Controllers to notify Supervisory Authorities

3. Obligation for the Data Controllers to communicate a Data Breach to Data Subjects

Homepage | Data Protection Commission

Notifying of Breaches

You only have to notify the relevant Supervisory Authority of a breach…

- Where it is likely to result in a risk to the rights and freedoms of individuals
- If unaddressed, such a breach is likely to have a significant detrimental effect on individuals – for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage

In the event of a data breach causing **high risks** to Data Subjects, the Controller must notify the affected Data Subjects without undue delay

Quick Quiz

High Risk
Risk
Near Miss

Which of the following would be classified as a data breach under GDPR

A.A laptop, with customer details, is left on a train, it has no password and the hard drive is not encrypted

B.A paper file listing the profit margins by customer account numbers is left in a restaurant

C.A laptop, with customer details, is left on a train, it is password protected but the hard drive is not encrypted

D.A laptop, with customer details, is left on a train, it is password protected and the hard drive is strongly encrypted

E.A file of patients and their associated medical histories is accidently deleted and there is no backup file

F.A file of patients and their associated medical histories is accidently deleted and there is a backup file replaced immediately

Consequences of Failure

Data Controllers & Data Processors have joint liability for Data Breaches

Data Subjects have the right to sue…

- For material and non-material damage
- Separately or jointly (class actions)
- The Data Conroller and/or the Data Processor
- The Supervising Authority if they do not take action when a complaint is raised
- The regulations do not give an upper limit that can be awarded by the courts

The Supervising Authority can impose administrative fines

- Intended to be **"effective, proportionate, and dissuasive"** (Article 83)
- Maximum fine – €20M or 4% previous years global turnover for tier 1 breaches (Article 83)
- Maximum fine – €10M or 2% previous years global turnover for tier 2 breaches (Article 83)
- Can be mitigated by demonstrating that an effective and robust framework is in place to protect personal data

Statistics

On 2 September 2021, the Data Protection Commission (DPC) announced it has imposed a €225 million administrative fine against WhatsApp Ireland Limited , as well as a reprimand and an order to bring its processing into compliance.

In December 2022 the DPC fined Meta Ireland a total of €390 million for breaches of the GDPR relating to its Facebook (€210 million) and Instagram (€180 million) services. In addition, the DPC also noted that Meta Ireland must bring its processing operations into compliance with the GDPR within a period of three months.t

Fines

Data Protection Commission fines confirmed
30th November 2022
The Irish Data Protection Commission (DPC) yesterday had decisions to impose administrative fines on five different organisations confirmed in the Dublin Circuit Court The decisions in relation to each of the five separate inquiries can be found below.

MOVE Ireland - August 2021 (€1,500)
Teaching Council - December 2021 (€60,000)
Limerick City and County Council - December 2021 (€110,000)
Slane Credit Union - January 2022 (€5,000)
Bank of Ireland Group plc - March 2022 (€463,000)

Deputy Commissioner Graham Doyle and Deputy Commissioner Cian O'Brien have provided an overview of these investigations, discussing the outcomes, fines and reprimands, in the latest DPC podcast - available here.

Ireland ranked second highest for GDPR fines - DLA Piper survey

Nearly €1.1 billion in fines have been imposed for a wide range of infringements of Europe's General Data Protection Regulation, a new survey shows today.
This represents a 594% annual increase in fines imposed since January 2021, according to international law firm DLA Piper's latest annual General Data Protection Regulation (GDPR) fines and data breach survey.
A total of 6,802 data breaches were reported to the Irish Data Protection Commission in the past 12 months, the survey shows.
Ireland recorded the sixth highest level of breach notifications across Europe and fourth highest on a per capita basis.
The survey shows that Luxembourg, Ireland and France top the rankings for the highest individual fines - €746m, €225m and €50m respectively.
Luxembourg and Ireland have each imposed record breaking fines moving them from the bottom to the top of the league tables.

DPIA (Data Protection Impact Assessment)

An assessment primarily aimed at identifying risks to Personal Information

GDPR mandates that a DPIA must be carried out when designing new processes that carry a high risk of data breaches

Privacy by Design & Default

Privacy by Design and Default, sometimes known as “Privacy by Design”, is a concept that prioritises privacy and data protection compliance from the start, when a system is being developed

GDPR mandates that all new projects that manipulate PII **must follow this approach**

The DPIA is a fundamental part of Privacy by Design

Profiling

The GDPR defines profiling as “any form of automated processing intended to evaluate certain personal aspects of an individual”, in particular to analyse or predict their:

- Performance at work
- Economic situation
- Health
- Personal preferences
- Reliability
- Behaviour
- Location
- Movements

The GDPR places considerable limitations on profiling

Pseudonymisation

“Anonymisation” of data means processing it with the aim of irreversibly preventing the identification of the individual that it concerns

“Pseudonymisation” of data means replacing any potentially identifiable information concerning an individual’s characteristics with a pseudonym, eg using codes or numbers to ensure that the data subject cannot be identified

Technical and organisational measures can be used to ensure that the personal data is accessible by an identified or identifiable person

- However it still remains “personal data”
- The identifiable data must be kept separate from the pseudonymous data
- Forms should include encryption or tokenisation

Principles & Rights

Principles

1. Legality, Transparency, & Fairness
2. Purpose Limitation
3. Minimisation
4. Accuracy
5. Storage Limitation
6. Integrity & Confidentiality
7. Accountability

Rights

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Principles

1 Legal – 3 groups of PII : standard, sensitive, criminal offence data

Fair – 8 Rights

& Transparent – plain English, free, readable

2 Purpose Limitation – PII for explicit and legitimate purposes, must not be further processed

3 Minimisation – relevant, adequate, limited

4 Accuracy – PII kept up to date

5 Storage Limitation – retention periods : legal requirements, have consent, how many copies, where is it stored – DPC can advise

6 Integrity & Confidentiality - security

7 Accountability – DC accountable not DPO, demonstrate robust process, policies, procedures, effective documentation, SARS, DPIA, audits…

Data Subjects Rights

1 Informed : DS should be clear about what, why and how PII is processed eg privacy notice, cookie notice…

2 Access : DS has the right to know what data is held on them, triggered by a SAR

3 Rectification : DS can request corrections to PII eg; marital status

4 Erasure : DS can request to be forgotten

5 Restrict Processing : DS can ask an organisation to stop processing their PII eg; weekly subscription stop for 1 month

6 Portability : DS can request PII in a machine readable format

7 Object : DS can object to an organisation processing their PII

8 Automated Decision Making & Profiling : DS can request human contact and query a decision

Consent

An indication of the data subject's wishes, which affirmatively and clearly indicates consensual acceptance by the Data Subject of the processing of their personal data

"Consent" of the data subject means:

- Freely given
- Specific
- Informed

Subject Access Request

Often called just “Access Request”

Under the GDPR Data Subjects have the legal right to ask a Data Controller or a Data Processor what PII they hold on them

Data Subjects also have the right to stop data processing or terminate it and have their PII erased

Legal Basis for Data Processing

Another useful GDPR requirements' checklist is one that presents you with the legal bases for data processing.

For most websites, it is the legal basis of **consent** that is relevant, but it might be useful for you to know what other bases exist for data processing in the European Union.

In this GDPR checklist, you find the legal bases for processing of data as **required by the GDPR**:

- **Consent**: the data subject gives their unambiguous and free consent to process their data.
- **Contractual**: data processing is necessary to execute or to prepare to enter into a contract that the data subject is a part of.
- **Legal obligation**: data processing is necessary in order to comply with a legal obligation.
- **To save somebody's life**: when the processing of data is necessary to prevent death.
- **Legitimate interest**: arguably the most flexible of the bases

When processing personal data of EU citizens, one of the above legal bases must be presented. If this is not possible, you are not allowed to process personal data.

You find more on the legal bases for data processing in **Article 6 of the GDPR**.

Test your knowledge

Workshop quiz

Q1 Which of the following is a role described by the GDPR?

a) Data Processor

b) Data Privacy Official

c) Data Commissioner

d) None of the above

Q2 Which one of the following is a right?

a) The right to be protected

b) The right of access

c) The right to review

d) The right to respite

Workshop quiz

Q3 Who gives consent?

a) Data Processor

b) Data Subject

c) Supervisory Authority

d) Data Processor

Q4 The main focus of the GDPR is…?

a) International trade

b) Trade internal to the EU

c) People and their personal information

d) People and their ability to access information

Workshop quiz

Q5 Under GDPR, organisations in breach of GDPR can be fined up to a maximum of:

a) 8% of annual global turnover

b) 2% of annual global turnover

c) 3% of annual global turnover

d) 4% of annual global turnover

Q6 Which one of the following is the best example of special data?

a) Your name

b) Your phone number

c) Your ethnic origin

d) Your online identifier

Workshop quiz

Q7 Which if the following is Special Category Data?

a) Kara Ovington

b) jermain@dcmlearning.ie

c) 01/11/2022

d) O negative

Q8 How many Lawful processing reasons do you need for the following data, 1 or 2?

a) Your name

b) Your phone number

c) Your ethnic origin

d) Your online identifier

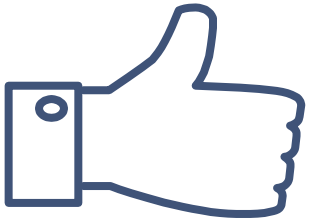
Useful Websites

Homepage | Data Protection Commission

Privacy Policy Template - TermsFeed

Juro | Privacy policy

Privacy, Security and Information Blog | Fieldfisher



THANKS!


dcm
THE
LEARNING
EXPERTS