Essential Guide to Data Protection

Trainer: Paula Williams

1

Course Content

- An understanding of the General Data Protection Regulations
- What you need to be doing and why

Course Summary
This course will develop your understanding of what good data handling is in practice and a of the legal requirements placed on a company under the general data protection regulations.

Course Content:

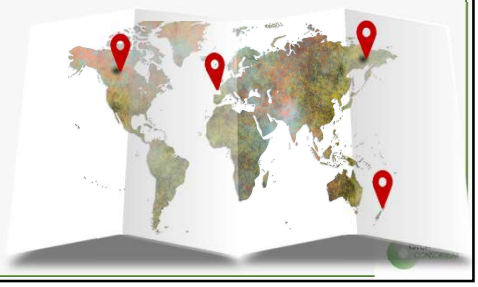
- Why data protection is important
- The data protection requirements a company needs to meet
- Personal data and sensitive data
- The principles of good data handling
- Lawful reason for processing personal information
- An individual's right
- What is considered a data breach
- The role of the DPO and the Regulator

2

The Rise of Data Protection

When we get data protection and data privacy <u>wrong</u> real lives are affected

- Data Driven World
- Digital Universe and Physical Universe
- Identify Theft and Financial Loss
- Individuals can Protect their Privacy
- GDPR standardising Data Protection



3

GDPR Requirements

Cultural Change

4

GDPR Requirements

Cultural Change

1

ACCOUNTABILITY

Greater **accountability** for the way they collect, process, retain and secure an individual's personal information.

2

TRANSPARANCY

More **transparency** about the handling of personal data.

3

LAWFUL REASON

Have a legal basis **(Lawful Reason)** for processing.

4

INDIVIDUAL RIGHTS

Processing in-line with an **individual's rights**

5

ADEQUECY

Ensure **adequate protection** when transferring to another country

6

EVIDENCE

Be able to **evidence** compliance with the new data protection rules

7

DATA PRIVACY

Ensure the management of **data privacy** is built into the fabric of how a company operates

8

DATA BREACHES

Mandatory reporting of **data breaches** involving personal data

Data Protection Officer

5

Data Categories

Personal Data

Any information relating to an identified or identifiable natural person ('data subject') who can be identified, directly or indirectly.

The definition of personal data has been increased to include location data (GPS), genetic data e.g. biometrics, online identifiers (IP addresses) and social identifiers e.g. religion.

Sensitive Personal Data

Is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sexual information, criminal proceedings or convictions.

Also Includes: *Opinions, Files, Back ups, Data Combinations, CCTV, Recorded Telephone Calls*

6

GDPR Principles

Personal information must be:

Transparency

1. fairly and lawfully processed; transparent
2. processed for limited purposes and not in any manner incompatible with those purposes

Data Quality

3. adequate, relevant and not excessive
4. accurate and where necessary, kept up to date
5. not kept for longer than is necessary

Security

6. kept secure
   - processed in line with the individuals rights;
   - not transferred to countries outside the Bailiwick/EEA without adequate data protection.

7

Lawful Processing of Personal Information

Data can be processed legitimately if at least **one** of the following applies:

1.	Contract	An individual is entering into a contract or is already in a contract which covers the processing of their information
2.	Consent	If the person agrees and gives clear consent for the processing of their information. It must be verifiable that consent was specifically given by the individual.
3.	Legal Obligation	Processing is required by law for legal or regulatory compliance.
4.	Legitimate Interests	Information may be processed when a company or third party, has a legitimate interest to do so, unless overridden by the interests, rights or freedoms of the individual *e.g. defence of a court claim.*
5.	Protect Vital Interests	Where processing is needed to protect the vital interests of an individual (often in relation to health and safety).
6.	Task in Public Interest	For the performance of a task that is being carried out in the public interest or in the exercise of official authority vested in a company.

Sensitive Data: more astringent requirements. Require one of the above and a defined condition to process.

8

Defined Conditions for Sensitive Personal Information

Sensitive data can be processed if **one** of the following applies:

1.	The individual has given explicit consent.	6.	To exercise or defend a legal claim or by the courts.
2.	Processing is required for employment, social security, social protection and has appropriate safeguards.	7.	When required for the reason of substantial public interest. The right to data protection must be respected and safeguards in place.
3.	To protect the vital interests, where individual is physically or legally incapable of giving consent.	8.	For preventative medical purposes or occupational health.
4.	Legitimate activities of a Foundation, Association or Not-for-Profit with appropriate safeguards and is not disclosed externally without consent.	9.	When required in the interest of public health. This includes health and medical care.
5.	When the personal information has clearly, already been made public by the individual.	10.	To archive information in the public interest, for statistical, scientific or historical research purposes.

Sensitive personal information must have **astringent security** measures in place to ensure adequate protection of the information.

9

Individuals Rights

- Right to be Informed
- Right to Access (subject access request)
- Right to Rectification (amend or correct)
- Right to Object (to use)
- Right not to be subject to Fully Automated Decisions

ADDITIONAL

- The right to Erasure
- The right to Restrict Processing
- The right to Data Portability

10

Role of Data Protection Officer (DPO)

- Data Protection Compliance
- Handling and Reporting Data Breaches
- New Policies and Procedures
- Liaise with SMT and Data Protection Commissioners Office

Office of Data Protection Authority

- Independent Supervisory Authority's
- Investigate issues
- Conduct Audits
- Corrective Actions
- Impose Fines
- Restrict Processing

11

What Has Changed …

Security Measures

- Sharpening of security procedures (cyber)
- Transferring personal data
- Use of emails, mobile devices

Data Handling

- How data is stored, processed, shared and retained
- How to handle requests to exercise an 'Individuals Rights' ***(identification)***
- **New procedures:** erasure, data portability, subject access requests, use privacy notices, restriction on processing, opting in to marketing
- Collection of personal information and note taking ***(not excessive, accuracy)***
- Reporting concerns or if suspect data breach

12

What is a Data Breach?

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Can include:

- access by an unauthorised third party
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data

Is there personal data involved?

Is there a risk to the rights and freedoms of an individual?

Must be reported within 72 hours

13

Risk of Fines

Higher Fines

GDPR: Up to €20 million (£17.5m) or 4% of worldwide annual turnover (highest)

Local: Up to £10 million or 2% of worldwide annual turnover

(capped at £300,000 for smaller companies)

1. A breach of GDPR principles
2. Issues surrounding the rights of an individual
3. Where data processing is unlawful
4. Where consent cannot be proven or processing was continued after consent was withdrawn
5. Breaches of sensitive data
6. Transfers to countries where data privacy rights are not equivalent
7. Issues around cooperation with the Data Commissioner (or not meeting corrective actions)

14

What can I Do?

Familiarise yourself with current security procedures and changes

- Check **identification** before discussing or releasing personal information
- Do not **record** anything that is unfair or untrue
- Only use personal information **to do your job** *(legal basis)*
- **Do not** leave personal information **lying around** or on your screen
- Know **what to tell individuals** about how their data is being used
- Use **strong passwords**
- Avoid accessing personal information from **portable devices**
- **Clear your desk** and **lock** personal information in filing cabinets
- Ensure your workplace is **secured** when leaving the office
- **Dispose** of information securely when it is no longer needed.
- **Do not** pass personal information on to another person unless you know they are **authorised** to have that information.

15

Password Security

Password Barrier

- **Access management** - different levels of access are assigned to login names
- **Granted** when you start a new job or change your role
- Manage against **insider threat** (or a disgruntled employee)

Brute force

Computer program inputs passwords from a comprehensive list of common passwords (billions of password combinations)

A good way of ensuring your passwords are secure is to:

- change your passwords regularly
- use a longer, more complex and random password is the more difficult it will be for a criminal to guess e.g. Not Rufus2021.

16

Password Security

A much better password could more accurately be called a pass phrase and go something like this:

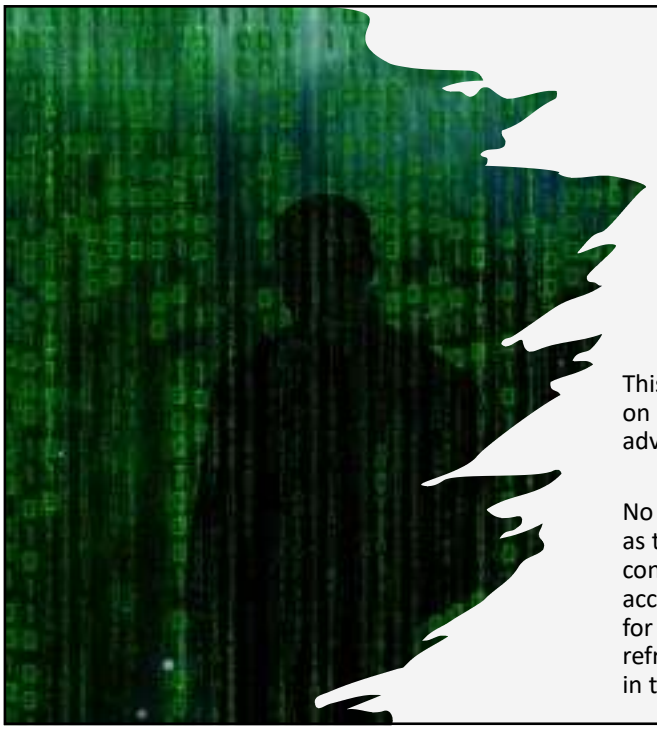
My first job was at Pizza Hut and I was paid £250 per week.

Which you can turn into **MfjwaPHaIwp$250pw**

Good Habits:

1. Make passwords long (12 characters or more)
2. Include numbers, symbols and special characters
3. Don't use a dictionary word or combination of dictionary words
4. Pass phrases make best passwords
5. Change passwords regularly at least every 30 to 60 days
6. Consider using a Password Manager

17



Essential Guide to Data Protection

Trainer: Paula Williams

18