

21 Academy

Course

Online Sessions

Data Protection Officer

Data Protection Officer/Lead

www.21academy.education



2099 5486



21 Academy | 21 Academy | 21 Academy

Data Protection Officer/ Lead Course

Session 4

DPIAs

+

Policies &
Procedures

+

Auditing

Session 3

Data Subject
Rights

+

Withdrawing
Consent

+

DARs

+ GDPR in
employment

Session 2

Controller
Role

+

Processor
Role

+

Transfers
outside EU

Session 1

Introduction
to the DPO
Role

+

Personal
Data

+

6 Principles

Session No. 5 – November 2025

- 1. Dealing with IT & Security**
- 2. Data Security Failures**
- 3. Recording and Reporting Breaches**
- 4. The Costs & Implications of Getting GDPR Wrong**

KEY GDPR INGREDIENTS TO COMPLIANCE



KEY GDPR INGREDIENTS TO COMPLIANCE

Grounds



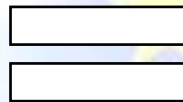
Principles



Rights



Special
Rules



Compliance

KEY GDPR INGREDIENTS TO COMPLIANCE

Grounds



Principles



Rights



Special
Rules

+ SECURITY =

Compliance

Key Laws

1. GDPR
2. Chapter 586; DPA
3. S.L.586.01 (e-communications sector)
4. (AI ACT)



Dealing with IT & Security

➡ Why should we worry about information security?

- ❑ Poor information security leaves systems and services at risk and may cause **real harm and distress** to individuals – lives may even be endangered in some extreme cases.

Dealing with IT & Security

👉 Why should we worry about information security?

❑ Some **examples of the harm** caused by the loss or abuse of personal data include:

- identity fraud;
- fake credit card transactions;
- targeting of individuals by fraudsters;
- witnesses put at risk of physical harm or intimidation;
- offenders at risk from vigilantes;
- exposure of the addresses of service personnel, police and prison officers, and those at risk of domestic violence;
- fake applications for tax credits; and
- mortgage fraud.

Dealing with IT & Security

🔑 GUIDING PRINCIPLES



Privacy By Design



Privacy By Default



GDPR, Article 5(1)f – the 6th Principle

Dealing with IT & Security

➤ GUIDING PRINCIPLES

GDPR, Article 5(1)f – the 6th Principle



*Personal Data shall be processed in a manner that ensures **appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate **technical or organisational measures***

(‘integrity and confidentiality’).

Dealing with IT & Security

➤ GUIDING PRINCIPLES

GDPR, Article 5(1)f – the 6th Principle



- ❑ to have ‘appropriate technical and organisational measures’

Dealing with IT & Security

➡ GUIDING PRINCIPLES

GDPR, Article 5(1)f – the 6th Principle



- ☐ GDPR provides **specifics** about what you have to do about the security of your processing and how you should
 - (i) assess your information **risk** and
 - (ii) put appropriate **security measures** in place.

Dealing with IT & Security

➤ GUIDING PRINCIPLES

GDPR, Article 5(1)f – the 6th Principle



- ☐ The security principle goes beyond the way you store or transmit information.
- ☐ **Every aspect** of your processing of personal data is covered, not just cybersecurity.

Dealing with IT & Security

GUIDING PRINCIPLES

GDPR, Article 5(1)f – the 6th Principle

☐ Security measures put in place should seek to ensure :

CONFIDENTIALITY



1. the data can be accessed, altered, disclosed or deleted only by those you are **authorised** to do so (and that those people only **act within the scope** of the authority you give them);

INTEGRITY



2. the data you hold is **accurate + complete** in relation to why you are processing it; and

AVAILABILITY



3. the **data remains accessible and usable**, ie, if personal data is accidentally lost, altered or destroyed, you should be able to recover it and therefore prevent any damage or distress to the individuals concerned

Dealing with IT & Security

➤ GUIDING PRINCIPLES

PRIVACY BY DESIGN



GDPR :- The controller shall, both **at the time of the determination of the means for processing & at the time of the processing itself**, implement appropriate technical and organisational measures designed to implement data-protection principles in an effective manner

Dealing with IT & Security

➤ GUIDING PRINCIPLES

PRIVACY BY DESIGN



The **ICO** encourages organisations to ensure that privacy and data protection is a key consideration in the **early stages** of any project, and then throughout its **lifecycle**.

Example when:

1. *building new IT systems for storing or accessing personal data;*
2. *developing legislation, policy or strategies that have privacy implications;*
3. *embarking on a data sharing initiative; or*
4. *using data for new purposes.*

Dealing with IT & Security

➡ GUIDING PRINCIPLES

PRIVACY BY DESIGN



7 Principles (Ontario IPC)

1. **Proactive** not Reactive; Preventative not Remedial
2. Privacy as the **Default** Setting
3. Privacy **Embedded** into Design
4. **Full Functionality** — Positive-Sum, not Zero-Sum
5. End-to-End Security — **Full Lifecycle** Protection
6. Visibility and Transparency — Keep it **Open**
7. Respect for User Privacy — Keep it **User-Centric**

Dealing with IT & Security

➡ GUIDING PRINCIPLES

PRIVACY BY DEFAULT



GDPR :- The controller shall implement **mechanisms** for ensuring that, **by default**, only those personal data are processed which are **necessary** for each specific purpose of the processing,

(& not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage).

Dealing with IT & Security

➤ GUIDING PRINCIPLES

PRIVACY BY DESIGN



Privacy Impact Assessments (DPIAs)
*are an integral part of taking a
privacy by design & default
approach.*



Impact Assessments

- **What is it?** An assessment of the impact of the envisaged processing operations on the protection of personal data
- **Mandatory** – *the controller **shall** carry out...*
 - **High Risk Situations**
 - **As a Pre-requisite to processing**
 - **With Prior Consultation with DP Commissioner**

Impact Assessments



Especially when

- i. Using '**new technologies**';
- ii. Using extensive and systematic evaluation of **personal aspects** relating to persons based on **automated processing** (including profiling) leading to **decisions that produce legal effects**;
- iii. Large scale processing of **sensitive data**
- iv. Systematic processing of a **publicly accessible area** on a large scale

Impact Assessments

Article 29 W.P. : high risk is likely to include :



- i. **Evaluation or Scoring** (e.g. using credit agencies, offering genetic tests to predict health risks, building marketing profiles based on usage or website navigation);
- ii. **Data concerning vulnerable data subjects** (e.g. children, employees, elderly)
- iii. **Matching or combining datasets** in a way that exceeds the reasonable expectations of data subjects;
- iv. **Where processing prevents data subjects from exercising a contract or using a service;** (e.g. a bank requiring to screen a credit reference to give a loan)



IDPC:

[Data Protection Impact Assessment - IDPC](#)

EDPB :

[wp248 rev.01](#)

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679

EDPB :

[edpb_guidelines_202502_blockchain_en.pdf](#)



A DPIA is needed if personal data will be processed using Blockchain Technology

*“The EDPB recommends setting out **technical and organisational procedures to disclose software vulnerabilities** to all participants, including an **emergency plan** that allows algorithms to be changed when a vulnerability is identified and to **notify security incidents** and personal data breaches to the relevant SAs, and to communicate the incident to the involved data subjects”*

1. Carry out an evaluation of the security safeguards necessary to assure the security of the blockchain appropriate to the risks.
2. The governance of software and protocol evolution should be documented.
3. Set out technical and organisational procedures to limit the impact of a potential algorithm failure (as an attack on one of the cryptographic primitives used in the blockchain).
4. limit accessibility of the blockchain and ensure the blockchain’s confidentiality. (implemented and verified)

Impact Assessments



To include:

- i. Description of processing / purposes
- ii. Assessment of necessity + proportionality
- iii. Assessment of risks
- iv. Measures envisaged to address risks
- v. References to Codes of Conduct
- vi. **Seek views of DPO**
- vii. (where appropriate) **seek views of data subjects (or their reps / unions ?)**

Impact Assessments



1. Must be **prior** to processing;
2. Must be **continual** (not a one time process);
3. Processors should assist controllers;
4. Recommended to seek independent expert advice.

ISO/IEC 29134:2017 : Information technology --
Security techniques -- Guidelines for privacy impact
assessment

Impact Assessments



The WP29 DPIA Guidelines suggest that a DPIA should be "**continuously reviewed and regularly re-assessed**" as a matter of good practice

Dealing with IT & Security



GDPR Legal & IT/Security Audits

WHY?



HOW?

WHY?



HOW?

WHY?



WHO?

HOW?

WHY?



WHO?

WHEN?



WHEN?



WHEN?

**IF YOU
HAVENT
STARTED**

**START
NOW**



WHY?



WHY?



1. WORK TOWARDS GDPR COMPLIANCE

WHY?



- 1. WORK TOWARDS GDPR COMPLIANCE**
- 2. UNDERSTAND WHAT PD IS PROCESSED**

WHY?



- 1. WORK TOWARDS GDPR COMPLIANCE**
- 2. UNDERSTAND WHAT PD IS PROCESSED**
- 3. IMPROVE EFFICIENCIES + SMARTER USE OF YOUR DATA**

WHY?



1. **WORK TOWARDS GDPR COMPLIANCE**
2. **UNDERSTAND WHAT PD IS PROCESSED**
3. **IMPROVE EFFICIENCIES + SMARTER USE OF YOUR DATA**
4. **FACILITATE DATA MANAGEMENT (E.G. RESPONSE TIME)**

WHY?



1. **WORK TOWARDS GDPR COMPLIANCE**
2. **UNDERSTAND WHAT PD IS PROCESSED**
3. **IMPROVE EFFICIENCIES + SMARTER USE OF YOUR DATA**
4. **FACILITATE DATA MANAGEMENT (E.G. RESPONSE TIME)**
5. **MITIGATE RISKS**

GDPR COMPLIANCE

WHY?



WHY?



GDPR COMPLIANCE



Principle of accountability

*Controller = responsible for, and be able to **demonstrate compliance** with, the data protection principles;*

WHY?



GDPR COMPLIANCE



Principle of accountability

*Controller = responsible for, and be able to **demonstrate compliance** with, the data protection principles;*



Record keeping obligation;

WHY?



GDPR COMPLIANCE

Principle of accountability

*Controller = responsible for, and be able to **demonstrate compliance** with, the data protection principles;*

Record keeping obligation;

Provide records to supervisory authority on request

WHY?



GDPR COMPLIANCE

Principle of accountability

*Controller = responsible for, and be able to **demonstrate compliance** with, the data protection principles;*

Record keeping obligation;

Provide records to supervisory authority on request

Facilitates DPO

WHY?



GDPR COMPLIANCE

Principle of accountability

*Controller = responsible for, and be able to **demonstrate compliance** with, the data protection principles;*

Record keeping obligation

Provide records to supervisory authority on request

Facilitates DPO

Facilitates Responses to objection/access/rectification/portability/breaches

Facilitates
Compliance with
organisation &
security measures

WHY?

Facilitates
Responses to
objection/access/
rectification/
portability/breaches



Facilitates DPO

GDPR COMPLIANCE

Principle of accountability

*Controller = responsible for, and
be able to **demonstrate
compliance** with, the data
protection principles;*

Record keeping obligation

Provide records to
supervisory authority on
request



**Facilitates
Compliance with
organisation &
security measures**



RECITAL 83 :

In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should **evaluate the risks** inherent in the processing and **implement measures** to mitigate those risks, such as encryption.





**Facilitates
Compliance with
organisation &
security measures**



RECITAL 83 :



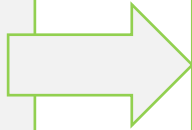
In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should **evaluate the risks** inherent in the processing and **implement measures** to mitigate those risks, such as encryption.



Those measures should ensure an **appropriate level of security, including confidentiality**, taking into account the **state of the art** and the **costs of implementation** in relation to the risks and the nature of the personal data to be protected.



**Facilitates
Compliance with
organisation &
security measures**



RECITAL 83 :

In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should **evaluate the risks** inherent in the processing and **implement measures** to mitigate those risks, such as encryption.



Those measures should ensure an **appropriate level of security, including confidentiality**, taking into account the **state of the art** and the **costs of implementation** in relation to the risks and the nature of the personal data to be protected.



In assessing data security risk, **consideration should be given to the risks** that are presented by personal data processing, such as:

- **accidental or unlawful destruction,**
- **loss,**
- **alteration,**
- **unauthorised disclosure of, or access** to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.



RECITAL 83 :

In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should **evaluate the risks** inherent in the processing and **implement measures** to mitigate those risks, such as encryption.

Facilitates
Compliance with
organisation &
security measures



Those measures should ensure an **appropriate level of security, including confidentiality**, taking into account the **state of the art** and the **costs of implementation** in relation to the risks and the nature of the personal data to be protected.

Article 5(f)
6th Principle of
Integrity &
Confidentiality



In assessing data security risk, **consideration should be given to the risks** that are presented by personal data processing, such as:

- **accidental or unlawful destruction,**
- **loss,**
- **alteration,**
- **unauthorised disclosure of, or access to,** personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.



Article 30(1)g

Controller to **keep records of** .. *a general description of the technical and organisational security measures*



Article 32 Security of Processing

Controller to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- (a) the **pseudonymisation and encryption** of personal data;
- (b) the ability to ensure the ongoing **confidentiality, integrity, availability and resilience** of processing systems and services;
- (c) the **ability to restore** the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (d) a process for **regularly testing, assessing and evaluating the effectiveness** of technical and organisational measures for ensuring the security of the processing.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes and risk of varying likelihood and severity for the rights of persons...





Documentation

Ensure that there is:

- A **suite of security policies and procedures** which specify the technical, administrative and physical safeguards for personal data. These documents should include policies or instructions to employees which, at a minimum, address how to manage certain risks such as secure password management, using software/hardware, emails, clear desk policies, using social media, loss of data or equipment, using third party processors and bring your own device (BYOD).
- A **disaster recovery plan**.
- A **records retention policy**, procedures and schedule. This must be updated regularly and the criteria for retention made clear to employees.
- An **appropriate policy document**, if special categories of personal data or criminal offences data are processed.



Documentation

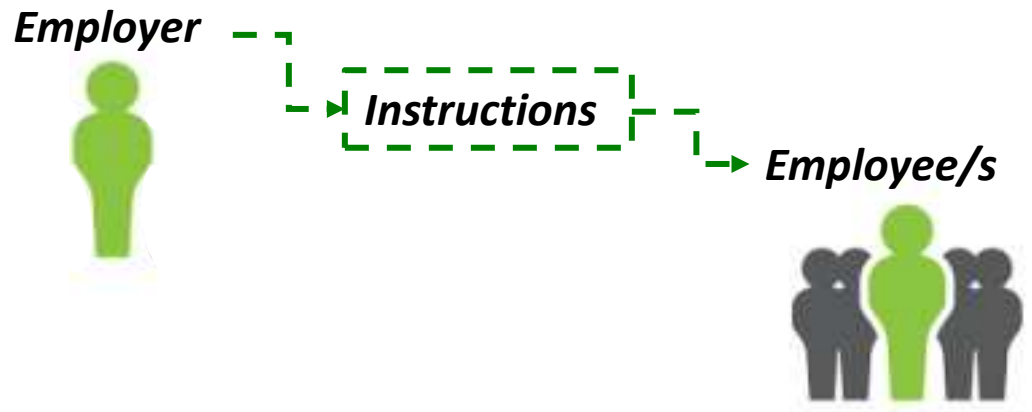
Ensure that these documents:

- Are **published and easily accessible** to employees and where applicable, contractors and third parties.
- Are **reviewed** regularly.
- Meet the **requirements of the laws**, regulations, standards and frameworks your organisation is subject to.
- **Meet business need.**



Article 32(4)

Controller and processor shall take steps to ensure that any natural **person acting under the authority of the controller** or the processor who has access to personal data does not process them **except on instructions** from the controller,



Appoint accountable individuals and departments



- Assign accountability and responsibility for security.
- Designate individuals and departments:
 - according to the size of your organisation;
 - based on criteria relevant to your organisation such as risk, industry and threat level, volume of data and scale of processing;
 - based on responsibilities including organisational ones and technical acumen.
- Where responsibilities overlap, identify joint responsibilities.



Carry out training and communication



- Ensure that training and communication is in place to train all staff who process personal data, including special categories of data
- Staff be
 - given onboarding training;
 - Understand their role and responsibilities in protecting data;
 - be familiar with your information security resources and procedures;
 - be reminded of these at regular intervals (frequency should be based on risk);
 - understand data security measures designed to protect them and their handling of personal data (antivirus, SPAM controls, clear desk policies, reporting lost or stolen equipment);
- understand what constitutes data security breaches (understand what constitutes a threat (phishing attacks, blagging, deception, unauthorised data manipulation)



Monitor

- Monitor **general standards of good industry** and sector practice on an ongoing basis and take account of the state of the art and costs of implementation.
- Implement **recognised standards** such as ISO 27001 or benchmark against such standards.
- Eliminate data protection risks by **anonymising** data where possible.



Check Third-Party Arrangements

- Understand your network of third party arrangements (this will include both controllers and processors).
- Ensure the contractual provisions and contractually specified data security measures meet the standard you require.
- Ensure your third party processors know how to report data breaches.
- Where necessary, help third parties meet the minimum data security standards you require, especially where you are dependent on their services or they could pose data security risk to your business.
- For organisations that transfer personal data to third party service providers, review these contracts to ensure that they have the appropriate provisions and consider audits



NO-ONE-SIZE-FITS-ALL
adopt a risk-based approach



This Risk Assessment should take account of factors such as:

1. the **nature and extent** of your organisation's premises and computer systems;
2. the **number of staff** you have;
3. the extent of their **access** to the personal data; and
4. personal data held or used by a **third party** on your behalf



security measures should seek to ensure that:

- i. only **authorised people** can access, alter, disclose or destroy personal data;
- ii. those people only **act within the scope** of their authority; and
- iii. if personal data is accidentally lost, altered or destroyed, it can be **recovered** to prevent any damage or distress to the individuals concerned

GDPR LEGAL EXPERTS ●



WHO?

GDPR LEGAL EXPERTS ●

GDPR ICT EXPERTS ●



WHO?

GDPR LEGAL EXPERTS



GDPR ICT EXPERTS



YOUR DECISION MAKERS



WHO?

GDPR LEGAL EXPERTS ●

GDPR ICT EXPERTS ●

YOUR DECISION MAKERS ●



WHO?

GDPR LEGAL EXPERTS

GDPR ICT EXPERTS

YOUR DECISION MAKERS



WHO?

YOUR TEAM MEMBERS / STAFF

HOW?



● HOW?

**requires a
structured &
planned approach**



● HOW?

**requires a
structured &
planned approach**

1. Appoint a team + Leader
2. Rope in IT
3. Define a Project Plan



● HOW?

**requires a
structured &
planned approach**

1. Appoint a team + Leader
2. Rope in IT
3. Define a Project Plan
4. Training – understand definitions + your obligations + rights



● HOW?

**requires a
structured &
planned approach**



1. Appoint a team + Leader
2. Rope in IT
3. Define a Project Plan
4. Training – understand definitions + your obligations + rights
5. Gather relevant information.



● HOW?

**requires a
structured &
planned approach**

1. Appoint a team + Leader
2. Rope in IT
3. Define a Project Plan
4. Training – understand definitions + your obligations + rights
5. Gather relevant information.

- 
- **dynamic consultation**
 - **Interviews/surveys**
 - **Documentation**



●HOW?

**requires a
structured &
planned approach**



1. Appoint a team + Leader
2. Rope in IT
3. Define a Project Plan
4. Training – understand definitions + your obligations + rights
5. Gather relevant information.

E.g.
Fenech & Fenech Advocates
DATA INVENTORY FORM

- **dynamic consultation**
- **Interviews/surveys**
- **Documentation**



DATA INVENTORY FORM

25 Sections per process



- Process Description
- Process Flow
- Controller/Processor (joint/sub)
- Categories of personal data
- Purpose/s
- Grounds
- Principles
- Information Obligation
- Data Subject Rights
- Automated Decision Making / profiling
- Security measures
- Documentation (e.g. consent form)
- Breach notification procedures & policies



- A **systematic description** of the processing is required:
 - nature, scope, context and purposes of the processing are taken into account ;
 - personal **data, recipients and the period** for which the personal data will be stored are recorded;
 - a functional **description** of the processing operation is provided;
 - the **assets** on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified; and
 - compliance with **approved codes of conduct** is taken into account.

● HOW?

**requires a
structured &
planned approach**



1. Appoint a team + Leader
2. Rope in IT
3. Define a Project Plan
4. Training – understand definitions + your obligations + rights
5. Gather relevant information. (interview / survey individuals + documentation)
6. Prepare a Data Map





● HOW?

Data Mapping

1. DATA ITEMS

(e.g. names, email addresses, records)

2. FORMATS

(e.g. hard copy forms, online data entry, database)

3. TRANSFER METHODS

(e.g. post, telephone, internal/external)

4. LOCATIONS

(e.g. offices, Cloud, third parties)



● HOW?

Data Mapping

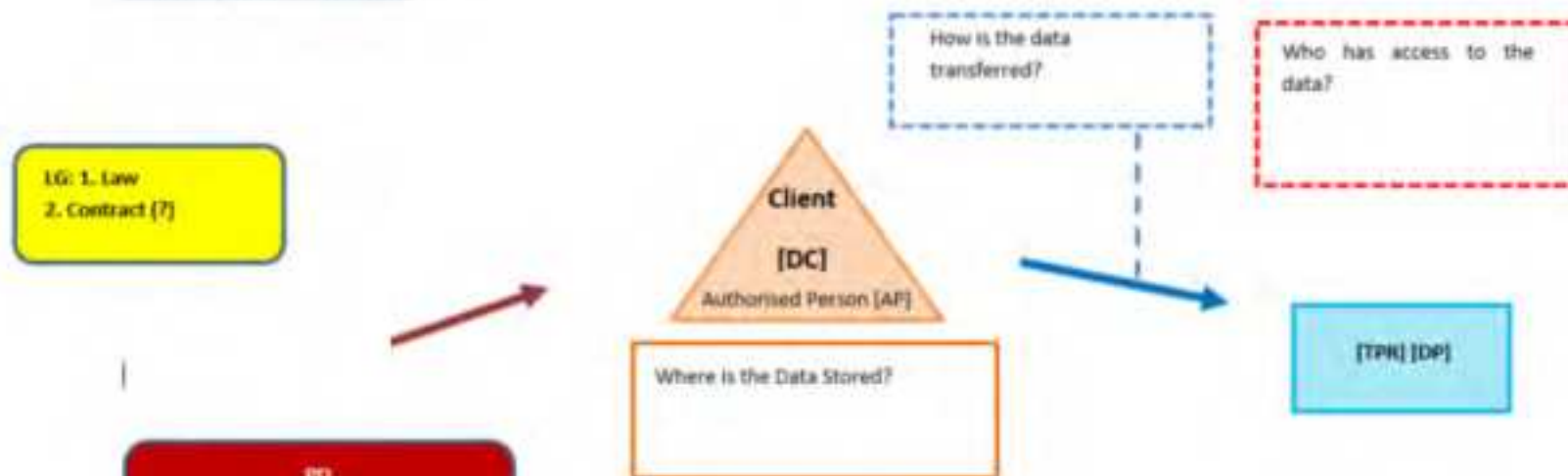
Must identify:

- categories of personal data;
- special category data;
- categories of data subjects
- the purpose and means of processing (processing includes any use of the data including collection, storage, disclosure, global data transfers); and
- who has access to personal data.



Data Flow - Mapping Exercise

CODE - Entity - PROCESS

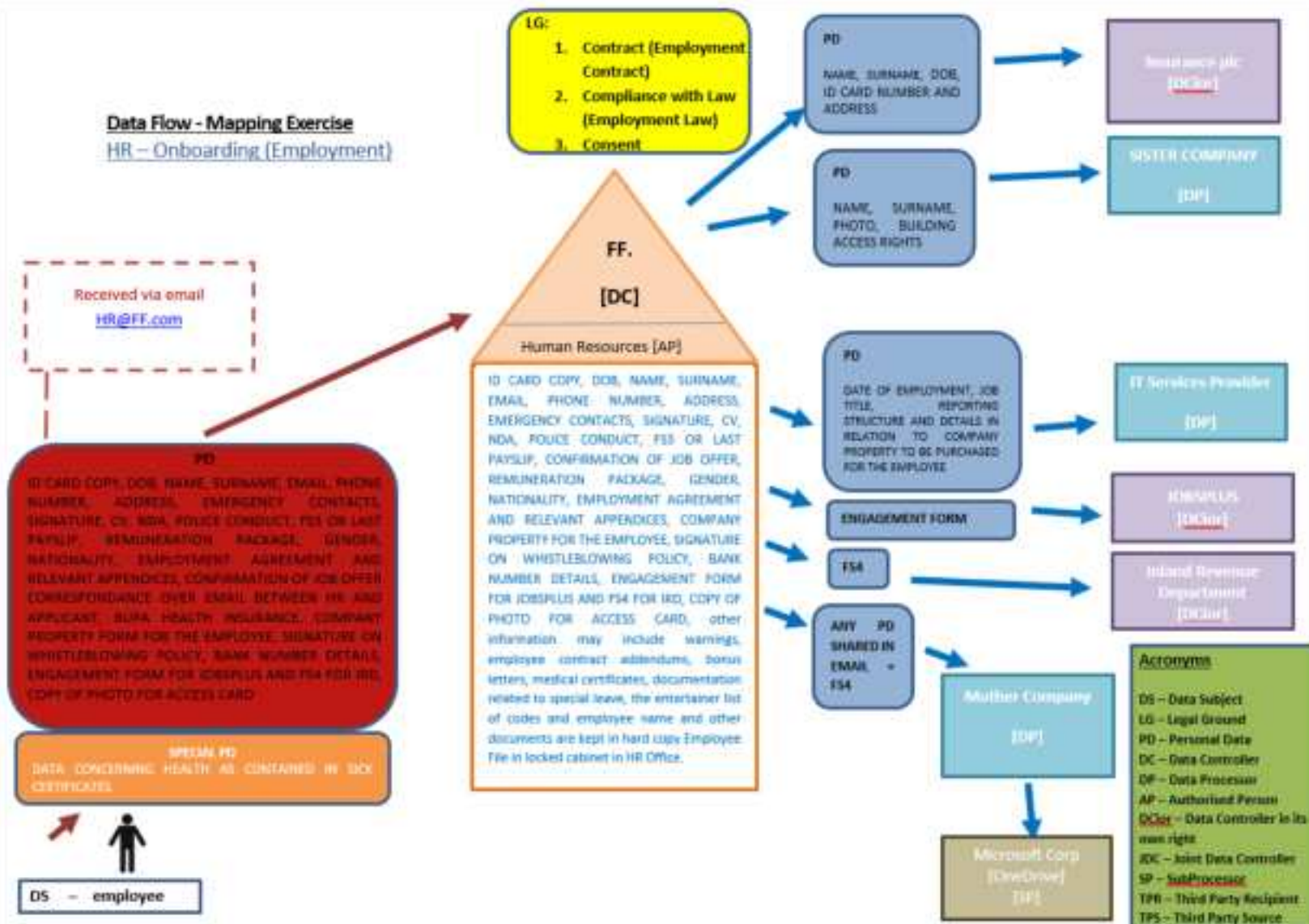


Acronyms

DS - Data Subject
LG - Legal Ground
PD - Personal Data
DC - Data Controller
DP - Data Processor
AP - Authorized Person
DCor - Data Controller in
its own right
JDC - Joint Data Controller
SP - ~~Sub Processor~~
TPR - Third Party
Recipient
TPS - Third Party Source

Data Flow - Mapping Exercise

HR – Onboarding (Employment)



● HOW?

**requires a
structured &
planned approach**



1. Appoint a team + Leader
2. Rope in IT
3. Define a Project Plan
4. Training – understand definitions + your obligations + rights
5. Gather relevant information. (interview / survey individuals + documentation)
6. Prepare a Data Map
7. Consider 'Main Establishment' + Lead Authority



Lead Authority

● HOW?

**requires a
structured &
planned approach**



1. Appoint a team + Leader
2. Rope in IT
3. Define a Project Plan
4. Training – understand definitions + your obligations + rights
5. Gather relevant information. (interview / survey individuals + documentation)
6. Prepare a Data Map
7. Consider 'Main Establishment' + Lead Authority
8. Legal Audit – Gap Analysis Report + Recommendations



● HOW?

requires a
structured &
planned approach



Legal Audit – Gap Analysis Report + Recommendations

A **risk-based approach** to managing data security:

- Understand your organisation's **risk appetite**.
- Understand your **risk environment** (physical (sites and locations, geographies), organisational, technical (digital, technology), services, people (employees, contractors, customers, clients)).
- Understand your organisation's **governance and cybersecurity strategies** to know where data security fits in.
- Assess the **risks inherent in the processing**, taking into account the nature, scope, context and purpose of the processing and the risk of varying likelihood and severity for the rights and freedoms of individuals.
- **Interpret risk** in a way that works for your organisation.
- Controls and measures should be **proportionate** to the risk:
- Identify **measures already in place** to mitigate the risks (these may sit within other parts of the business as part of cybersecurity risk management or physical security protocols).
- **Ensure that any risk mitigations are implemented.**

- **HOW?**
requires a
structured &
planned approach



Legal Audit – Gap Analysis Report +
Recommendations

Consider:

1. **measures** contributing to the **proportionality** and the **necessity** of the processing on the basis of specified, explicit and legitimate purpose(s), lawfulness of processing, adequate, relevant and limited to what is necessary data, and limited storage duration;

and

2. **measures** contributing to the **rights** of the data subject

- **HOW?**
requires a
structured &
planned approach



Legal Audit – Gap Analysis Report +
Recommendations

Consider: **Risks to the rights and freedoms of data subjects.**
& measures envisaged to mitigate.

● HOW?

requires a
structured &
planned approach



1. Appoint a team + Leader
2. Rope in IT
3. Define a Project Plan
4. Training – understand definitions + your obligations + rights
5. Gather relevant information. (interview / survey individuals + documentation)
6. Prepare a Data Map
7. Consider 'Main Establishment' + Lead Authority
8. Legal Audit – Gap Analysis Report + Recommendations
9. Implement Changes





● HOW?

**requires a
structured &
planned approach**

1. Appoint a team + Leader
2. Rope in IT
3. Define a Project Plan
4. Training – understand definitions + your obligations + rights
5. Gather relevant information. (interview / survey individuals + documentation)
6. Prepare a Data Map
7. Consider ‘Main Establishment’ + Lead Authority
8. Legal Audit – Gap Analysis Report + Recommendations
9. Implement Changes
10. Update documentation

● HOW?

**requires a
structured &
planned approach**



1. Appoint a team + Leader
2. Rope in IT
3. Define a Project Plan
4. Training – understand definitions + your obligations + rights
5. Gather relevant information. (interview / survey individuals + documentation)
6. Prepare a Data Map
7. Consider 'Main Establishment' + Lead Authority
8. Legal Audit – Gap Analysis Report + Recommendations
9. Implement Changes
10. Update documentation
11. Train & remind



● HOW?

**requires a
structured &
planned approach**



1. Appoint a team + Leader
2. Rope in IT
3. Define a Project Plan
4. Training – understand definitions + your obligations + rights
5. Gather relevant information. (interview / survey individuals + documentation)
6. Prepare a Data Map
7. Consider 'Main Establishment' + Lead Authority
8. Legal Audit – Gap Analysis Report + Recommendations
9. Implement Changes
10. Update documentation
11. Train & remind
12. Ongoing Compliance



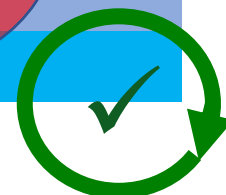


● HOW?

**requires a
structured &
planned approach**



1. Appoint a team + Leader
2. Rope in IT
3. Define a Project Plan
4. Training – understand definitions + your obligations + rights
5. Gather relevant information. (interview / survey individuals + documentation)
6. Prepare a Data MSECURITY
7. Consider 'Main Establishment' + Lead Authority
8. Legal Audit – Gap Analysis Report + Recommendations
9. Implement Changes
10. Update documentation
11. Train & remind
12. Ongoing Compliance



PHYSICAL SECURITY



- the quality of doors and locks, and the **protection of premises** by such means as alarms, security lighting or CCTV;
- **access control** to premises, and how **visitors** are supervised;
- Paper, waste and electronic **disposal**; and
- Security of **IT equipment**, particularly mobile devices

CYBER SECURITY



- **System/network security** – the security of network and information systems, including those which process personal data;
- **data security** – the security of the data held on systems, eg ensuring appropriate access controls are in place and that data is held securely;
- **online security** – eg the security of a website and any other online service or applications used; and
- **device security** – including policies on Bring-your-own-Device (BYOD).

- **Pseudonymisation and encryption are specified in the GDPR as two examples of measures that may be appropriate for you to implement.**
- This does not mean that you are obliged to use these measures. It depends on the nature, scope, context and purposes of your processing, and the risks posed to individuals.

- **ICO Guidance on Privacy Enhancing Technologies : How can PETs help with data protection compliance? | ICO**

PET	Does the PET provide input privacy?	Does the PET provide output privacy?
Homomorphic encryption (HE)	In some cases If processing depends on the encrypted input of two or more parties, HE is not guaranteed to protect these inputs from the owner of the secret key.	No The output may contain personal information. It can be combined with output privacy approaches such as differential privacy.
Secure multiparty computation (SMPC)	Yes	No The output may contain personal information. It can be combined with output privacy approaches such as differential privacy.
Zero-knowledge proofs (ZKPs)	Yes	No It may be possible to learn something about a person, depending on the nature of the query.
Federated learning (FL)	No FL can be combined with other input privacy techniques, such as SMPC and HE.	No FL does not prevent personal information from being shared through the output. It can be combined with output privacy approaches such as differential privacy.
Synthetic data (SD)	No Using synthetic data does not address security risks when managing input data processed as part of the synthetic data generation process.	No Synthetic data does not inherently provide output privacy, but it can be combined with output privacy approaches such as differential privacy.
Trusted Execution Environments (TEEs)	Yes	No TEEs can also deploy output privacy techniques, providing the code executed within them includes specific computations that provide those features.
Differential Privacy (DP)	No DP does not address the security risks when processing input personal information which is highly identifiable (ie before noise is applied that makes it less identifiable). Global DP can be combined with input privacy PETs, such as SMPC, to protect the input personal information between the input sources and the party adding the noise.	Yes

- **ICO Guidance on Privacy Enhancing Technologies : How can PETs help with data protection compliance? | ICO**

Processing activity	PETs which may aid compliance
Processing involving artificial intelligence, machine learning, and deep learning applications	PETs can help you assess and mitigate these risks. For example: homomorphic encryption ensures that only parties with the decryption key can access the information. This protects the information that is being processed (eg to train the AI model); SMPC can protect information sent to global model; differential privacy adds random noise during training to ensure the final model does not memorise information unique to a particular person's personal information; federated learning can minimise the amount of centrally held personal information and reduce the transfer of personal information between parties; and synthetic data can be used at the training stage to reduce the amount of personal information used to train artificial intelligence. Processing activities involving AI may require you to complete a DPIA. For more information, see our DPIA guidance .
Processing involving data matching that means combining, comparing or matching personal information obtained from multiple sources	PETs can help you assess and mitigate these risks. For example: SMPC and PSI can minimise the information shared and protect it during computation Processing activities involving matching information or combining datasets from different sources mean that you must complete a DPIA. For more information, see our DPIA guidance .
Processing involving IoT applications Eg smart technologies (including wearables)	PETs can help you assess and mitigate these risks. For example: Federated learning can be used to train machine learning models on a large number of decentralised IoT devices (eg wearable devices, autonomous vehicles). Depending on the circumstances of the processing, you can also use other PETs, such as SMPC , HE and DP , when you process personal information collected from IoT devices. Processing activities involving IoT may require you to complete a DPIA (eg large-scale processing of health information from wearables). For more information, see our DPIA guidance .
Processing involving data sharing between organisations, particularly data sharing likely to result in a high risk to people	PETs can help you assess and mitigate these risks. For example: SMPC , PSI and FL (when used with other PETs) can minimise the information transferred between parties. HE can enhance security by preventing parties accessing the input information without affecting utility You should carry out a DPIA for data sharing operations. You must do this if sharing it is likely to result in a high risk to people. See our data sharing code for further guidance.
Processing involving cloud computing applications	HE , TEEs and SMPC can be used for cloud computing processing tasks to provide enhanced security.
Processing involving anonymisation of personal information	DP can prevent people from being identified in published information or limit the amount of personal information released from queries. You must ensure that the risk of re-identification is sufficiently remote. Read our guidance on anonymisation for further information.



- [Guidelines 01/2025 on Pseudonymisation | European Data Protection Board](#)

PHYSICAL SECURITY



CYBER SECURITY



3-2-1 Back-up

Three copies, with two stored on different devices and one stored off-site.

- You must have the **ability to restore** the availability and access to personal data in the event of a physical or technical incident in a 'timely manner'.
- The GDPR does not define what a '**timely manner**' means. This depends on:
 - ✓ who you are
 - ✓ what systems you have; and
 - ✓ the risk that may be posed to individuals if the personal data you process is unavailable for a period of time.

Use Firewalls to secure your internet connection

- This effectively creates a 'buffer zone' between your IT network and other, external networks.
- Incoming traffic can be analysed to find out whether or not it should be allowed onto your network.

Choose the most secure settings for your devices and software

- Manufacturers often set the **default configurations** of new software and devices to be as open and multi-functional as possible. They come with 'everything on' to make them easily connectable and usable
- Check Settings. Change Passwords.
- For important accounts, use 2-factor authentication (2FA)

Control who has access to your data and services

- Set admin accounts;
- Check privileges;
- Standard accounts should be used for general work. By ensuring that your staff don't browse the web or check emails from an account with administrative privileges you cut down on the chance that an admin account will be compromised
- only use software from official sources

Protect yourself from viruses and other malware

- Anti-malware measures;
- Whitelisting;
- Sandboxing;

Keep your devices and software up to date

- Look out for & Install 'Patches';
- Operating systems, programmes, phones and apps should all be set to 'automatically update' wherever this is an option;
- Replace unsupported hardware or software;

PHYSICAL SECURITY



CYBER SECURITY



Penetration Testing

- Obligation to carry out '**stress tests**' (vulnerability scanning and penetration testing) of networks and information systems, which are designed to reveal areas of potential risk and things that you can improve.
- ICO : The GDPR now makes this an obligation for all organisations.

E-Mail Security

- Consider whether the content of the email should be encrypted or password protected.
- Make sure you choose the right address before you click send.
- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc).
- If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.

When a processor is involved



- A **data controller is responsible** for ensuring compliance with the GDPR and this includes what the processor does with the data.
- However, in addition to this, the GDPR's **security requirements also apply to any data processor** used.

When a processor is involved

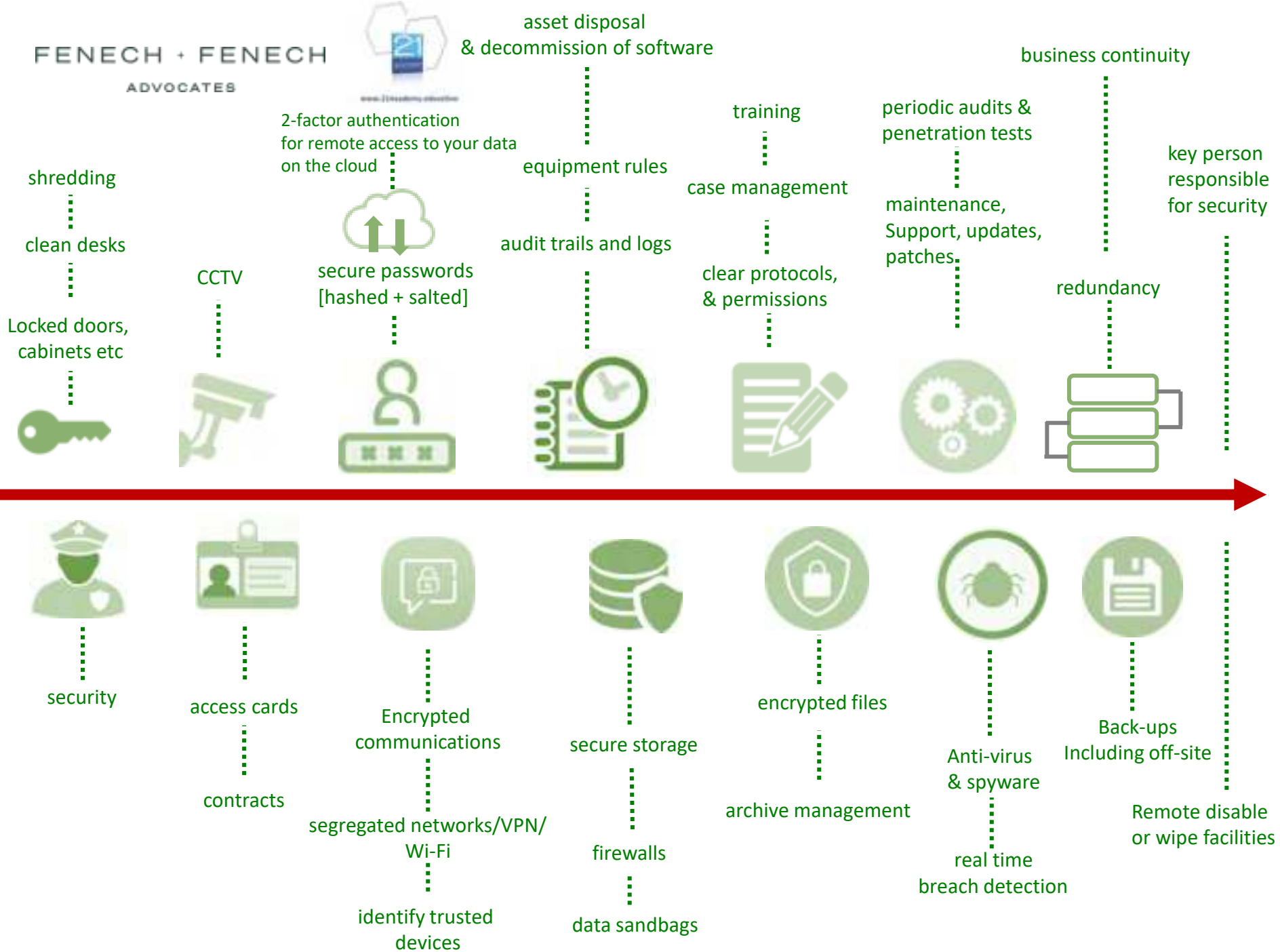


This means that a Controller should :-

- choose a data processor that **provides sufficient guarantees** about its security measures;
- Enter into a **written contract** which stipulates that the processor takes all measures required under Article 32 – basically, the contract has to require the processor to undertake the **same security measures** that you would have to take if you were doing the processing yourself; and
- The contract should includes a requirement that the processor **makes available all information** necessary to demonstrate compliance. This may include allowing for you to **audit and inspect** he processor, either yourself or an authorised third party.

Does your technology :

- ☐ Connect individuals to their personal data ?
- ☐ Categorise personal data by type and processing purposes?
- ☐ Trace the full data life-cycle?
- ☐ Permit search & retrieval?
- ☐ Enable rectification, redaction, erasure and anonymisation?
- ☐ Support process stoppage and suppression?
- ☐ Permit transmission of personal data ?
- ☐ In a secure way?





Training





Training

**Data
Inventory &
Mapping**





Training

**Data
Inventory &
Mapping**



Legal Audit



Training

**Data
Inventory &
Mapping**



Legal Audit

IT Audit





Take this seriously...
Make it an opportunity

Role of the DPO



The DPO role is deemed to be a cornerstone of ‘**accountability**’ a key principle enshrined throughout the GDPR and an obligation imposed upon Data Controllers who are **responsible for, and must be able to demonstrate compliance**, with the 6 Data Protection Principles



When do you need to appoint a DPO?

The appointment of a DPO is mandatory for the following organisations:

- **Public authorities or bodies** (excluding courts whose processing relates to their judicial operations).
- Organisations whose **core activities** involve **regular, systematic and large-scale monitoring** of data subjects.
- Organisations whose core activities consist of the **large-scale processing of special categories of data** or data relating to **criminal convictions** and offences.



Core Activity:

EDPB Guidance suggests that an organisation's core activities are those ***key operations necessary for achieving the organisation's objectives***, but warned against excluding from this definition any activities where the processing of data form an inextricable part of an organisation's activities



Core Activity:

EDPB Guidance gives the example of a **hospital**, whose core business is providing healthcare.

>> As a hospital needs to process patient health data to provide healthcare services safely and effectively, the processing should be considered one of the hospital's core activities, requiring them to appoint a DPO.

Core Activity:



Mere Back-office functions such as payroll administration or general IT support services would not be considered core activities.

Large Scale:

The WP29 Guidance states that it is not possible to define an arbitrary level at which processing becomes "**large-scale**".



It recommends considering the following factors :

- The **number** of data subjects concerned, either as a specific number or as a proportion of the relevant population.
- The **volume of data** and/or the **range** of different data items being processed.
- The **duration, or permanence**, of the data processing activity.
- The **geographical extent** of the processing activity.

Large Scale:

The WP29 Guidance gives the following examples of large scale processing:



1. Processing of travel data of individuals using a city's public transport system (for example, tracking through travel cards).
2. Processing of customer data in the regular course of business by an insurance company or a bank.
3. Processing of personal data for behavioural advertising by a search engine.

Large Scale:

The WP29 Guidance provides two examples that do not constitute large-scale processing:



1. Processing of patient data by an individual physician.
2. Processing of personal data relating to criminal convictions and offences by an individual lawyer.

Systematic

The WP29 Guidance interprets "**systematic**" as meaning one or more of the following:



1. Occurring according to a system.
2. Pre-arranged, organised or methodical.
3. Taking place as part of a general plan for data collection.
4. Carried out as part of a strategy.

Systematic

It also provides examples of "**regular and systematic monitoring of data subjects**", which include:



1. Operating a telecommunications network.
2. Providing telecommunications services.
3. Data-driven marketing services.
4. Profiling and scoring for the purposes of risk assessment (for example, for the purposes of credit scoring, the establishment of insurance premiums, fraud prevention or the detection of money laundering).
5. Location tracking.
6. Loyalty programmes.
7. Connected devices (for example, smart meters, smart cars, home automation and so on).



Both controllers and processors may be required to appoint a DPO.

Conflicts of Interest



The WP29 suggests that in order to avoid conflicts the DPO cannot hold another position within the organisation that involves determining the purposes and means of processing personal data.

Senior management positions such as chief executive, chief financial officer, head of marketing, head of IT or head of human resources are likely to cause conflicts. However, it is not just senior positions that should be considered to be off-limits.



Role of the DPO

Role of the DPO

The DPO shall have the following qualities :

1. A necessary level of **expert knowledge**, which level of knowledge shall be proportionate to the sensitivity, complexity and amount of data processed.
2. Expertise in national and European **data protection laws** and practices and in-depth understanding of the General Data Protection Regulation.
3. Sufficient understanding of the **processing operations** carried out, as well as the information systems, and data protection and **security** needs.
4. Sufficient knowledge of the **rules and procedures**

Role of the DPO

The DPO shall :

1. **inform and advise** on data protection and compliance with applicable law and approved practice, as well as **monitor compliance** with the same;
2. the DPO must collect information to identify processing activities, **analyse and check the compliance** of such activities and issue **recommendations**.
3. advise, inform and issue recommendations on any **Data Protection Impact Assessments (DPIA)**

Role of the DPO

Official guidance recommends that **advice of the DPO should be sought**, on the following issues, amongst others:

1. whether or not to carry out a DPIA;
2. what methodology to follow when carrying out a DPIA;
3. whether to carry out the DPIA in-house or whether to outsource it;
4. **what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects**
5. whether or not the DPIA has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR

The DPO shall give particular importance in the monitoring of compliance in data processing operations in high risk scenarios.

Role of the DPO

The DPO shall contribute to the development and maintenance of all data **protection policies, procedures and processes** in relation to the protection of personal data, in particular via

- the implementation of the principles of data processing,
- data subject rights,
- data protection **by design and by default**,
- records or processing activities,
- **security of processing** and
- notification of data breaches.

Role of the DPO

The DPO shall **allocate responsibilities** internally to ensure continuous compliance with applicable law across all departments/sectors

Role of the DPO

The DPO shall ensure that **training and awareness** sessions are available and delivered to all Employees, in particular to those Employees directly/closely involved in processing operations relating to personal data.

Role of the DPO

The DPO shall develop and provide advice on **procedures for effective security** as well as on the allocation of information security responsibilities.

Role of the DPO

ICO on training :

You should provide appropriate **initial and refresher training**, including:

- your **responsibilities** as a data controller under the GDPR;
- **staff responsibilities** for protecting personal data – including the possibility that they may **commit criminal offences** if they deliberately try to access or disclose these data without authority;
- the **proper procedures**;
- the **dangers of people trying to obtain personal data** by deception (eg by pretending to be the individual whom the data concerns, or enabling staff to recognise ‘phishing’ attacks), or by persuading your staff to alter information when they should not do so; and
- any **restrictions you place on the personal use of your systems** by staff (eg to avoid virus infection or spam).

Handling Data Breaches



Security and Data Breaches



GDPR “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”



Loss of **Confidentiality**

unauthorised or accidental **disclosure** of, or access, to personal data

Loss of **Integrity**

unauthorised or accidental **alteration** of personal data

Loss of **Availability**

accidental or unauthorised loss of **access** to, or **destruction** of personal data



 Send	To...	<u>joe@mitla.org.mt</u>
	Cc...	
	Bcc...	
Subject:		Apologies

Whoops! Sent the attachment to the wrong Joe

Could you please delete it?





Data Breach report



verification



**Likelihood that breach results in
“risk” to privacy of DS**



**File a Data Breach Notification
“without undue delay” and “where
feasible” within 72 hours of being
“aware”**



Likely to result in “high risk”



**Inform the DS
‘without undue delay ‘**

When does a controller become “aware” of a data breach?



Article 29 WP considers the controller as being “aware” when that controller has a **reasonable degree of certainty** that a security incident has occurred that has led to personal data being compromised.

BUT – Controller is expected to have the means and capability to be “aware” of data breaches

Notification to Data Subject



- ☐ The **name and contact** details of the Appointed Person;
- ☐ The likely **consequences** of the Personal Data Breach;
- ☐ **The measures taken** or proposed to be taken by the company to address the Personal Data Breach, including measures to mitigate its possibly adverse effects.
- ☐ **Recommendations** to the Data Subject for measures which they can take to mitigate their risks and/or secure their personal data;

- The notification must be concise, **transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child**. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means
- free of charge

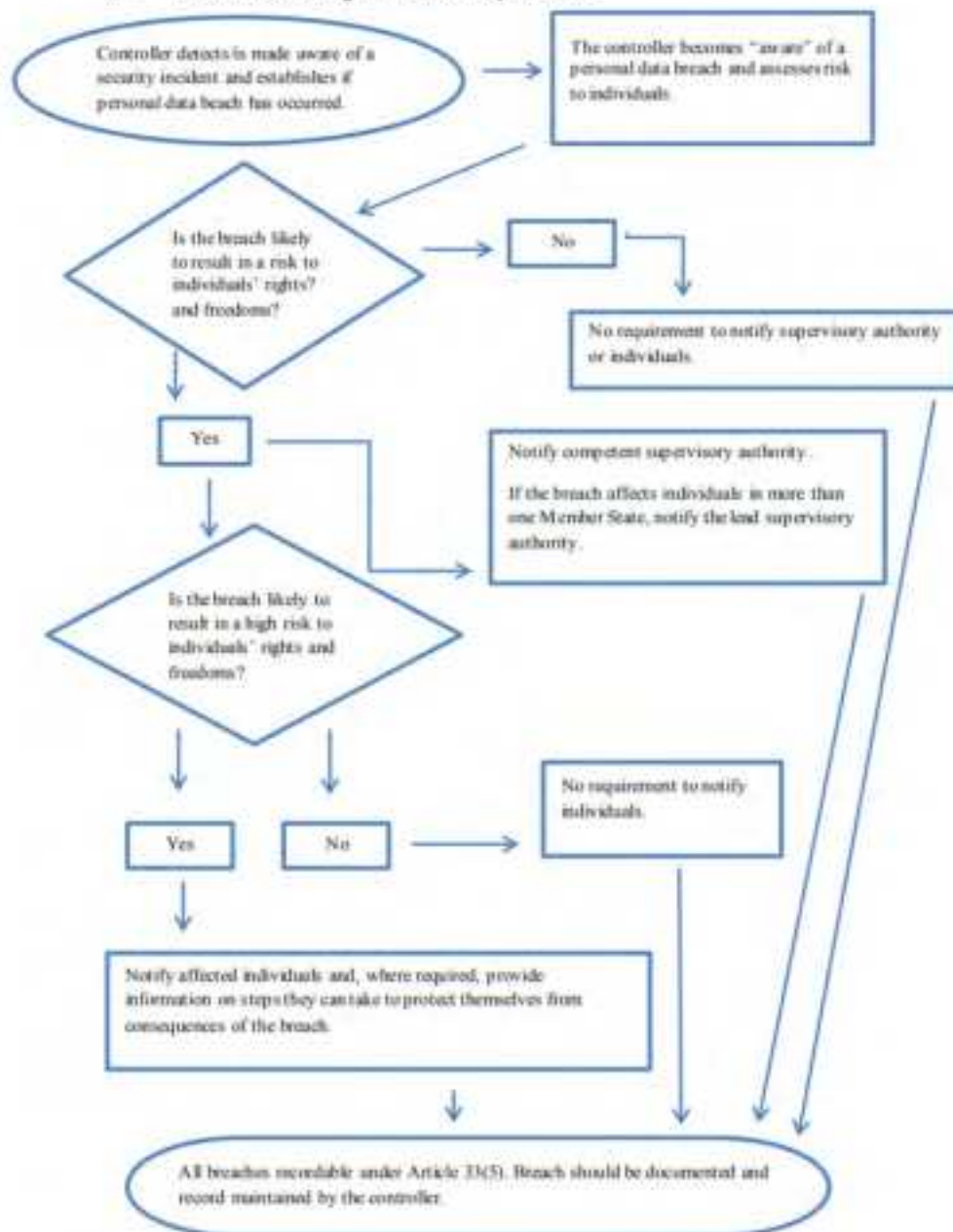
EXCEPTIONS TO NOTIFYING THE D.S.



1. If **appropriate technical and organisational protection measures were implemented**, and those measures were applied to the personal data affected by the Personal Data breach (e.g. encryption)
2. If **subsequent measures** were taken to ensure that the high risk to the rights and freedoms of the impacted data subjects is no longer likely to materialise;
3. The notification to the impacted Data Subjects would involve **disproportionate effort**.

VII. Annex

A. Flowchart showing notification requirements





**You need to
develop,
implement and
maintain a**

**DATA BREACH
PROTOCOL**



1. Who is responsible?
2. What if that person is unavailable?
3. Who will inform the DPO?
4. How fast will you react?
5. How is the level of risk assessed?
6. What remedial action will be taken?
7. What logs will be maintained?



Risk Assessment Criteria

1. **Type of breach**
2. **The nature and sensitivity of the Personal Data Breach**
3. **The volume of personal data in the Personal Data Breach**
4. **The ease of identification of individuals through the Personal Data Breach**
5. **Severity of consequences for impacted individuals**
6. **Whether the Personal Data Breach can be easily contained**
7. **Special Characteristics of the Data Subjects**
8. **The nature of the Data Controller**
9. **The number of affected Data Subjects**



Risk Assessment Criteria

ENISA

European Union Agency for Network and Information Security

4 Levels

LEVEL OF IMPACT	DESCRIPTION
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
Very high	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).



Risk Assessment Criteria

ENISA

European Union Agency for Network and Information Security

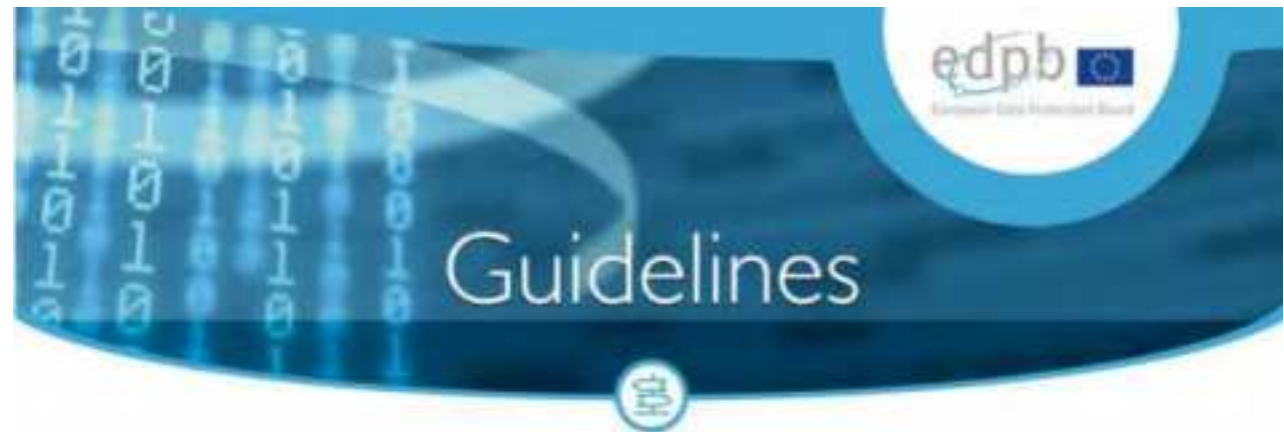
Evaluation of Impact must be **Qualitative**

1. Type of personal data
2. Criticality of the processing operation
3. Volume of the personal data processed
4. Special characteristics of the data controller/processor
5. Special characteristics of the data subjects
6. Identifiability of the data subjects
7. Intelligibility of personal data:



<https://idpc.org.mt/report-a-breach/>
Report a data breach

“IMPORTANT: controllers must carry out a risk assessment to decide whether the security incident poses any risks to the data subject and, as a consequence, whether the breach has to be notified to the Supervisory Authority or otherwise. **For instance, the event of one email sent to one wrong recipient is unlikely to result in a risk to the rights and freedoms of individuals and this Office therefore should NOT BE NOTIFIED.”**



Guidelines 01/2021

on Examples regarding Data Breach Notification

Adopted on 14 January 2021

Version 1.0

**** practice-oriented, case-based guidance***



Guidelines 01/2021
on Examples regarding Data Breach Notification
Adopted on 14 January 2021
Version 1.0



Ransomware with proper backup and No Exfiltration

Vs

Ransomware with NO proper backup

Vs

Ransomware with NO proper backup and Exfiltration



Guidelines 01/2021
on Examples regarding Data Breach Notification
Adopted on 14 January 2021
Version 1.0



Exfiltration by a former employee.

Vs

Accidental Transmission to a Trusted party.

Vs

Stolen Material Storing Encrypted Data

Vs

Stolen Material Storing Non-Encrypted Data

The Costs & Implications of getting GDPR Wrong

The IDPC (or competent authority) is also required to consider the **technical and organisational measures** you had in place when considering an **administrative fine**.

The Costs & Implications of getting GDPR Wrong

Directive
95/46/EC



€23,000



€25,000



€600,000



£500,000

GDPR



**€20 million
Or
4% of global group
turnover**

Whichever is the higher

Fines Pre-GDPR



GET THE MESSAGE?

**Victim of
criminal
offence**



- Boomerang Video - £60,000
- Talk Talk – £400,000

(malware – failure to maintain software and inspect for bugs)



GET THE MESSAGE?

**Genuine
Error**



- NHS - £185,000

(unwilling disclosure of hidden fields)



GET THE MESSAGE?

Abuse



- € 1.1 Million
(monitoring of employee's emails)



GET THE MESSAGE?

Abuse



- € 1.46 Million
(capturing of employee's movements)



GET THE MESSAGE?

**Blatant
Abuse**



**Italy Group of Companies
in total = €11,000,000**

**(abusing customer data for money
Transactions to China)**



Recital 13 – GDPR

The aim is:

*“To provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, **and equivalent sanctions in all Member States***

€20 million

OR

4% of global group turnover



✓ HIGHER POTENTIAL FINES

Art. 29 W.P.: Authorities are encouraged to use a considered and balanced approach ...

BUT “the point is not [to] qualify the fines as a last resort, nor to shy away from issuing fines”



Security

Last year's ICO fines would be 79 times higher under GDPR

TalkTalk's £400,000 penalty was big – how about £59 MILLION?

By John Leyden 29 Apr 2017 at 08:00

29  SHARE 



Fines from the Information Commissioner's Office (ICO) against Brit companies last year would have been £59m rather than £880,500 if the pending General Data Protection Regulation (GDPR) had been applied, according to analysis by NCC Group.

Breach of GDPR



BANK ĊENTRALI TA' MALTA
EUROSISTEMA
CENTRAL BANK OF MALTA

February 2020

- **REPRIMAND from IDPC**
- **Lack of Legal Ground**
- **Data Breach**

Breach of GDPR

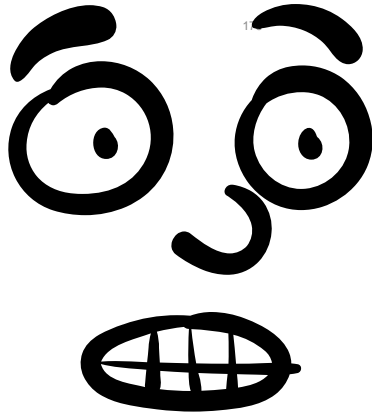


424 0385	SEAN	ZAI	THISTLE
495 0111	MARIA ANTONELLA	ZAI	CANTIK
622 0651	JOSIENNE	ZAI	AMAND
622 0651	JOSIENNE	ZAI	AURORA
488 0395	ANTONIO	ZAI	JOCALA
489 0631	CARMELA	ZAI	JOCALA
968 0477	CLAUDIA	ZAI	21 TA
490 0328	JOSEPH	ZAI	JOCALA
369 0052	JOSEPH MARY	ZAI	21 TA
370 0198	LUKE	ZAI	21 TA
371 0122	MARK	ZAI	21 TA
625 0120	ANTONIA	ZAI	165 SA
337 0046	BRIDGETTE	ZAI	SHAMR
338 0649	CARMEL	ZAI	SHAMR
267 0309	CHANTELLE	ZAI	DERNIS
339 0306	DANIELA	ZAI	SHAMR
286 0541	FRANCIS	ZAI	11 RED
287 0345	GRACIE	ZAI	11 RED
626 0170	JOSEPH	ZAI	290 PL
627 0170	LUCIENNE	ZAI	290 PL

January 2022 – C Planet IT Solutions

- ADMINISTRATIVE FINE from IDPC
€65, 000
- Infringements of Articles 6(1), 9(1), 9(2), 14, 32(1), 5(1)(f), 33(1) and 34(1) GDPR

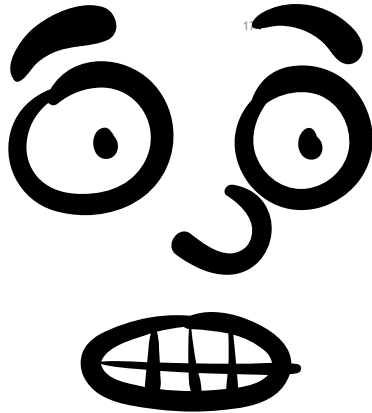
Right of Access



2020

- **€20,000 fine from IDPC**
- **Copy of personal data undergoing processing was only partially provided following a right of access request**

Unsolicited marketing



2020

- **€15,000 fine from IDPC**
- **unsolicited marketing
electronic communications
without consent and for
ignoring a right to object
request**

Breach of GDPR

2022

- **ADMINISTRATIVE FINE from IDPC
€250, 000**
- **Controller infringed principles of security regarding personal data of data subjects and failed to implement appropriate technical and organisational measures**



Decisions

[Home](#) | [Decisions](#)



**Decisions issued by the Information and Data Protection
Commissioner**

**Inadequate Security,
Technical & Organisational
Measures**



December 2019

€320, 000

Inadequate Storage Measures

Inadequate Security, Technical & Organisational Measures



January 2022

€26, 500, 000

**Unlawfully processing users' personal data for
telemarketing purposes**

CCTV Monitoring



April 2019

€36, 800

Data Breach; Policies; Child Data

Inadequate Security, Technical & Organisational Measures

August 2019



- Bulgarian National Revenue Agency fined €2.6 Million

Leakage of personal data in a hacking attack due to inadequate technical and organisational measures to ensure the protection of information security.

Personal data concerning about 6 million persons was illegally accessible.

Inadequate Security, Technical & Organisational Measures



Sept 2025

- The Spanish DPA imposed a fine of EUR 1,500,000 on **SERVICIOS FINANCIEROS CARREFOUR, E.F.C.**
- The controller suffered a cyberattack due to insufficient technical and organisational measures.
- The original fine of EUR 2,500,000 was reduced to EUR 1,500,000 due to immediate payment and admission of responsibility by the controller.

Inadequate Security, Technical & Organisational Measures



October 2025

- The UK DPA imposed a fine of circa £ 14,000,000 (EUR 6,880,000) on CAPITA group.
- CAPITA PENSION SOLUTIONS LIMITED acts as the data processor for the CAPITA Group, which suffered a cyber attack.
- The categories of data exfiltrated from Capita's systems as a result of this Incident were **sensitive**, with a range of special category data being compromised,
- The processor :
 - (i) failed to implement adequate technical and organisational measures to ensure data security and
 - (ii) failed to adequately react to the incident.

Inadequate Security, Technical & Organisational Measures



October 2025

NON-CONFIDENTIAL FOR PUBLICATION

11. Relevant industry standards for Information Security Governance

71. In considering whether the Capita Entities have complied with their obligations under the UK GDPR, the Commissioner has had regard to the relevant industry standards and frameworks, including:

- (i) The National Cyber Security Centre ("**NCSC**") guidance, including NCSC Cyber Essentials;⁵⁵
- (ii) The Centre for Internet Security ("**CIS**") Critical Security Controls ("**CIS Controls**"), and Implementation Group 3 ("**IG3**");^{56, 57, 58}
- (iii) ISO 27001 (Capita is an accredited organisation);
- (iv) National Institute for Standards in Technology Cybersecurity Framework ("**NIST CSF**");⁵⁹ and
- (v) MITRE ATT&CK framework.⁶⁰

IV. THE COMMISSIONER'S FINDINGS OF INFRINGEMENT

Inadequate Security, Technical & Organisational Measures



October 2025

Relevant Industry Standards⁷⁹

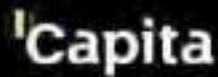
PAM and Active Directory

90. NCSC Guidance on preventing lateral movement, first published on 8 February 2018, recommends implementing a tiering model for administrative accounts to comply with the 'Principle of Least Privilege'.⁷⁴ Specifically:

"The principle of 'least privilege' (where accounts and users have the minimum amount of access needed to perform their role) should be implemented wherever possible. A tiering model for administrative accounts ensures they only have access to the specific administrative capabilities needed, rather than all of them. Using various tiers of administrative accounts limits the number of very high privileged accounts in use, and reduces the access an attacker gains if a lower privilege administrator account is compromised.

*"Accounts with full privilege across an enterprise (such as a domain admin, global admin, or cloud admin account) should **not** normally be used".*

Inadequate Security, Technical & Organisational Measures



Capita

October 2025

Penetration Testing

94. Penetration Testing is an established concept⁹⁴ referred to in the following guidance:

(i) CIS control 18⁹⁵ states that an ISO organisation should have an established and maintained penetration testing program. This includes performing an external penetration test (at least) annually.

(ii) The NCSC has guidance on what an 'ideal' penetration test would look like. This includes the types of testing, the engagement and how they can be used effectively.⁹⁶

(iii) ISO 27001 identifies that organisations should manage technical vulnerabilities and requires organisations to keep an accurate inventory of assets. Relevant aspects of Control 8.8 provide in relation to 'taking appropriate measures to address technical vulnerabilities':

(i) Section (a) states that organisations should 'take appropriate and timely action in response to the identification of potential technical vulnerabilities ...';

(ii) Section (e) requires organisations to 'address systems at high risk first'; and

(iii) Section (f)(ii) states that 'if no update is available ... [organisations should consider] other controls such as: raising awareness of the vulnerability'.

Inadequate Security, Technical & Organisational Measures



October 2025

Costs of implementation

136. The Commissioner understands that the implementation and testing of Active Directory tiering and PAM across a large, multi-domain network such as the Capita network is a complex, potentially costly, and resource-intensive task. Indeed, the Commissioner notes that in its 18 July 2024 response to the Commissioner's queries, Capita provided a copy of its Cyber Transformation Programme 2021 – 2023 which outlined the costs associated with achieving, adopting, and implementing PAM.¹¹⁸

137. Whilst significant, the burden of introducing these measures needs to be balanced alongside the security benefits of implementing tiering, and the significant risks to the rights and freedoms of natural persons of allowing enhanced freedom of movement for threat actors. Furthermore, the Commissioner is mindful of Capita's size and resources, and believes that it is reasonable to expect Capita to go further in keeping its personal data secure than may be expected from a smaller and less well-resourced organisation.

138. The findings made above in respect of the costs of implementation apply to each of the Capita Entities. However, the Commissioner considers that Capita plc bears primary responsibility for the implementation of the appropriate security standards throughout the Capita environment.

Inadequate Security, Technical & Organisational Measures



October 2025

The Italian DPA imposed a fine of EUR 80,000 on the Ospedaleiro-Universitaria Careggi.

- The controller, a university hospital, used software that allowed medical personnel to search through the data subject's history, even if this was unrelated to the specific medical treatment.

Inadequate Security, Technical & Organisational Measures



June 2025

The Greek DPA imposed a fine of EUR 550,000 on Vodafone – PANAFON A.E.E.T.

The controller failed to implement sufficient technical and organisational measures to ensure data security, resulting in a telecommunications shop being able to wrongfully assign multiple SIM cards to an individual.

The controller also failed to use a processor that could guarantee the implementation of sufficient technical and organisational measures, and failed to govern the processing with an adequate data processing agreement.

Inadequate Security, Technical & Organisational Measures



June 2025

The UK DPA imposed a fine of circa **EUR 2,700,000** on 23andMe, Inc

- The controller, a company offering DNA testing to private individuals, failed to implement sufficient technical and organizational measures to ensure data security, especially in regards to the sensitivity of the processed data.
- Between April and September 2023, a hacker carried out a **credential stuffing attack** on 23andMe's platform, exploiting **reused login credentials** that were stolen from previous unrelated data breaches.
- This resulted in the unauthorised access to personal information belonging to 155,592 UK residents, potentially revealing names, birth years, self-reported city or postcode-level location, profile images, race, ethnicity, family trees and health reports. The type and amount of personal information accessed varied depending on the information included in a customer's account.
- ICO found lack of **additional verification steps** for users to access and download their raw genetic data.
- The DPA considered the controller's failure to identify the attack earlier and its failure to adequately inform the DPA about the breach as **aggravating factors**.



Malta Data Protection Act Chapter 586



Malta Data Protection Act

Administrative fines may also be imposed on public authorities

HOWEVER depending on the nature of infringement, the fines on public authorities are capped at €25,000 for each violation and a possible daily fine payment of €25 for each day during which such violation persists or, capped at €50,000 for each violation and a possible daily fine payment of €50 for each day during which such violation persists.



Malta new Data Protection Act

- ☐ Any person who **knowingly provides false information** to the Commissioner **OR does not comply with any lawful request** pursuant to an investigation by the Commissioner, shall be **guilty of an offence**.
- ☐ Conviction shall give rise to a fine (*multa*) of not less than €1,250 up to €50,000 or to imprisonment for 6 months or to both such fine (*multa*) and imprisonment.
- ☐ The Bill also empowers the Minister to enact further provisions on criminal offences.
- ☐ This is what may lead to personal criminal responsibility for officers (directors, company secretary etc.) of a company.



Malta new Data Protection Act

- Data subjects who feel aggrieved may, apart from complaining with the IDPC, institute an action for an **effective judicial remedy** against the controller or processor concerned.
- This could also include the institution of an **action for damages** against the controller or processor who processes personal data in contravention of the provisions of the GDPR.
- If the court finds that the controller or processor is liable for the damage caused, the court shall determine the amount of damages, including, but not limited to, **moral damages** as the court may determine, due to the data subject

And finally...



- 1. Reputational Cost**
- 2. Loss of investment in marketing**
- 3. Loss of share price**

Within 2 days of the breach, TalkTalk shares had dropped by more than 10% followed by further decline to the end of the year.

Any Questions?

