



www.21Academy.education

Data Protection Officer Course - GDPR Compliant



Session 1

Introduction
to the DPO
Role

+

Personal
Data

+

6 Principles

Session 2

Controller
Role

+

Processor
Role

+

Transfers
outside EU

Session 3

Data Subject
Rights

+

Withdrawing
Consent

+

DARs

+ GDPR in
employment

Session 4

DPIAs

+

Policies &
Procedures

+

Auditing

Data Protection Officer Course - GDPR Compliant

Final Session – 27.10.2020

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



**Fenech
& Fenech**
ADVOCATES

sarah.cannataci@fenlex.com

KEY GDPR INGREDIENTS TO COMPLIANCE



KEY GDPR INGREDIENTS TO COMPLIANCE

Grounds



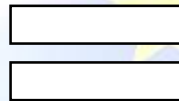
Principles



Rights



Special
Rules



Compliance

KEY GDPR INGREDIENTS TO COMPLIANCE

Grounds



Principles



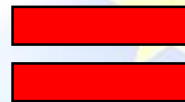
Rights



Special
Rules



SECURITY



Compliance

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



- ☐ This is not a new data protection obligation.
- ☐ It replaces and mirrors the previous requirement to have ‘appropriate technical and organisational measures’ under the Data Protection Act (and EU Directive)

Dealing with IT & Security

➡ GUIDING PRINCIPLES

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



- ❑ BUT, the GDPR provides **more specifics** about what you have to do about the security of your processing and how you should assess your information **risk** and put appropriate **security measures** in place.

What was best practice is now law.

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



CONFIDENTIALITY
INTEGRITY
AVAILABILITY

❑ Security measures put in place should seek to ensure :

1. the data can be accessed, altered, disclosed or deleted only by those you have **authorised** to do so (and that those people only act within the scope of the authority you give them);
2. the data you hold is **accurate and complete** in relation to why you are processing it; and
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 (PIAs)
*are an integral part of taking a
privacy by design & default
approach.*



Impact Assessments

- 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)

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



Fenech
& Fenech
ADVOCATES

Dealing with IT & Security



GDPR Legal & IT/Security Audits

WHY?



HOW?

WHY?



HOW?

WHY?



WHO?





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

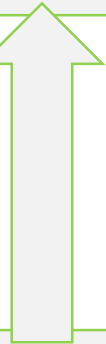
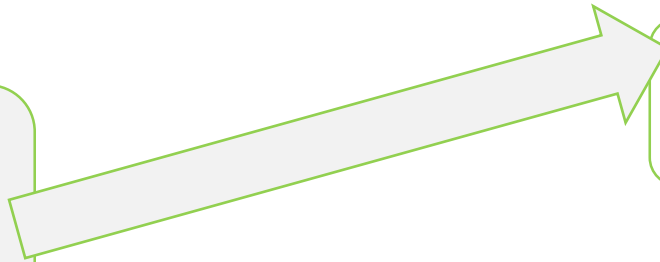
GDPR COMPLIANCE

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.



**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.

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



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.

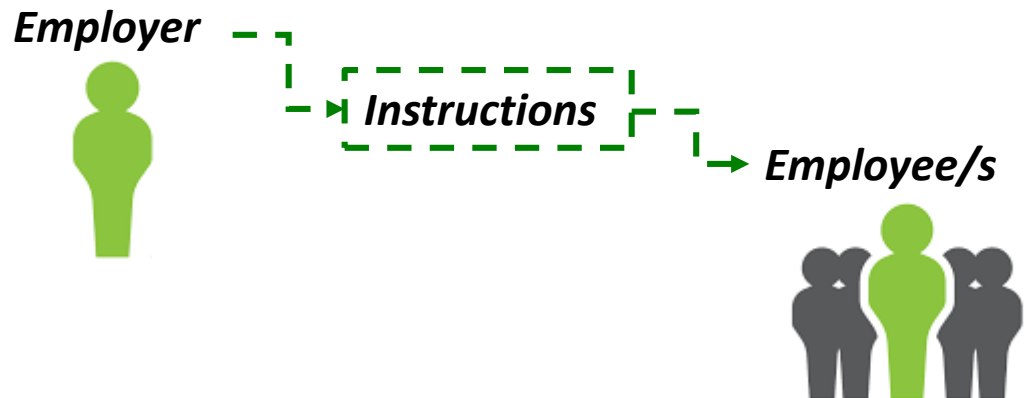
Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes and risk of varying likelihood and severity for the rights of persons...





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,





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**

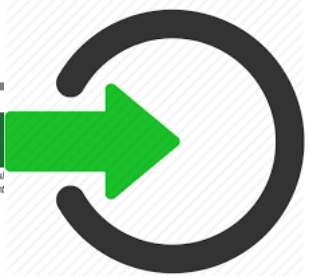




This tool is created by Fenech & Fenech Advocates to facilitate your audit towards achieving GDPR compliance; if you refer to any **documentation/references** whilst populating your responses, please be sure to use a clear reference methodology and provide us with each document referenced accordingly. Where you use multiple please just provide one template. If you use **abbreviations** please insert the abbreviation and full meaning in the Key Definitions section. If you have any questions please contact the firm's lead partner on your audit; This document is a tool and does not represent legal advice. It serves to establish the processing of personal data GDPR will apply as from 25th May 2018. Supervisory authorities are given discretion to regulate certain areas of data protection law, therefore the legislation is expected to develop over time, as will the interpretation thereof by the supervisory authorities and other competent courts.

PERSONAL DATA INVENTORY

towards GDPR compliance



PROCESSING ACTIVITIES FOR YOUR DEPARTMENT

(PLEASE COMPLETE ONE PER PROCESS (OR SET OF RELATED PROCESSES) CARRIED OUT BY YOUR DEPARTMENT)

1. NAME OF PLATFORM/SYSTEM (insert name, if any)	ENTITY NAME DEPARTMENT NAME PLATFORM/SYSTEM/PROCESSING ACTIVITY NAME OR REFERENCE	Click or tap here to enter text. Click or tap here to enter text. Click or tap here to enter text.	FOR FF USE	FOR FF USE														
2. Insert MAIN PURPOSE/S for which the personal data was initially collected.	<ul style="list-style-type: none">• Purpose Title: (please provide a title E.g. #1:Recruitment CV Data• Personal Data & Purpose Description (e.g. processing of name, surname, tel. no, email address + work history + studies + age, provided on CV, for recruitment purposes, carried out manually/electronically using the system known as ABC);	Click or tap here to enter text. PLEASE DESCRIBE PROCESS (OR SET OF PROCESSES) IN DETAIL Click or tap here to enter text.	FOR FF USE	FOR FF USE														
3. What ROLE does your Department have in the processing of the Personal Data using the platform/system referred to in the prior TAB?	<table><tr><td>Data Controller</td><td><input type="checkbox"/></td><td></td></tr><tr><td>Joint Data Controller</td><td><input type="checkbox"/></td><td>if so, specify joint Controller : Click or tap here to enter text. Is it regulated by a Joint Controller-Agreement? (please tick) YES <input type="checkbox"/> NO <input type="checkbox"/> If YES please provide reference : Click or tap here to enter text.</td></tr><tr><td>Data Processor</td><td><input type="checkbox"/></td><td>if so, specify Controller : Click or tap here to enter text. Is it regulated by a Processing Agreement? (please tick) YES <input type="checkbox"/> NO <input type="checkbox"/> If YES please provide reference : Click or tap here to enter text.</td></tr><tr><td>Sub-Processor</td><td><input type="checkbox"/></td><td>if so, specify Controller : Click or tap here to enter text. Is it regulated by a Processing Agreement? (please tick) YES <input type="checkbox"/> NO <input type="checkbox"/> If YES please provide reference : Click or tap here to enter text.</td></tr><tr><td>Other Comments</td><td colspan="2">Click or tap here to enter text.</td></tr></table>	Data Controller	<input type="checkbox"/>		Joint Data Controller	<input type="checkbox"/>	if so, specify joint Controller : Click or tap here to enter text. Is it regulated by a Joint Controller-Agreement? (please tick) YES <input type="checkbox"/> NO <input type="checkbox"/> If YES please provide reference : Click or tap here to enter text.	Data Processor	<input type="checkbox"/>	if so, specify Controller : Click or tap here to enter text. Is it regulated by a Processing Agreement? (please tick) YES <input type="checkbox"/> NO <input type="checkbox"/> If YES please provide reference : Click or tap here to enter text.	Sub-Processor	<input type="checkbox"/>	if so, specify Controller : Click or tap here to enter text. Is it regulated by a Processing Agreement? (please tick) YES <input type="checkbox"/> NO <input type="checkbox"/> If YES please provide reference : Click or tap here to enter text.	Other Comments	Click or tap here to enter text.		FOR FF USE	FOR FF USE
Data Controller	<input type="checkbox"/>																	
Joint Data Controller	<input type="checkbox"/>	if so, specify joint Controller : Click or tap here to enter text. Is it regulated by a Joint Controller-Agreement? (please tick) YES <input type="checkbox"/> NO <input type="checkbox"/> If YES please provide reference : Click or tap here to enter text.																
Data Processor	<input type="checkbox"/>	if so, specify Controller : Click or tap here to enter text. Is it regulated by a Processing Agreement? (please tick) YES <input type="checkbox"/> NO <input type="checkbox"/> If YES please provide reference : Click or tap here to enter text.																
Sub-Processor	<input type="checkbox"/>	if so, specify Controller : Click or tap here to enter text. Is it regulated by a Processing Agreement? (please tick) YES <input type="checkbox"/> NO <input type="checkbox"/> If YES please provide reference : Click or tap here to enter text.																
Other Comments	Click or tap here to enter text.																	
4. Who takes DECISIONS about the personal data being processed?	<table><tr><td>At the level of your Department</td><td><input type="checkbox"/></td><td>Other: Click or tap here to enter text.</td></tr><tr><td>at Entity level</td><td><input type="checkbox"/></td><td></td></tr><tr><td>at Group level</td><td><input type="checkbox"/></td><td></td></tr></table>	At the level of your Department	<input type="checkbox"/>	Other: Click or tap here to enter text.	at Entity level	<input type="checkbox"/>		at Group level	<input type="checkbox"/>		FOR FF USE	FOR FF USE						
At the level of your Department	<input type="checkbox"/>	Other: Click or tap here to enter text.																
at Entity level	<input type="checkbox"/>																	
at Group level	<input type="checkbox"/>																	
5. WHERE is the "personal data" being processed.	EU/EEA <input type="checkbox"/> or NON-EU/EEA <input type="checkbox"/> or in both the EU and in NON-EU/EEA <input type="checkbox"/> Other Comments : Click or tap here to enter text.	FOR FF USE	FOR FF USE															
6. If the processing is not based in the EU/EEA, is the processing being carried out in the context of processing	(i) Offering of goods or services, irrespective of whether a payment is required, to Data Subjects in the EU? YES <input type="checkbox"/> NO <input type="checkbox"/> (ii) Monitoring of behaviour (as far as behaviour takes place within the Union) of Data Subjects in the EU? YES <input type="checkbox"/> NO <input type="checkbox"/> Other Comments : Click or tap here to enter text. If the answer to (i) or (ii) is YES ... does your department have a designated representative in an EU Member State? * YES <input type="checkbox"/> NO <input type="checkbox"/> If yes please specify who : Click or tap	FOR FF USE	FOR FF USE															



DATA INVENTORY FORM

25 Sections per process



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

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)

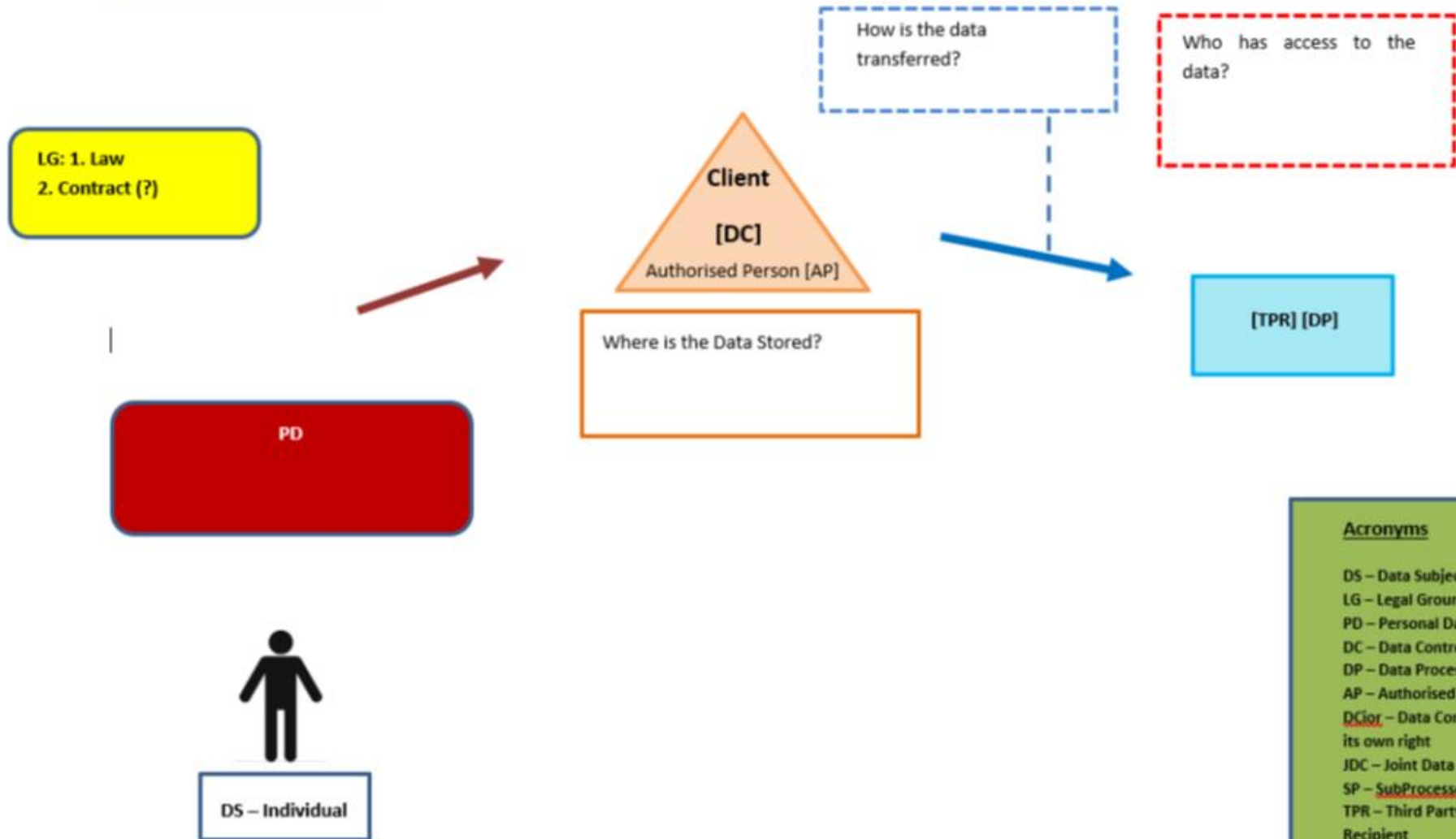
4. LOCATIONS

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



Data Flow - Mapping Exercise

CODE – Entity – PROCESS

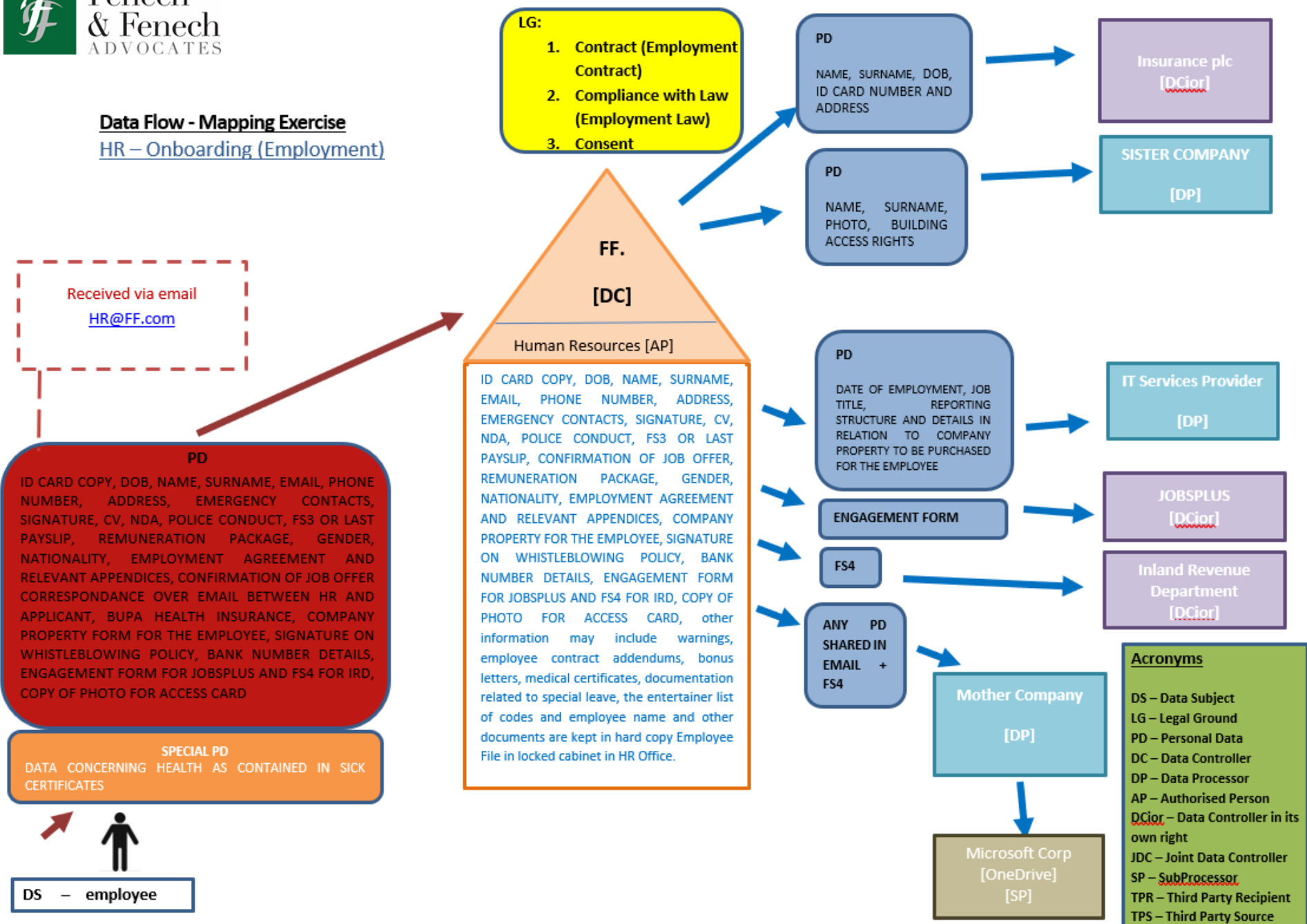


Acronyms

DS – Data Subject
 LG – Legal Ground
 PD – Personal Data
 DC – Data Controller
 DP – Data Processor
 AP – Authorised Person
 DC_{ior} – Data Controller in its own right
 JDC – Joint Data Controller
 SP – SubProcessor
 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



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

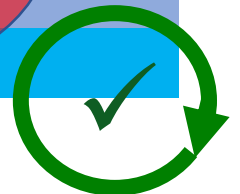


HOW?

- 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).

PHYSICAL SECURITY



CYBER SECURITY



- **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.

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.

PHYSICAL SECURITY



CYBER SECURITY



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.

PHYSICAL SECURITY



CYBER SECURITY



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)

PHYSICAL SECURITY



CYBER SECURITY



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

PHYSICAL SECURITY



CYBER SECURITY



Protect yourself from viruses and other malware

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

PHYSICAL SECURITY



CYBER SECURITY



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.

PHYSICAL SECURITY



CYBER SECURITY



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** the 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?



shredding

clean desks

Locked doors,
cabinets etc



CCTV



2-factor authentication
for remote access to
your data on the cloud



secure passwords
[hashed + salted]



asset disposal
& decommission of software

equipment rules

audit trails and logs



training
case management

clear protocols,
& permissions



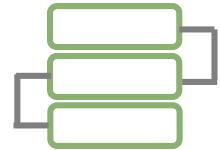
periodic audits &
penetration tests

maintenance,
Support, updates,
patches



business continuity

redundancy



key person
responsible
for security



security



access cards

contracts



Encrypted
communications

segregated networks/VPN/
Wi-Fi

identify trusted
devices



secure storage

firewalls

data sandbags



encrypted files

archive management



Anti-virus
& spyware

real time
breach detection



Back-ups
Including off-site

Remote disable
or wipe facilities



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

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 to identify callers**;
- 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...	joe@mitla.org.mt
	Cc...	
	Bcc...	
Subject		Apologies
<p>Whoops! Sent the attachment to the wrong Joe</p> <p>Could you please delete it?</p>		





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

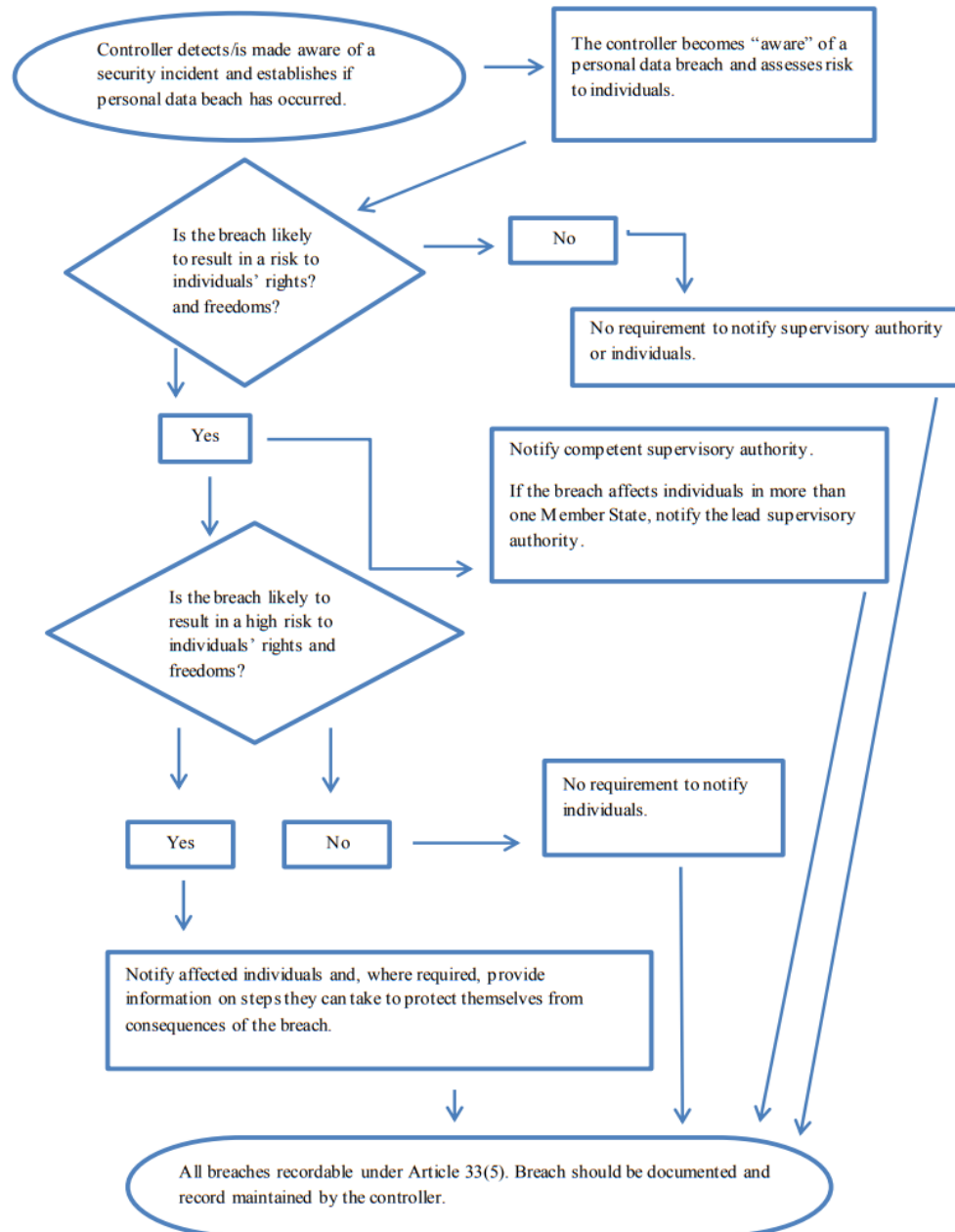
EXCEPTIONS TO NOTIFYING THE D.S.



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:**

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



€23,000



€25,000



€600,000



£500,000



€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**



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

**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 28 Apr 2017 at 08:03

29 SHARE ▼



Fines from the Information Commissioner's Office (ICO) against Brit companies last year would have been £69m 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**

**Inadequate Security,
Technical & Organisational
Measures**



April 2020

€50, 000

DPO Conflict of Interest

**Inadequate Security,
Technical & Organisational
Measures**



December 2019

€320, 000

Inadequate Storage Measures

CCTV Monitoring



April 2019

€36, 800

Data Breach; Policies; Child Data



GET THE MESSAGE?

**Terms and
Conditions of
Use**



- **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. It was found that personal data concerning about 6 million persons was illegally accessible.



Malta new Data Protection Act Chapter 586



Malta new 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?



Case Study 1

Denis has been an employee with the Company for just under six (6) months. This is his first job after having successfully completed his studies at University. Upon starting his new job, Denis is trained on how to use the new software he will be spending the majority of his day on. He is informed by HR that the Company has several policies including an HR policy and a bulky Information Security Policy. Denis is advised to go through both policies and to familiarise himself with them. Denis is also informed that throughout the year he will be attending some internal sessions related to these policies and their practical use within the work place. Denis never really reads through the policies as he deems them to be lengthy and a waste of time, apart from the fact that he believes that as long as he does a good job he will never have to resort to them. As the months go by, Denis excels in his new role and is a key player within his new team, so much so that upon the expiry of his probation he is given a raise and is praised by his team lead in a one on one meeting held a few days after his six (6) month mark.

It's a Friday, and Denis just can't wait to start off his weekend. He schedules an onsite meeting at a client for 3pm, with the aim of wrapping up by 4:30pm and making his way home. Denis needs to take several things with him for his meeting, including his work laptop, a pen drive containing marketing material, and a proposal which he, along with his colleagues prepared in relation to the services being offered to the client. He also has a box file filled with printed material which contains some contracts and supporting documentation which need to be signed off by the client.

Denis arrives for his meeting on time and settles into a boardroom. He connects to the open access wi-fi from his laptop and inserts the pen drive into his laptop. He copies the information onto his laptop desktop for easy access, removes the pen drive and hands it over to one of the secretaries and tells her to pass it on to Mr. Borg's PA, as Mr. Borg could not make the meeting. He tells the secretary that Mr. Borg can keep the pen drive as it is his own, not the Company's.

Denis finishes off his presentation and the meeting goes smoothly. He gets up to leave, when he is asked by one of his clients about the documents which he was supposed to bring along. Denis looks around and realises that the box file is nowhere to be seen. Denis keeps his cool and tells the client that he must have left them at the office on his way out and will drop them off on Monday. He walks down into the lobby of the building, which is shared by several other companies utilising the office block, he takes a quick glance at the area where he had been waiting and the box file is nowhere to be seen. He thinks to himself that it must be in his car, he checks his car, and again the box file isn't there. Denis is certain that he had the box file with him as he remembered carrying it out of the car as he approached the building.

Denis begins to worry, but thinks to himself, it's 5pm on a Friday, this can wait till Monday morning. Denis remembers that he has copies of all the contracts on his laptop anyway and that he can just reprint everything on Monday morning.

Case Study 2

Paul has been an employee of the Company for many years. Paul deals with customers on a daily basis and is praised by both customers and colleagues for his can-do attitude and his work ethic. Admittedly, Paul's IT knowledge is limited, and apart from browsing the web and sending and receiving emails, he doesn't really do anything else. Seeing as Paul visits clients often, he has access to his emails on his mobile phone too.

The month of December is a busy one for Paul, he's finalising several projects and seeing to customers' needs as year end approaches. One morning, Paul is a little bit overwhelmed by the several calls and emails which he is receiving. Two of his colleagues have called in sick, and a customer is anxious about the completion of a project and has already called Paul three (3) times that morning. Paul writes an email to one of his customers, in it Paul attaches the updated rates for 2019, previous correspondence with the client relating to products and consignments, and scanned ID cards of the Directors of the company/customer he is corresponding with. Paul has attached the scanned copies in order to confirm that the details are still correct since they hadn't been updated in a while, and because of GDPR everyone keeps telling Paul that data has to be accurate.

Paul finalizes the email and is inputting the recipient details. He receives another phone call (number four (4)) from the same customer who has been harassing him all morning, flustered Paul inputs the recipient details and clicks send. In the meantime, Paul receives an email. It goes to his junk folder, but it seems to be coming from one of his regular customers. He drags it into his inbox and opens it. He clicks on the link which prompts him to input his login details as it says the system has logged him out. Paul inputs his details and his laptop freezes. He has an old laptop, so Paul is not shocked by this at all. He does a hard restart, switches his laptop back on and goes back to work.

The following morning Paul receives a call from John West. John asks Paul whether he will be sending the info re the 2019 rates any time soon and whether he had had any time to sift through his previous emails. Paul is confused as he had already sent an email the previous day. He goes onto his sent items folder and realises that he had sent the email to John Snow and not to John West. Paul forwards the email and its contents to John West and considers the matter closed.

After lunch, Paul starts wondering why he had not yet received any emails that day. He checks that his ethernet cable is correctly connected into his laptop and restarts his laptop. When this doesn't seem to fix the problem, he calls the IT department. Upon examining the issue, the IT team figure out what Paul had done the previous day and that all emails being sent to him were being diverted onto another email account.

CONCLUSION – SECURITY IN BRIEF (ICO)

- ❑ personal data must be processed securely by means of ‘appropriate technical and organisational measures’ – this is the ‘**security principle**’.
- ❑ Doing this requires you to consider things **like risk analysis, organisational policies, and physical and technical measures**.
- ❑ You also have to take into account additional requirements about the security of your processing – and these **also apply to data processors**.
- ❑ You can consider the **state of the art and costs** of implementation when deciding what measures to take – but they must be appropriate both to your circumstances and the risk your processing poses.

CONCLUSION – SECURITY IN BRIEF (ICO)

- ☐ Where appropriate, you should look to use measures such as **pseudonymisation and encryption**.
- ☐ Your measures must ensure the '**confidentiality, integrity and availability**' of your systems and services and the personal data you process within them.
- ☐ The measures must also enable you to **restore access and availability** to personal data in a timely manner in the event of a physical or technical incident – **Business Continuity**.
- ☐ You also need to ensure that you have appropriate processes in place to **test the effectiveness of your measures, and undertake any required improvements**.

CONCLUSION – SECURITY IN BRIEF (ICO)

- ☐ Carrying out an **information risk assessment** is one example of an organisational measure, but you will need to take other measures as well.
- ☐ You should aim to build a **culture of security awareness** within your organisation.
- ☐ You should **identify a person with day-to-day responsibility for information security** within your organisation
- ☐ make sure this person has the **appropriate resources and authority** to do their job effectively

Questions?

sarah.cannataci@fenlex.com





www.21Academy.education