

Data Protection Officers /Lead – GDPR Compliance

21 Academy



CAMILLERI PREZIOSI
ADVOCATES



Breakdown of today's session

1. Legal requirements surrounding Data Protection Impact Assessments
("DPIAs")

2. How to conduct a DPIA

3. Policies and Procedures

4. Auditing





The GDPR – A Risk-Based Regulation





Privacy by Design and Privacy by Default

- To promote compliance with data protection laws and regulations from the earliest stages of initiatives involving personal data
- Privacy as a fundamental component in the design and maintenance of information systems and mode of operation for each organisation



Privacy by Design and Privacy by Default

by design measures may include e.g. pseudonymisation or other privacy-enhancing technologies

by default measures ensure that only personal data which is necessary for each specific purpose is processed e.g. privacy settings should, by default, be set on the most privacy-friendly setting



Privacy by Design – Article 25 GDPR

*Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, **both at the time of the determination of the means for processing and at the time of the processing itself**, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate safeguards into the processing to meet requirements of GDPR and protect the rights of data subjects.*





Privacy by Design – Article 25 GDPR

privacy by design = conducting DPIAs

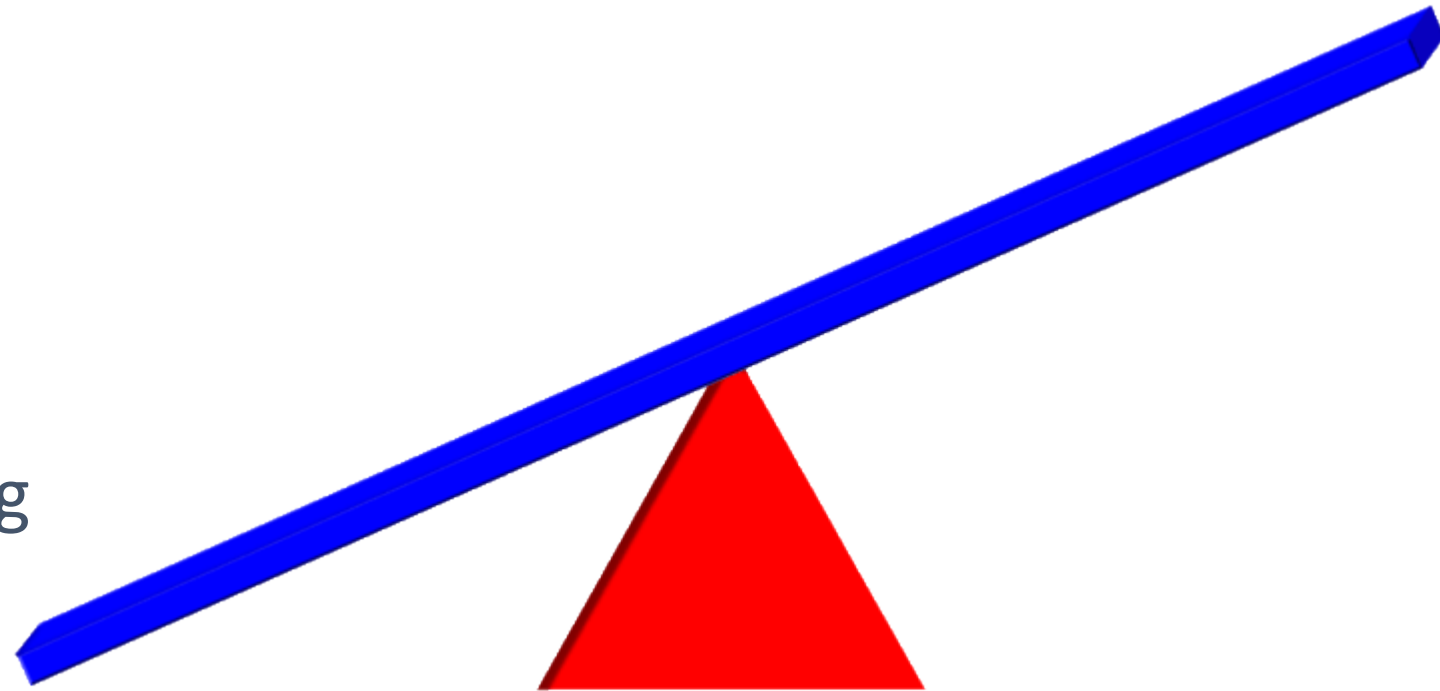
A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.



A Balancing Act

Rights and
Freedoms of Data
Subjects

Processing
Activities





What is a DPIA?

1. Describe the processing
2. Assess its necessity and
3. Manage risks





Article 35 GDPR

Section 3

Data protection impact assessment and prior consultation

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.
3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
 - (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
 - (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
 - (c) a systematic monitoring of a publicly accessible area on a large scale.
4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.





Article 35 GDPR

-
7. The assessment shall contain at least:
- (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
 - (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
 - (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
 - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.
9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.
10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.
11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.





When is a DPIA required?

- Processing is “likely to result in a high risk to the rights and freedoms of natural persons”
- Note the “in particular using new tech” in Art 35(1)
- Good practice to carry out a DPIA for any major project which requires the processing of personal data or where it is evident that the processing operations are not able to satisfy the GDPR.



IDPC Requirements for DPIA

- Systematic Monitoring
- Automated Decisions
- Use of Innovative Technologies
- Special Categories of Data
- Biometric Data
- Genetic Data
- Data Concerning Vulnerable Persons
- Employee Monitoring



Timing: Conducting a DPIA?

To be carried out **prior** to the initiation of the processing activity.

(e.g. prior to the use of CCTV)





What should a DPIA address?

Either:

A set of similar processing operations

e.g. public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application

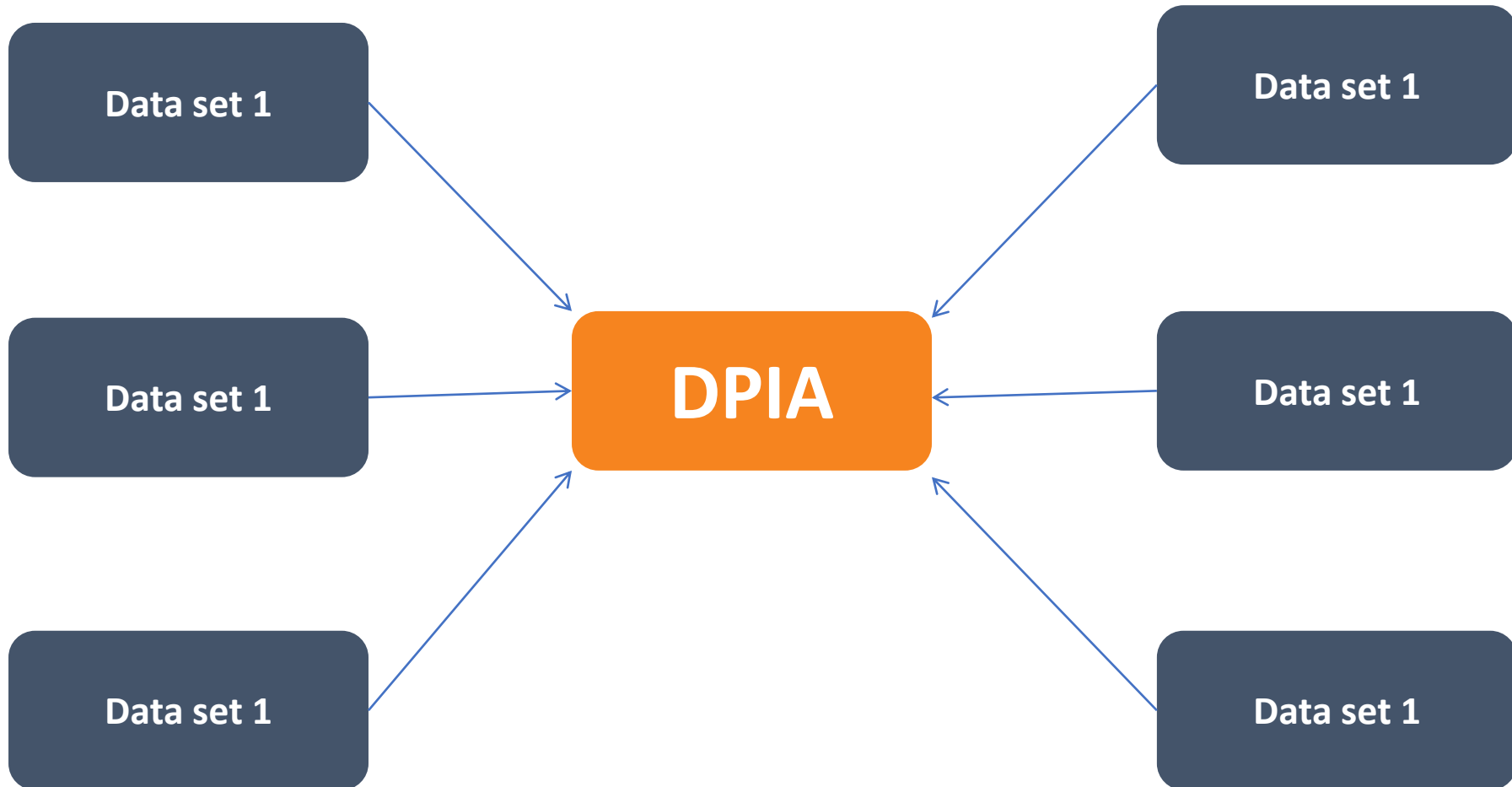
Or:

A single processing operation

e.g. introduction of CCTV

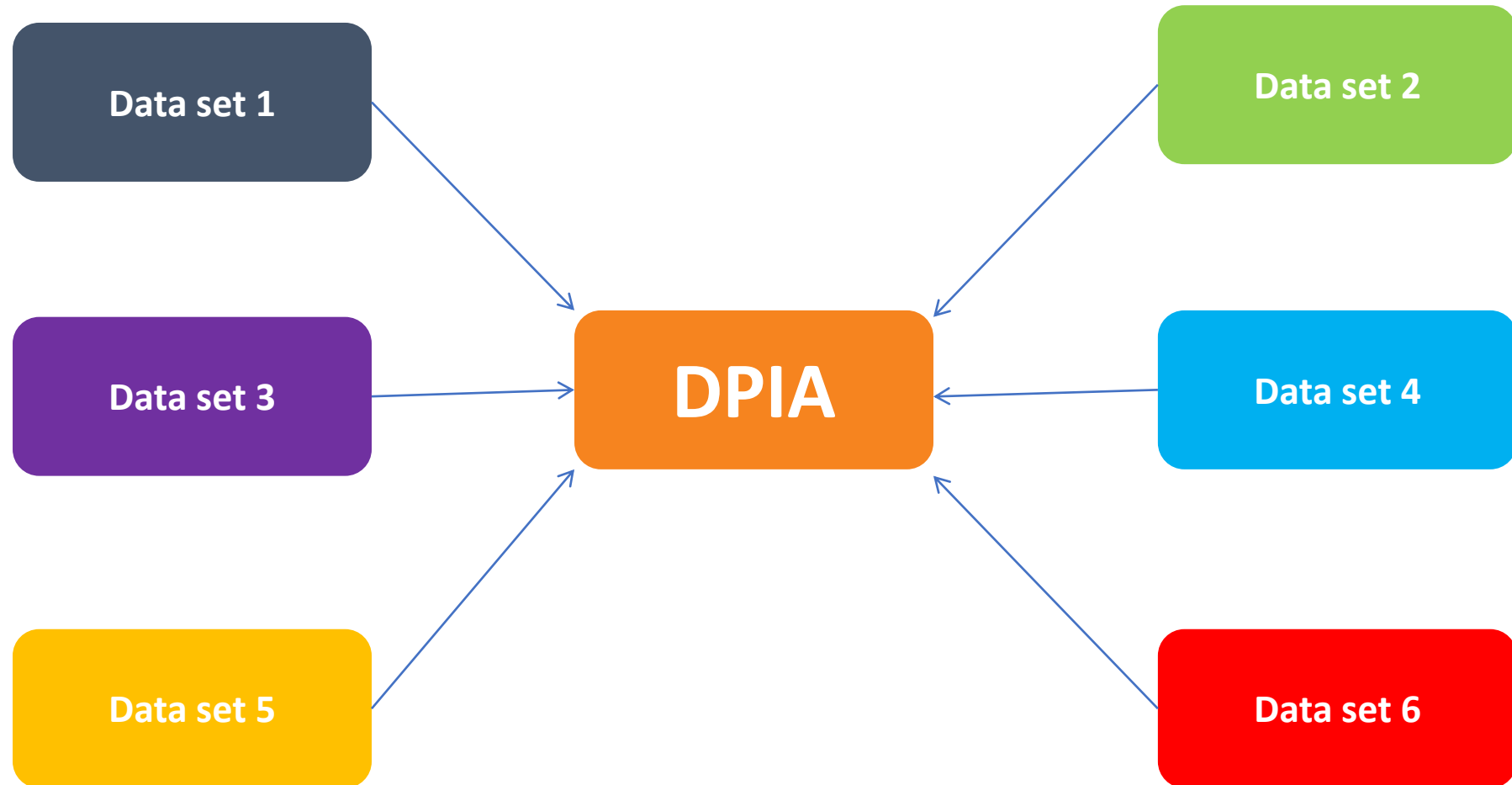


DPIA – Single Processing





DPIA – Multiple Processing

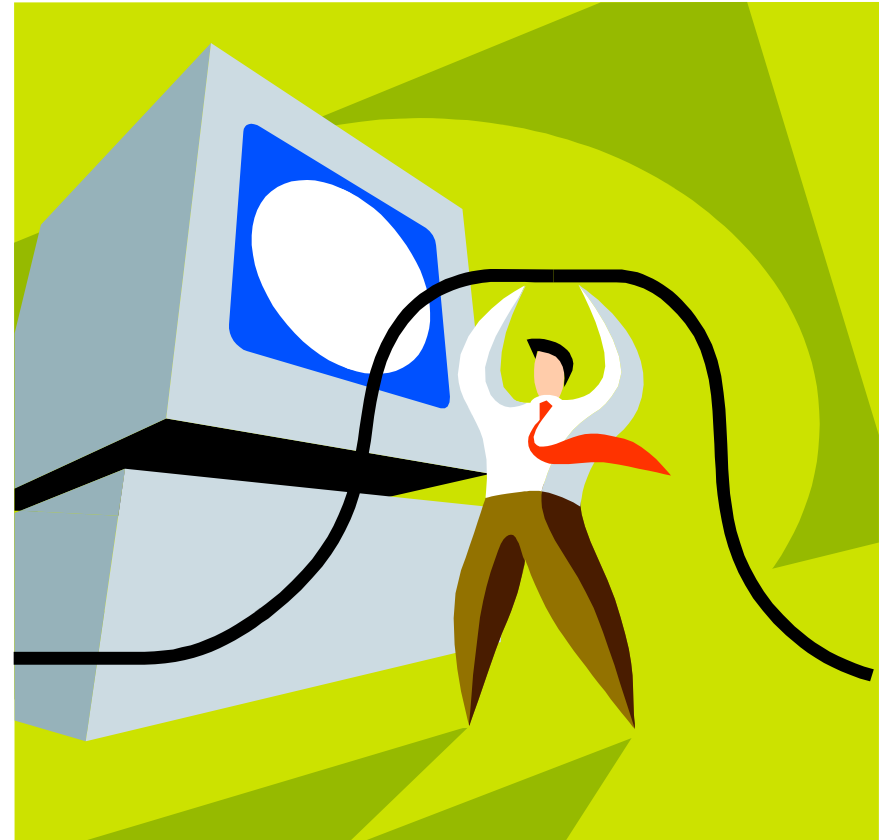




Who is obliged to carry out a DPIA?



Data Controller



Data Processor





Article 35 of the GDPR

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks

Article 5 of the GDPR

“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).”



Who is the Data Controller ?

An entity which, alone or together with at least another entity, determines the purposes and means of the processing of personal data

Data Controller



Personal Data

Data Subject



DPO Involvement



Data Protection Officer

Data Controller



DPO Involvement

Art 35(2) GDPR

The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.





Data Subject Involvement

Art 35(9) GDPR

Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.



Processor Involvement

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

- (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
- (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- (c) takes all measures required pursuant to Article 32;
- (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
- (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
- (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
- (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
- (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.





When is a DPIA mandatory?

Processing is likely to result in a **high risk** to the rights and freedoms of natural persons



HIGH RISKS



Art 35(3) GDPR

1. Systematic and extensive evaluation based on automated processing (including profiling)
2. Processing on a large scale of special categories or of personal data relating to certain criminal convictions and offences
3. A systematic monitoring of a publicly accessible area on a large scale





Systematic Monitoring

- Processing used to observe, monitor or control data subjects, including data collected through networks or “a systematic monitoring of a publicly accessible area” (Article 35(3)(c)).
- This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s).





Automated Decision Making

- Includes '*profiling*' – Article 22 GDPR

means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

- On which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person

such as automatic refusal of an online credit application or e-recruiting practices without any human intervention (recital 71).



Large Scale Processing: Special Categories of Data



- This includes for example information about individuals' political opinions, as well as personal data relating to criminal convictions or offences as defined in Article 10.
- An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details.
- Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals. These personal data are considered as sensitive because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud).
- This criterion may also include data such as personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications.



Monitoring of Publicly Accessible Areas on a Large Scale



- The GDPR does not define what constitutes large-scale, though recital 91 provides some guidance.
- In any event, the EDPB recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:
 - a) the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
 - b) the volume of data and/or the range of different data items being processed;
 - c) the duration, or permanence, of the data processing activity;
 - d) the geographical extent of the processing activity.





WP 29 Guidelines

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

WP 29 also set out **9 criteria** to be considered in order to provide a more concrete set of processing operations that require a DPIA



**Evaluation or
scoring**

**Automated-
decision making
with legal
significant effect**

**Systematic
Monitoring**

Sensitive Data

**Data Processed on
a large scale**

**Matching or
combining
datasets**

**Data concerning
vulnerable data
subjects**

**Innovative
organisational
solutions**

**Processing prevent
data subjects from
exercising their
rights**



Matching or Combining Datasets

For example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.

Evaluation or Scoring

- Including profiling and predicting, especially from “aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements” (recitals 71 and 91).
- Examples of this could include a financial institution that screens its customers against a credit reference database or against an anti-money laundering and counter-terrorist financing (AML/CTF) or fraud database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioural or marketing profiles based on usage or navigation on its website.



Examples of processing	Possible Relevant criteria	DPIA likely to be required?
A hospital processing its patients' genetic and health data (hospital information system).	<ul style="list-style-type: none"> - <u>Sensitive data or data of a highly personal nature.</u> - Data concerning vulnerable data subjects. - Data processed on a large-scale. 	Yes
The use of a camera system to monitor driving behavior on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates.	<ul style="list-style-type: none"> - Systematic monitoring. - Innovative use or applying technological or organisational solutions. 	
A company systematically monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, <i>etc.</i>	<ul style="list-style-type: none"> - Systematic monitoring. - Data concerning vulnerable data subjects. 	
The gathering of public social media data for generating profiles.	<ul style="list-style-type: none"> - Evaluation or scoring. - Data processed on a large scale. - Matching or combining of datasets. - <u>Sensitive data or data of a highly personal nature:</u> 	
An institution creating a national level credit rating or fraud database.	<ul style="list-style-type: none"> - Evaluation or scoring. - Automated decision making with legal or similar significant effect. - Prevents data subject from exercising a right or using a service or a contract. - <u>Sensitive data or data of a highly personal nature:</u> 	
Storage for archiving purpose of pseudonymised personal sensitive data concerning vulnerable data subjects of research projects or clinical trials	<ul style="list-style-type: none"> - Sensitive data. - Data concerning vulnerable data subjects. - Prevents data subjects from exercising a right or using a service or a contract. 	



Examples of processing	Possible Relevant criteria	DPIA likely to be required?
A processing of “personal data from patients or clients by an individual physician, other health care professional or lawyer” (Recital 91).	<ul style="list-style-type: none"> - <u>Sensitive data or data of a highly personal nature.</u> - Data concerning vulnerable data subjects. 	No
An online magazine using a mailing list to send a generic daily digest to its subscribers.	<ul style="list-style-type: none"> - Data processed on a large scale. 	
An e-commerce website displaying adverts for vintage car parts involving limited profiling based on items viewed or purchased on its own website.	<ul style="list-style-type: none"> - Evaluation or scoring. 	






What should the DPIA include?

 Purpose of Processing

 Technical and organisational security measures

 Description of categories of the data

 Assessment of High Risk, if any

 Description of the recipients





What should the DPIA include?

Art 35(7) GDPR

The assessment shall contain *at least*:

- (a) A description of the envisaged processing operations and the purposes of the processing;
- (b) An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- (c) An assessment of the risks to the rights and freedoms of data subjects;
- (d) The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance.



IDPC Guidelines



General Overview

What are the reasons for conducting a DPIA?

- New processing activity
- Due to changes that occurred to the existing processing activity

Note: A processing activity includes both manual and electronic operations.

Is the DPO involved in the DPIA process?

Describe the nature, scope, context and purpose of envisaged processing.

E.g.: Does the processing include: solely automated and automated processing, including profiling, with legal or similar significant effect; systematic monitoring and evaluation of personal aspects including online behaviour, processing that would exceed the reasonable expectation of the data subjects, use of new technologies, processing of data on a large scale, processing for which the exercise of data subjects rights will prove to be impossible or result disproportionate, processing for which the notification of a breach will result disproportionate? Indicate the methods used for the processing operation.

Attach any relevant supporting documents, such as a project proposal, data flow diagrams, related systems documentation, etc.





IDPC Guidelines

Describe the processing operations related to the envisaged processing.

E.g.: How will the personal data be collected, used, stored and deleted?

Legal basis for processing

Identify the proper legal ground(s), on the strength of which, the processing activity will be legitimised.

Article 6 GDPR sets out the legal criteria to process personal data.

Whereas the rule provides for a prohibition of the processing of special categories of data, the provisions of Article 9 foresee a list of derogations on which the controller can rely to justify the processing of sensitive data.

Categories of personal data processed

Identify the categories of personal data that will be processed, in particular, where special categories or data of a highly personal nature such as criminal offences or convictions or related security measures, or data concerning vulnerable data subjects such as children, location data, will be processed.





IDPC Guidelines



Security of processing

Identify and describe the technical and organisational measures adopted to protect the data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Did you consider the implementation of data protection by design and by default measures to enhance the security of personal data (such as pseudonymisation and encryption techniques, automated deletion of personal data on expiry of retention period and system's capabilities and functionalities to accede to data subjects' rights)?

Did you implement preventive measures to safeguard the personal data and ensure that procedures are in place to detect and report data breaches (e.g. incident response plans) to the supervisory authority within 72 hours from becoming aware of the breach?

Did you provide training and instructions to your staff on how to safeguard the personal data?

Are approved information security policies in place to provide the necessary internal guidelines as part of information security and risk management?

Additional safeguards

Do you follow any approved codes of conduct or international/industry applicable standards?





IDPC Guidelines

Processors

Will a processor and/or sub-processor be engaged to process data on your behalf?

If yes, have you carried out the necessary due diligence on the processor/sub-processor to ensure that they provide sufficient guarantees to implement appropriate technical and organisational measures that the processing will meet the requirements of the GDPR?

Is the relationship with the processor/sub-processor governed by means of a contract or other legal act under Union law. Take into account the minimum requirements set out under Article 28(3) GDPR.

Transfer of personal data to third countries or international organisations

Will the personal data be transferred to a third country?

If yes, will the transfer rely on:

- the basis of an adequacy decision;
- appropriate safeguards, including but not limited to, BCRs, standard data protection clauses adopted by the Commission, approved code of conduct and approved certification mechanism;





IDPC Guidelines

Authorisation from the supervisory authority shall be required if the transfer will be carried out on the basis of:

- contractual clauses entered into between data exporter and data importer in the third country;
- provisions to be inserted in administrative arrangements between public bodies.

Necessity and proportionality

Are the purposes of the processing operation specific, explicit and legitimate (purpose limitation principle)?

Does the processing actually achieve the intended purpose?

Is there another way to achieve the same outcome in a more privacy friendly manner?

Are the data collected adequate, relevant and limited to what is strictly necessary in relation to the purposes for which the data are processed (data minimisation principle)?

How do you ensure that the data provided are accurate and kept up to date (accuracy principle)?

What are the data retention periods, in particular, where different categories of personal data are processed (storage principle)?

What measures are in place to ensure that the data are deleted once the retention period has expired?



IDPC Guidelines



Data subject rights

Are measures in place for the data subjects to exercise their rights (transparency, right of access and to data portability, right to objects and to restrictions of processing, right to rectification and erasure)?

If applicable, how is consent obtained? Ensure that consent is freely-given, specific and informed. Consider opt-in mechanisms in online systems where required. Provide the data subject with an easy manner how to withdraw consent (e.g. opt-out).

Does the new processing allow you to respond to data subject access requests easily?

Risk Assessment (minimum requirements)

Identify the threats and the likelihood that such threats materialise into risks.

Identify all the possible risks.

Establish the number or potential number of affected data subjects by the processing activity.

Identify adverse effects and impact on the data subjects.





What form should the DPIA take?

- WP 29
- 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
- Annex 1 and 2



Annex 2 – Criteria for an acceptable DPIA

The WP29 proposes the following criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR:

- ☐ a systematic description of the processing is provided (Article 35(7)(a)):
 - ☐ nature, scope, context and purposes of the processing are taken into account (recital 90);
 - ☐ personal data, recipients and 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;
 - ☐ compliance with approved codes of conduct is taken into account (Article 35(8));
- ☐ necessity and proportionality are assessed (Article 35(7)(b)):
 - ☐ measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:
 - ☐ measures contributing to the proportionality and the necessity of the processing on the basis of:
 - ☐ specified, explicit and legitimate purpose(s) (Article 5(1)(b));
 - ☐ lawfulness of processing (Article 6);
 - ☐ adequate, relevant and limited to what is necessary data (Article 5(1)(c));
 - ☐ limited storage duration (Article 5(1)(e));
 - ☐ measures contributing to the rights of the data subjects:
 - ☐ information provided to the data subject (Articles 12, 13 and 14);
 - ☐ right of access and to data portability (Articles 15 and 20);
 - ☐ right to rectification and to erasure (Articles 16, 17 and 19);
 - ☐ right to object and to restriction of processing (Article 18, 19 and 21);
 - ☐ relationships with processors (Article 28);
 - ☐ safeguards surrounding international transfer(s) (Chapter V);
 - ☐ prior consultation (Article 36).
- ☐ risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):
 - ☐ origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
 - ☐ risks sources are taken into account (recital 90);
 - ☐ potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
 - ☐ threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
 - ☐ likelihood and severity are estimated (recital 90);
 - ☐ measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);
- ☐ interested parties are involved:
 - ☐ the advice of the DPO is sought (Article 35(2));
 - ☐ the views of data subjects or their representatives are sought, where appropriate (Article 35(9)).



DPIA – EXAMPLE & ACTIVITY





1. Executive Summary.....	3
2. Definitions.....	4
3. Project Details.....	5
4. The Assessment	8
<i>DPIA Background</i>	8
[REDACTED]	8
<i>Analysis of Processing Principles</i>	8
A. Lawfulness, fairness and transparency.....	9
B. Purpose limitation.....	10
C. Data minimisation and Storage limitation	11
D. Accuracy.....	12
E. Integrity and confidentiality (security).....	12
F. Accountability.....	12
G. Preliminary Conclusion	13
5. Consultation process.....	14
6. Risks and Measures to Reduce Risk	15
7. Legitimate Interest Assessment (“LIA”)	18
8. Sign off and record outcomes.....	24



Project Details – CCTV Installation

Key Information	
Data Controller	
Description of the Project	
Nature of the Project	
Purposes of the Project	
Context, Scope and Background of Project	
Data Subjects	
Types of Personal Data	
Special Categories of Personal Data	
Recipients of Personal Data	
Remote Access to CCTV Footage	





Project Details – CCTV Installation

Key Information	
Lawful basis	
Necessity and proportionality of the processing operations in relation to the purposes	
Assessment of the risks to the rights and freedoms of data subjects	

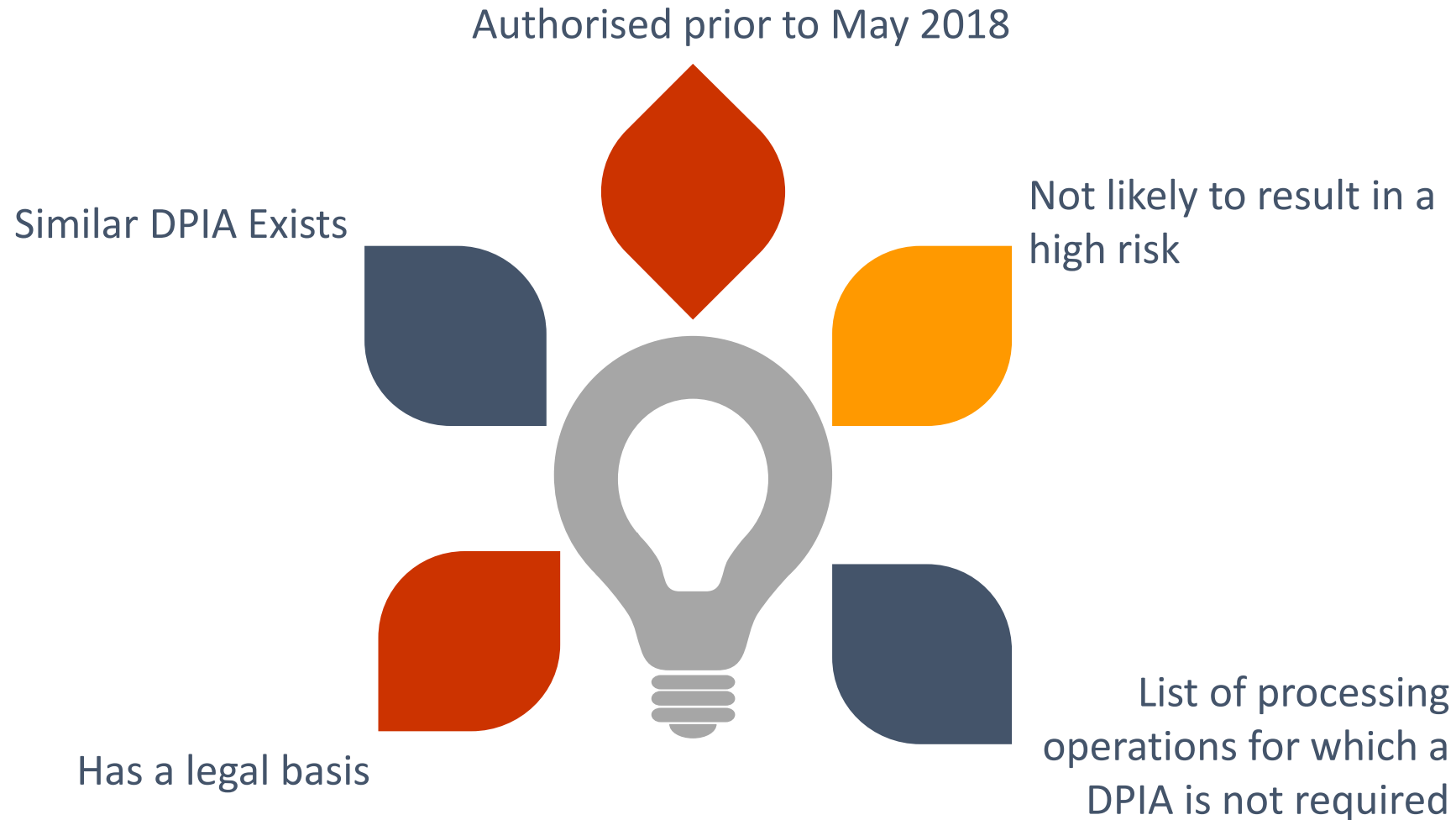


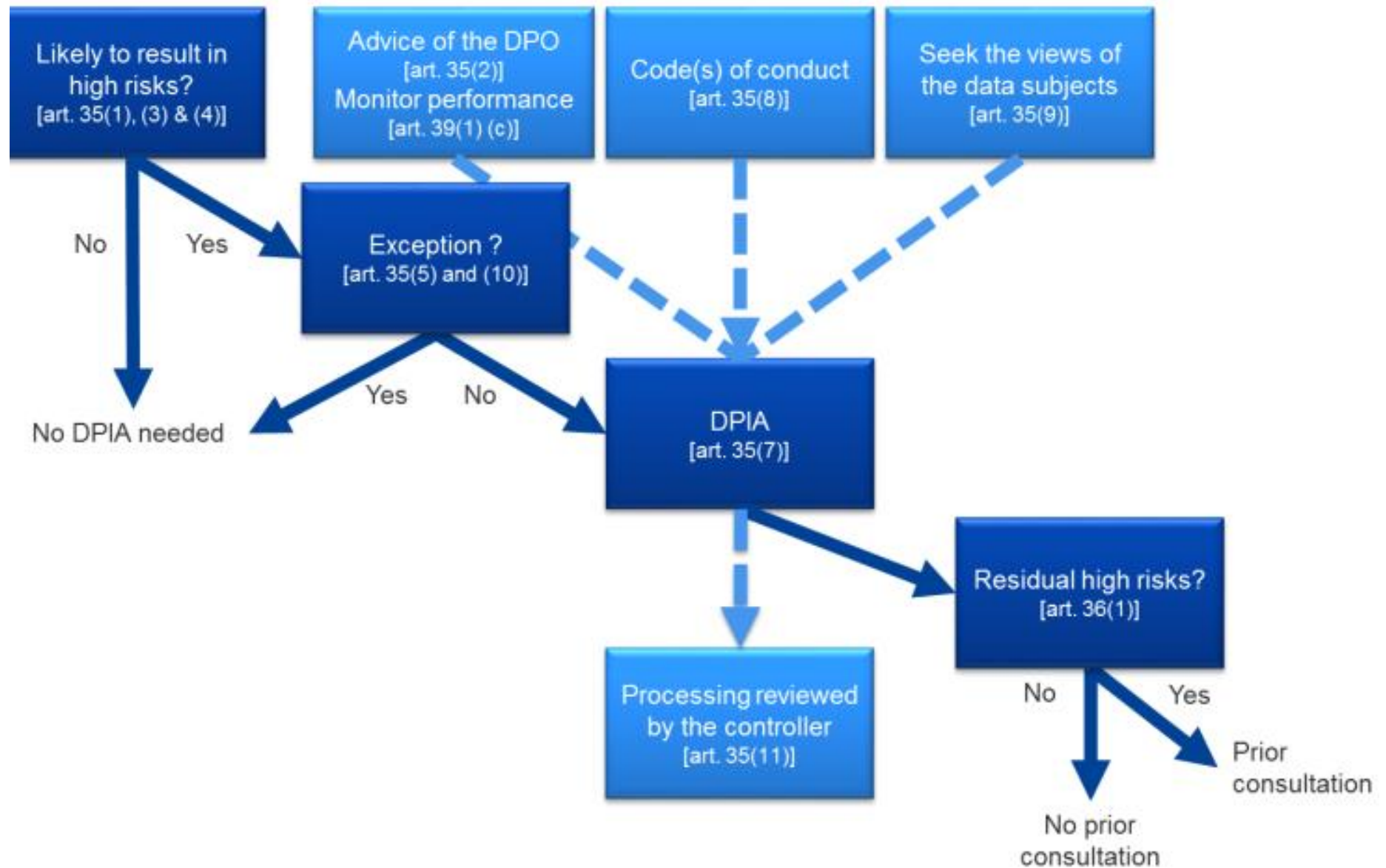
Consultation with the Supervisory Authority

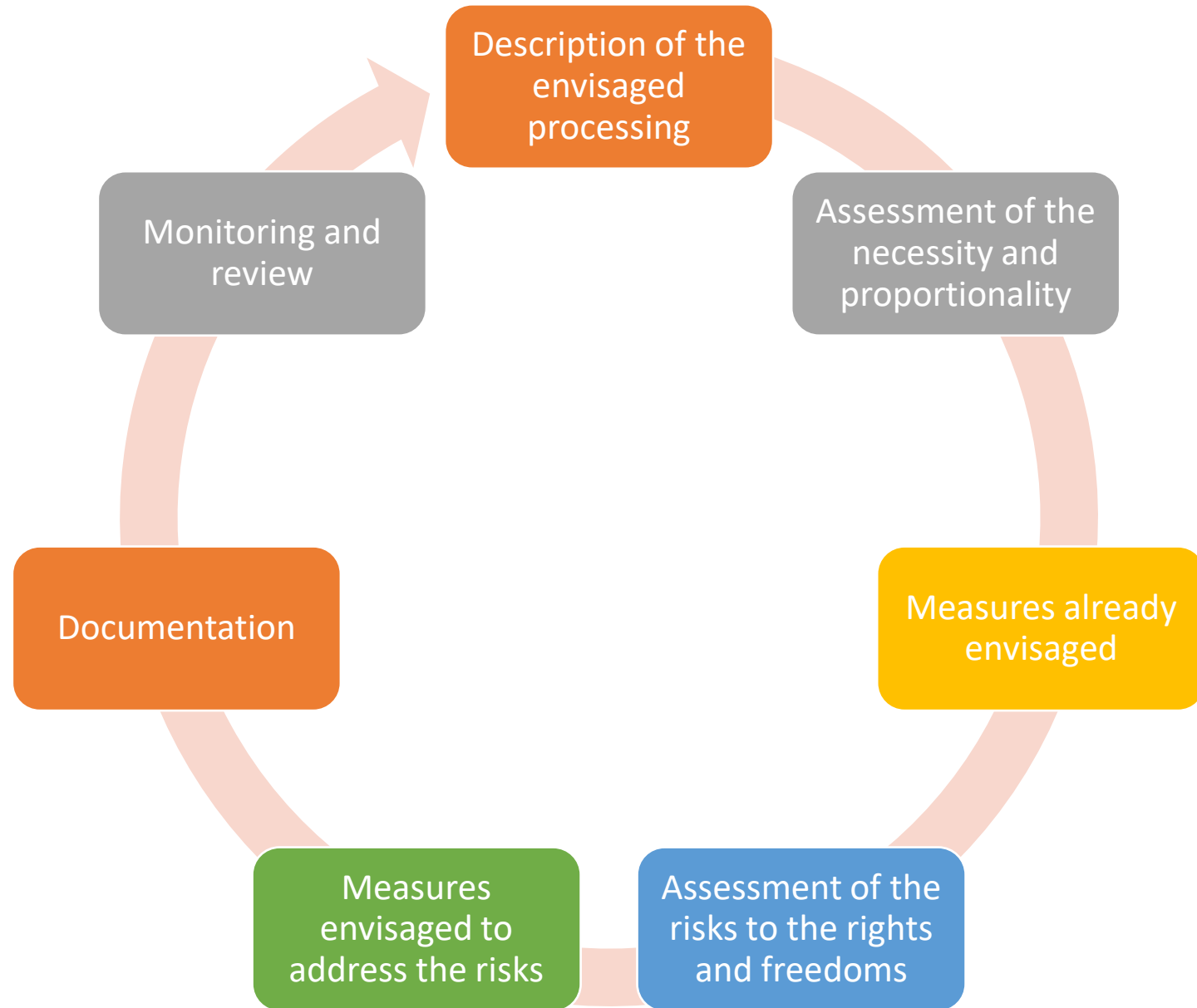
- If the risks identified in a DPIA cannot be sufficiently addressed by the data controller (i.e. the residual risk remains high), then the data controller must consult the supervisory authority prior to commencing the processing.
- Example: If it is not possible to reduce the number of people accessing the personal data, a high residual risk remains – therefore, consultation with the supervisory authority is required.



When is a DPIA not required?









What are the sanctions?

10, 000, 000 EUR







Or

**up to 2 % of the total
worldwide annual turnover**





Current Enforcement

+	ETid-2531	 ITALY	2024-11-13	5,000,000	Foodinho Srl	Art. 5 (1) a), c), d), e) GDPR, Art. 6 GDPR, Art. 9 (2) b) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 22 (3) GDPR, Art. 25 GDPR, Art. 28 GDPR, Art. 32 GDPR, Art. 35 GDPR, Art. 88 GDPR, Art. 2-septies Codice della privacy, Art. 114 Codice della privacy, Art. 47-quinquies Decreto legislativo 81/2015	Non-compliance with general data processing principles
+	ETid-2530	 SPAIN	2024-11-22	220,000	CARTONAJES BAÑERES, S.A.	Art. 15 GDPR, Art. 35 GDPR	Insufficient technical and organisational measures to ensure information security
+	ETid-2521	 BELGIUM	2024-12-17	200,000	Hospital	Art. 5 (1) f) GDPR, Art. 24 GDPR, Art. 32 GDPR, Art. 35 (3) GDPR	Insufficient technical and organisational measures to ensure information security
+	ETid-2517	 FRANCE	2025-02-04	40,000	Real estate company	Art. 5 (1) c) GDPR, Art. 6 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 32 GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
+	ETid-2514	 SPAIN	2024-12-10	4,000,000	GENERALI ESPAÑA, SOCIEDAD ANONIMA DE SEGUROS Y REASEGUROS	Art. 5 (1) f) GDPR, Art. 25 GDPR, Art. 32 GDPR, Art. 35 GDPR	Insufficient technical and organisational measures to ensure information security
+	ETid-2510	 SPAIN	2024-11-22	220,000	CARTONAJES BAÑERES, S.A	Art. 15 GDPR, Art. 35 GDPR	Insufficient technical and organisational measures to ensure information security





Instagram Record €405 million GDPR Fine

- In 2022, the Irish Data Protection Commission issued a record fine of €405 million to Meta Platforms Ireland Limited, which owns the Facebook and Instagram social media platforms
- Meta was found to have facilitated the publication of phone and email contact information of children on Instagram, which resulted in a high risk to the rights and freedoms of these data subjects and therefore necessitated a DPIA
- Meta failed to carry out a proper DPIA – it did not identify nor address the risks to data subjects
- Among other infringements, Meta was found to have breached Article 35(1) of the GDPR, which required it to conduct a DPIA in such circumstances





Re - Cap

- ✓ A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.
- ✓ The assessment must be carried out when the processing results in a high risk to the data subject's fundamental rights and freedoms
- ✓ The assessment should be carried out before the processing operation takes place and must be continually updated

Policies and Procedures





GDPR Recital 78

“In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.”



Policies - Examples





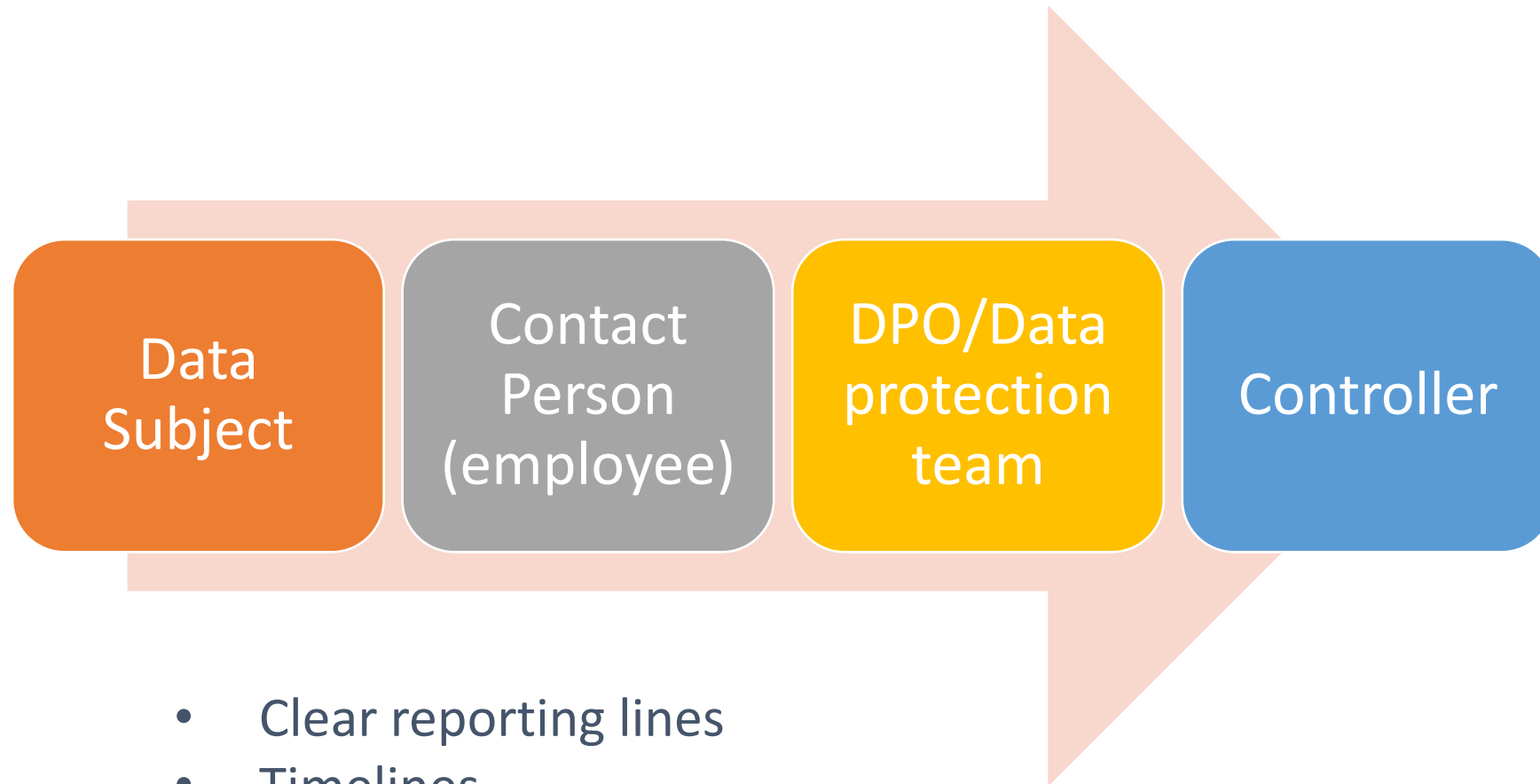
Data Subject Access Request Policy

- How do you recognise a SAR?
- What do you do if you receive a SAR verbally?
- What steps need to be taken to verify the identity of the requester?
- When can you refuse a request?
- What additional information do you need to provide?
- Do you have information management systems in place which allow you to easily retrieve information?





Data Subject Access Request Policy



Clean Desk Policy

- Specifies how employees should leave their working space when they leave the office
- Clear desks of papers
- Close laptop screens
- Keep files/papers under lock and key



CLEAN DESK POLICY



BEFORE YOU LEAVE...

- 1 Tidy your desk
- 2 Lock your screen
- 3 Put away sensitive documents



IT Security Policy

- Identifies the rules and procedures for all individuals accessing and using an organisation's IT assets and resources
- Passwords and encryption
- Confidentiality
- Accuracy of information
- Awareness and general security
- Breach reporting



Website Use Policy

- Sets out what users can and cannot do when using your website
- Prohibited uses
- Privacy notice
- Content standards
- Suspension and termination





Cookies Policy

- A cookie is a small text file that a website stores on your computer or mobile device when you visit the site.
- First party cookies are cookies set by the website you're visiting. Only that website can read them. In addition, a website might potentially use external services, which also set their own cookies, known as third-party cookies.
- Persistent cookies are cookies saved on your computer and that are not deleted automatically when you quit your browser, unlike a session cookie, which is deleted when you quit your browser.
- https://ec.europa.eu/info/cookies_en





Data Retention Policy

Key Principle: No more data is processed than is necessary and data is not kept for a period longer than necessary. (Data used e.g. for archiving purposes in the public interest, scientific or historical research purposes, can be kept for a longer period)

- Refer to **Laws** or Agreed **Industry Practices** on Retention of Information
- Absence of law: Justification based on individual **business needs**
 - *E.g. holding personal data for operational reasons*



Data Retention Policy

How to determine 'business needs':

- What is the data/information used for?
- Any legal or regulatory requirements?
- Do any agreed industry practices exist (where relevant)?
- Is it easy or difficult to make sure it remains accurate and up to date?
- Consider the current and future value of the information
- Consider the costs, risks and liabilities associated with retaining the information





Procedures



→ How are they going to be handled?



Procedures

- Clear reporting lines
- Open communication
- Encourage transparency
- Easily accessible policies and procedure structure
- Satisfactory documentary evidence



Auditing





Auditing – why is it necessary?

Before beginning a processing activity or attempting to undertake your GDPR audit, you must establish:

1. Exactly what data you are dealing with;
2. Whether you are a data controller or processor; and
3. Why you've come to the conclusions in 2.





The Accountability Principle





Appropriate technical and
organisational measures are a
must!





DP Auditing

- ✓ Gap Analysis
- ✓ Risk Analysis
- ✓ Legal Analysis
- ✓ Project Steering / Budget Planning
- ✓ Setting Up a data protection structure and management
- ✓ Monitoring the status of implementation
- ✓ Review Insurance Arrangements
- ✓ Assess Liability Exposure





CAMILLERI PREZIOSI

ADVOCATES

Data Protection Compliance Checklist

Questions:	Answers:
Data Mapping	
1. Which companies process personal data within the group?	
2. How are data collected?	
3. Which data are collected?	
4. What is the stated purpose/s of collection?	
5. Why are the data processed?	
6. How and where are the data stored (both physical data and soft-copies)?	
7. For how long are data retained and why?	
8. Do you have any data practices, processes or	





procedures in place? If yes, please supply.	
9. Do you collect any personal data not directly from the data subject?	
10. Are there any privacy and data protection policies in place? If yes, please supply.	
11. Do you carry out any form of profiling or automated decision making? If yes, on whom and for what purpose?	
12. Do you have CCTV cameras? If yes, where are the cameras located?	
13. Do your CCTV cameras only record video or sound as well?	
14. Is CCTV monitoring only used for security purposes or also for other purposes (such as disciplinary action)?	
15. Do you have notices in regard to CCTV?	
16. Do you monitor employee work communications (emails and calls)?	
17. Do you record calls?	
Accountability	



Data Inventories

Dataset	Responsible Person or Department	Classification	Data Owner	Data Format	Storage Means & Location	Includes Personal Data?	Includes Sensitive Data?





Personal Data Elements	Purpose/s of Processing	Legal Basis	Method of collecting consent	Legal Obligation	Legitimate Interests	Categories of data subjects



Legitimate Interests	Categories of data subjects	Recipients or categories of recipients of the personal data	International Transfers to Third Countries or another international organisation, including the identification of the third country/countries	Retention Period	Technical and organizational security measures	Policies in Place







CAMILLERI PREZIOSI
ADVOCATES

 INTERLAW®