

DATA PROTECTION OFFICERS – GDPR COMPLIANCE



CAMILLERI PREZIOSI
— ADVOCATES —



www.21Academy.education

Breakdown of Today's Session

- ✓ Legal requirements of a DPIA;
- ✓ How to conduct a DPIA;
- ✓ Policies and Procedures; and
- ✓ Auditing



www.21Academy.education

The GDPR – a risk based Regulation



www.21Academy.education

Privacy by Design and by Default

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



www.21Academy.education

Privacy by Design and 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



www.21Academy.education

Privacy by Design

Article 25 GDPR of *Privacy by Design*

*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.*



www.21Academy.education

Privacy by Design

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.



www.21Academy.education

What is a DPIA?

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



www.21Academy.education

When is a DPIA required?

Article 35 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.



www.21Academy.education

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 do a DPIA for any major project which requires the processing of personal data.



www.21Academy.education

Timing: Conducting a DPIA?

- ✓ To be carried out prior to the processing



www.21Academy.education

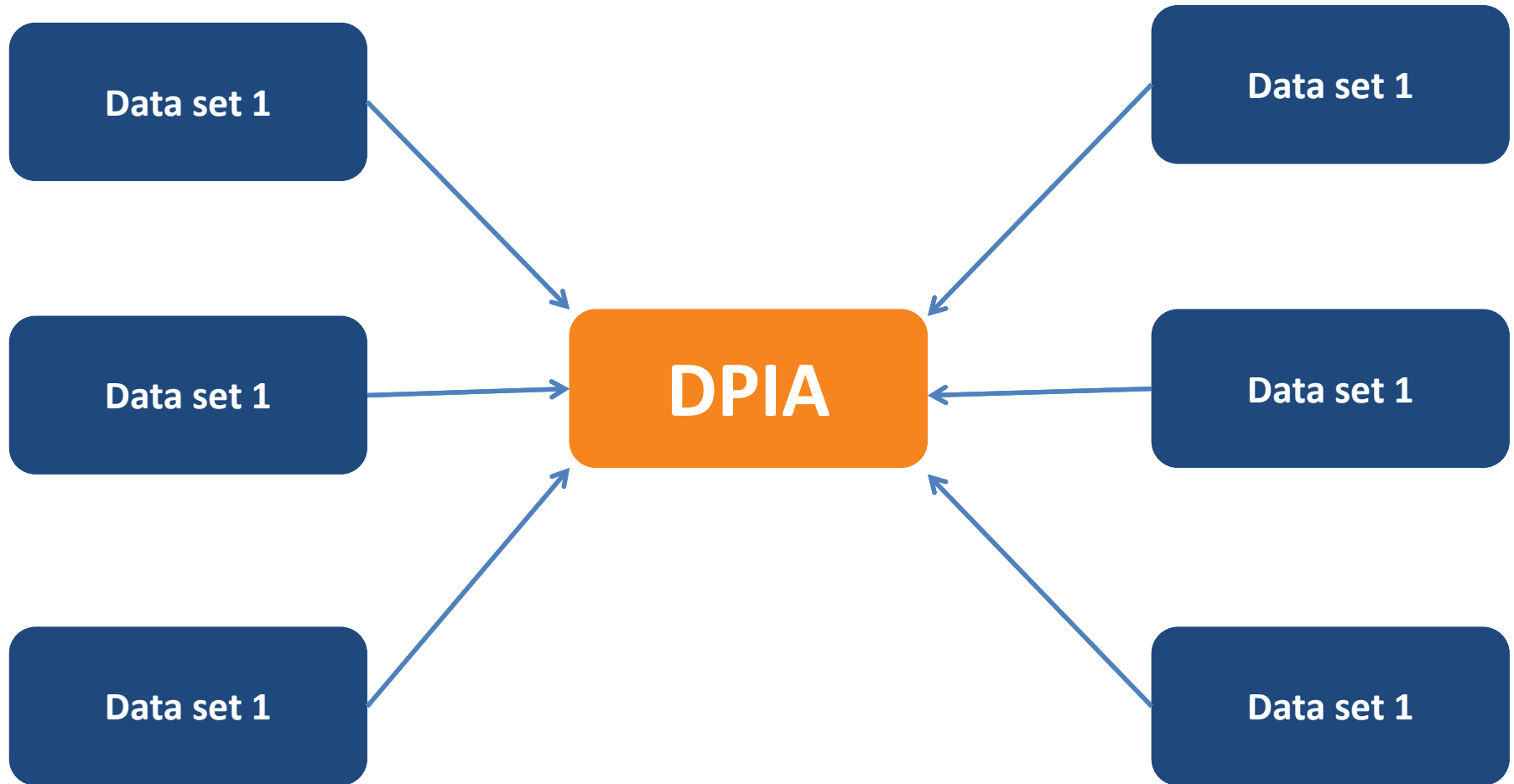
What should a DPIA address?

- ✓ Either: a single processing operation
e.g. introduction of CCTV
or
- ✓ 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

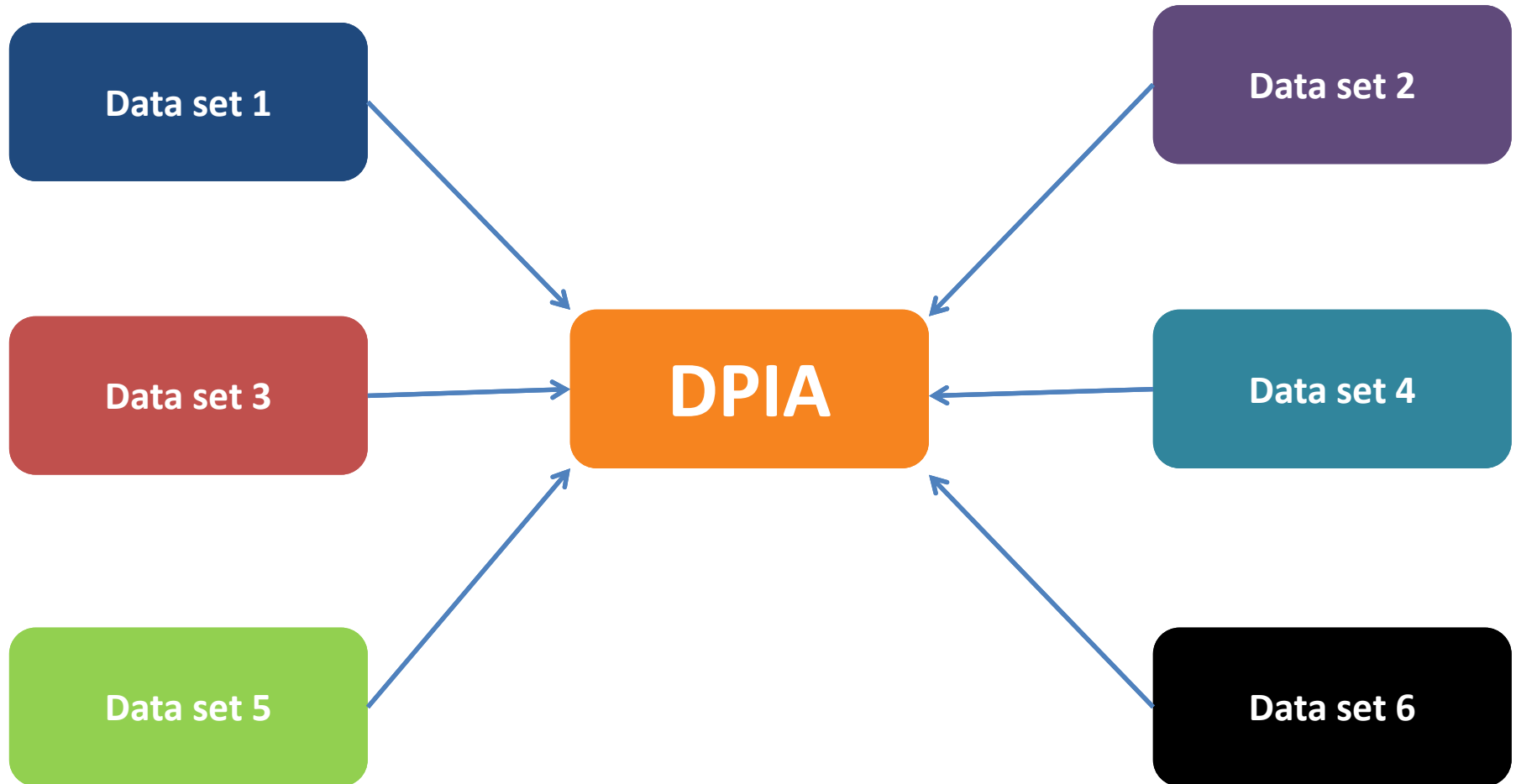


www.21Academy.education

DPIA – Single Processing



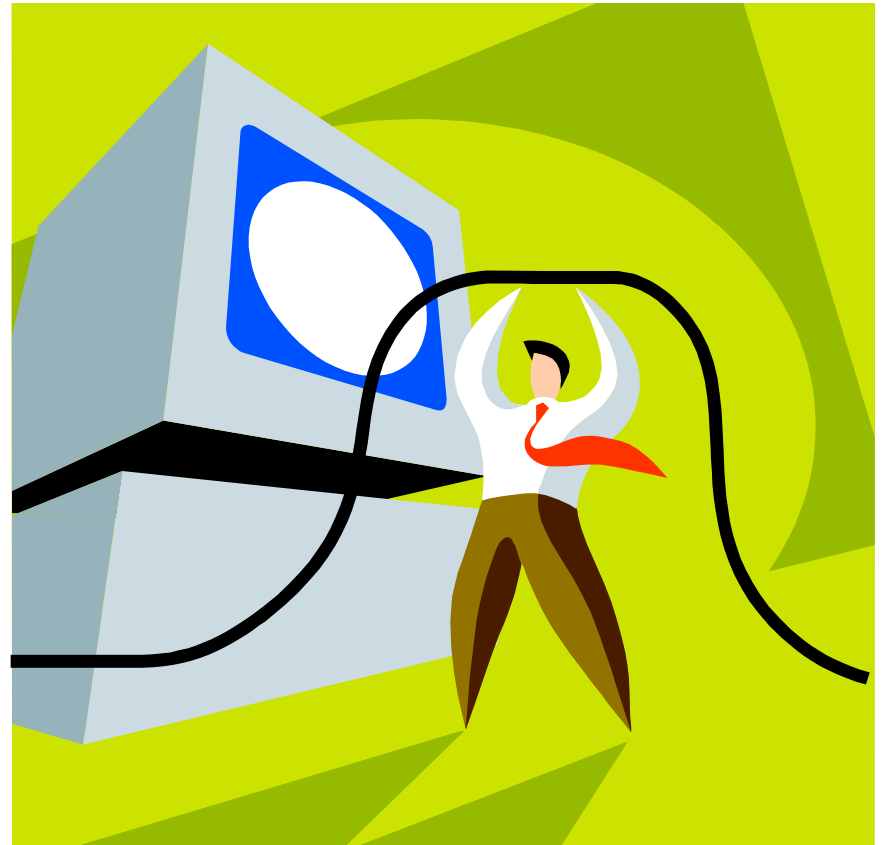
DPIA – Multiple Processing



Who is obliged to carry out a DPIA?



**Data
Controller**



Data Processor

Article 5 of the GDPR

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



www.21Academy.education

Who is the Data Controller ?

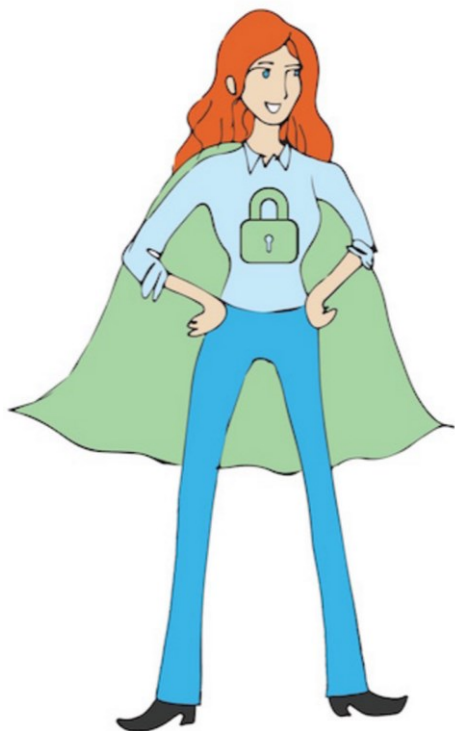
Data Controller

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



www.21Academy.education

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.



www.21Academy.education

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.



www.21Academy.education

Supervisory Authority Involvement

- Residual risks would still be present in the processing operation
- Processing in the public interest of:
 - (a) genetic data, biometric data or data concerning health for statistical or research purposes; or
 - (b) special categories of data in relation to the management of social care services and systems, including for the purposes of quality control, management information and the general national supervision and monitoring of such services and systems.



www.21Academy.education

When is a DPIA mandatory?

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



www.21Academy.education

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



www.21Academy.education

Automated Decision Making



www.21Academy.education

Large Scale Processing: Special Categories of PD Art 9(1)



www.21Academy.education

Monitoring of Public



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



www.21Academy.education

**Evaluation or
scoring**

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

**Systematic
Monitoring**

Sensitive Data

**Data Processed on
a large scale**

Matching datasets

**Data concerning
vulnerable data
subjects**

**Innovative
organisational
solutions**

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

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. 	

When is a DPIA mandatory?

Article 35(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.



www.21Academy.education

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

– The list is non-exhaustive in nature and shall complement and further specify such guidelines.



www.21Academy.education

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



www.21Academy.education

What should the DPIA include?

Art 37(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



www.21Academy.education

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.



www.21Academy.education

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.



www.21Academy.education

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?



www.21Academy.education

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;



www.21Academy.education

IDPC Guidelines

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?

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?



www.21Academy.education

IDPC Guidelines

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.

Identify mitigations measures appropriate to the risks.

Identify residual risks, if any.

Outcome

Comments by the DPO.

In the case of residual high risks, do you have a procedure in place to consult the supervisory authority pursuant to the requirements of Article 36 GDPR?

Devise an implementation plan of the necessary measures identified in the DPIA and target dates.

Approvals, signatures of responsible officers (including the DPO where applicable) and date.



www.21Academy.education

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)).



www.21Academy.education

When is a DPIA not required?

Authorised prior to May 2018

Similar DPIA Exists

Not likely to result in a high risk

Has a legal basis

List of processing operations for which a DPIA is not required



TIME FOR REVIEW

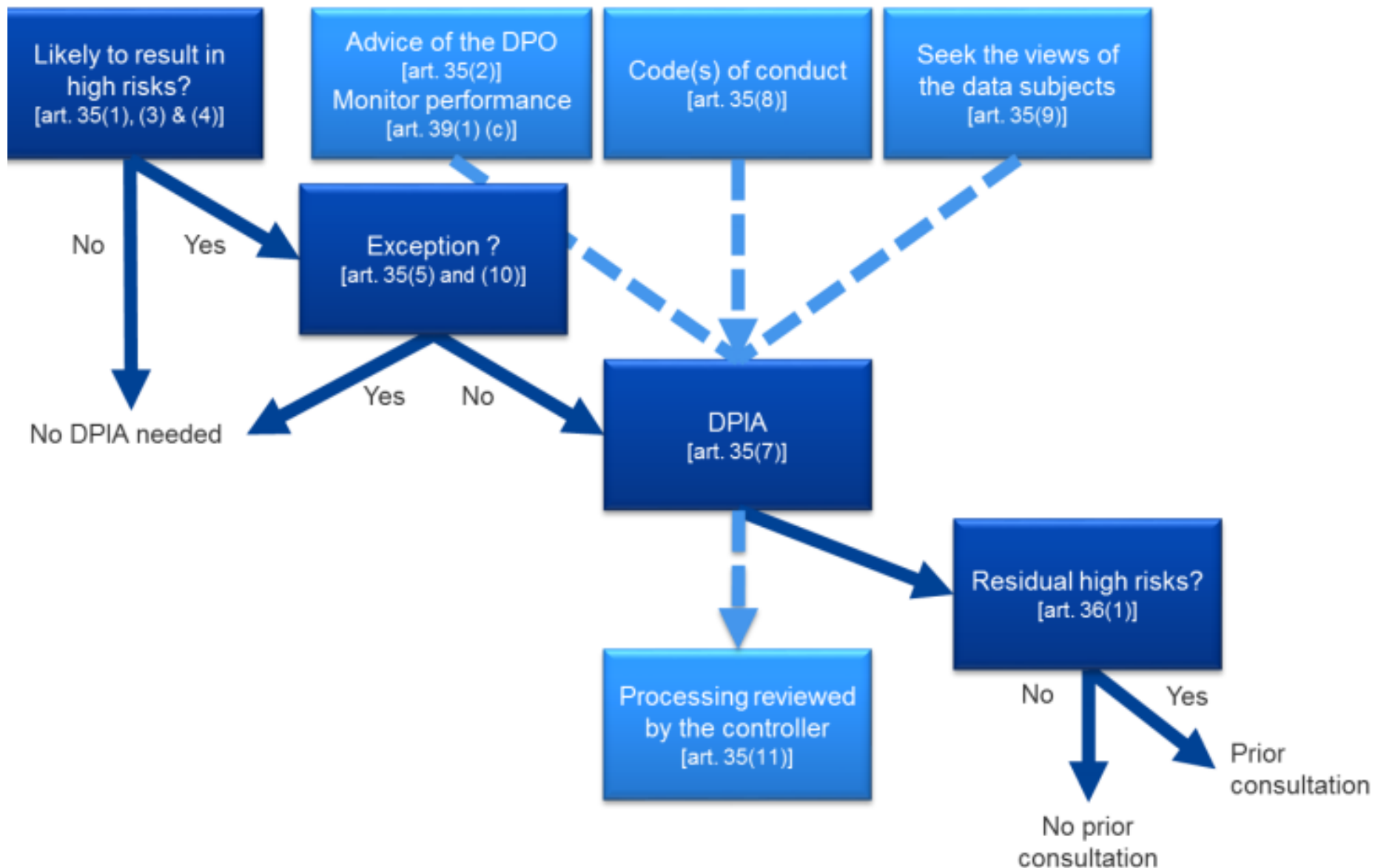


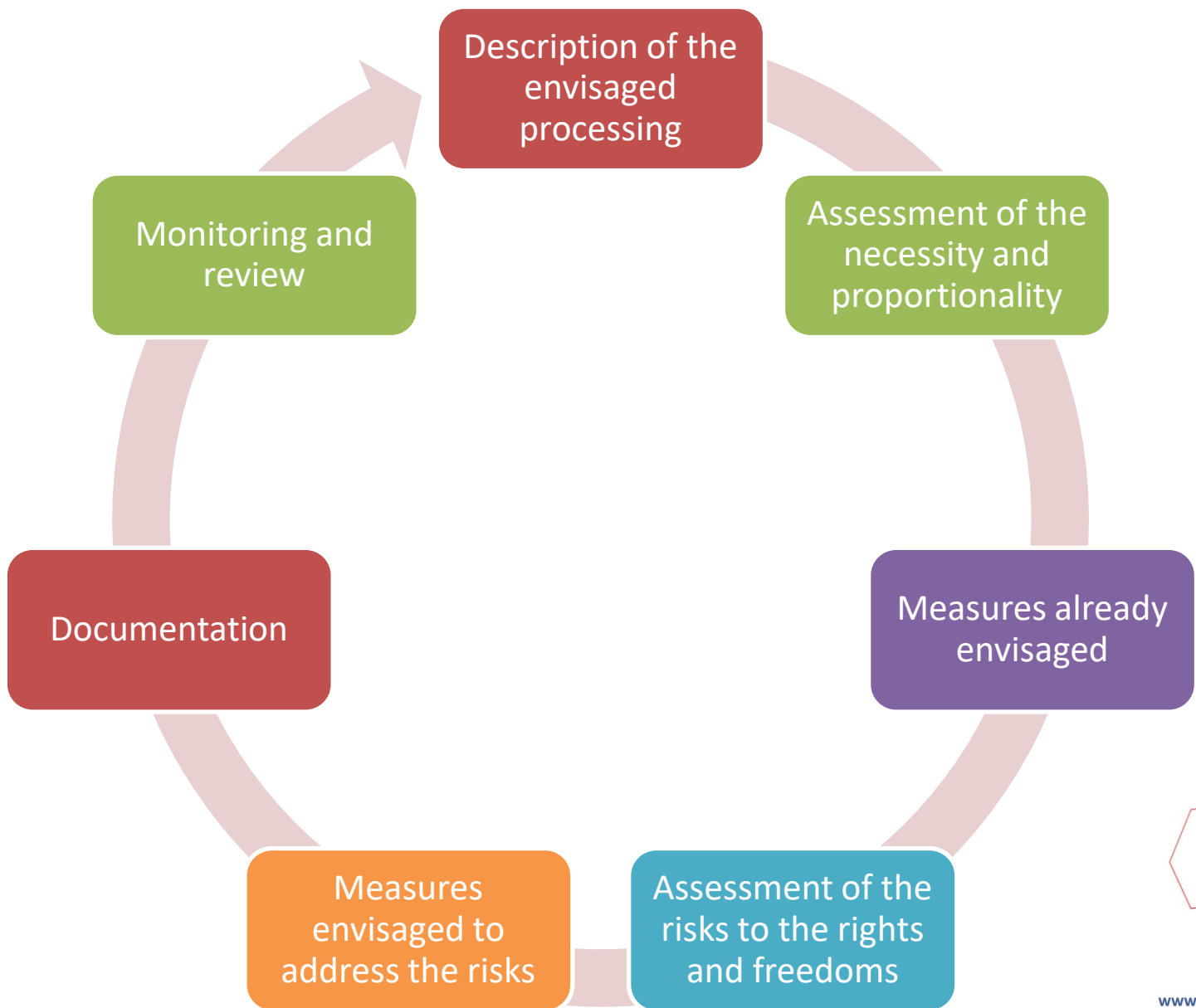
Re - Cap

- ✓ 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



www.21Academy.education





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



www.21Academy.education

What are the sanctions?

10, 000, 000 EUR

Or

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

Current Enforcement

 NORWAY	Norwegian Supervisory Authority (Datatilsynet)	2020-07-10	46,660	Municipality of Rælingen	Art. 32 GDPR, Art. 35 GDPR	Insufficient technical and organisational measures to ensure information security
---	---	------------	--------	--------------------------	-------------------------------	---



www.21Academy.education

Current Enforcement

 FINLAND	Deputy Data Protection Ombudsman	2020-05-29	72,000	Taksi Helsinki	Art. 5 GDPR, Art. 6 GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
 FINLAND	Deputy Data Protection Ombudsman	2020-05-22	16,000	Kymen Vesi Oy	Art. 35 GDPR	Non-compliance with general data processing principles



www.21Academy.education

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.”



www.21Academy.education

Policies

- ☐ Backup policy
- ☐ Call recordings policy
- ☐ CCTV/ANRP monitoring and recording procedure
- ☐ Clear screen and clean desk policy
- ☐ Complaint submission form
- ☐ Complaints register
- ☐ Data breach procedure
- ☐ Data breach register
- ☐ Data portability request procedure
- ☐ Data protection policy
- ☐ Data subject access request procedure and form



www.21Academy.education

Policies

- ☐ DPIA policy
- ☐ DPIA register
- ☐ Employee policy
- ☐ GDPR training policy
- ☐ IT security policy
- ☐ Joiners, movers and leavers procedure
- ☐ Retention policy
- ☐ Vehicle tracking policy
- ☐ Website privacy policy, terms of use and cookies
- ☐ Collection of consent, recording and withdrawal



www.21Academy.education

Procedures

**Data Subject
Access Request**

**Data
Portability**

Data Breach

**Data Subject
Consent
Withdrawal**



www.21Academy.education

TIME FOR REVIEW



Auditing



Auditing – why is it necessary?

Before you can do anything 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 those conclusions.



www.21Academy.education

The Accountability Principle



Appropriate technical and organisational measures are a must!



www.21Academy.education



www.21Academy.education

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



www.21Academy.education

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?



www.21Academy.education

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



www.21Academy.education

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



www.21Academy.education

TIME FOR REVIEW





www.21Academy.education

Thank you

Sharon Xuereb
Senior Associate, Camilleri Preziosi

Email: sharon.xuereb@camilleripreziosi.com
Telephone: (356) 21238989

CAMILLERI PREZIOSI
— ADVOCATES —

 **INTERLAW®**
An International Association of Independent Law Firms