

Managing Data and its Implications

Lecture Title: Internal Procedures



Lecturer: Angelito Sciberras

Date: 20 June 2026

Undergraduate Diploma

Last Lecture

- Assignment Questions
- Group Presentation Question
- CIA of Data Breaches
- Data Breach Procedure



Internal Procedures

- SAR Procedure (Lecture 04)
- Data Breach Reporting Procedure (Lecture 06)
- Data Protection Impact Assessment



Data Breaches



What is a data breach?



- A. When unauthorised people gain access to data
- B. When authorized people gain access to data
- C. When data is destroyed
- D. When data is used in the day to day functions of a business

Which is NOT a data breach?



- A. Loss of a company mobile phone
- B. Disposing of the company's intact old lap tops
- C. Saving personal data on the wrong pen drive
- D. Sending an email to all recipients in copy

Which suspected data breaches should be reported within the organisation?



A. All

B. If it becomes public knowledge

C. When there is a risk to the effected data subjects' rights and freedoms

D. Never

When should a suspected data breach be reported inside the organisation?



- A. 72 hours after it happens
- B. 24 hours after it happens
- C. 12 hours after it happens
- D. Immediately after it happens

What breaches should be reported outside the organisation, to the supervisory authority?



- A. All
- B. If it becomes public knowledge
- C. When there is a risk to the effected data subjects' rights and freedoms
- D. Never

When should a suspected data breach be reported outside the organisation, to the supervisory authority?



- A. Not later than 72 hours after it happens
- B. Not later than 24 hours after it happens
- C. Not later than 12 hours after it happens
- D. Immediately after it happens

When should a suspected data breach be reported to the affected data subjects?



- A. Always
- B. If a breach is likely to result in a high risk to the rights and freedoms of individuals
- C. If asked to do so by the supervisory authority
- D. Never

When should a data breach with high risk be notified to the effected data subjects?



- A. Not later than 72 hours after it happens
- B. Not later than 24 hours after it happens
- C. Not later than 12 hours after it happens
- D. As soon as possible

Is this a reportable data breach, if yes, who should have been informed?

A data controller sent paperwork to a child's birth parents without redacting the adoptive parents' names and address. After discovering the breach, the data controller did not inform the adoptive parents

- A. Not a reportable data breach
- B. Reportable to supervisory authority only
- C. Reportable to data subjects only
- D. Reportable to both supervisory authority and data subjects**



Is this a reportable data breach, if yes, who should have been informed?

A debt insolvency agent emailed a vulnerable new client's file in error to a colleague in a different department. The colleague who received the file immediately deleted the email and informed the sender of the error.

- A. Not a reportable data breach
- B. Reportable to supervisory authority only
- C. Reportable to data subjects only
- D. Reportable to both supervisory authority and data subjects



Is this a reportable data breach, if yes, who should have been informed?

An employee lost his briefcase, containing work on an unencrypted laptop and unredacted paper files relating to a sensitive court case - including information on criminal convictions and health information.

- A. Not a reportable data breach
- B. Reportable to supervisory authority only
- C. Reportable to data subjects only
- D. Reportable to both supervisory authority and data subjects**



Is this a reportable data breach, if yes, who should have been informed?

Initially, the employee told his manager that he believed the laptop was encrypted and the paper files were redacted. The manager reported the incident to the IT department, who remotely wiped the laptop.

- A. Not a reportable data breach
- B. Reportable to supervisory authority only
- C. Reportable to data subjects only
- D. Reportable to both supervisory authority and data subjects



Is this a reportable data breach, if yes, who should have been informed?

A courier, delivering medication for a pharmacy, delivered one set of medication to the wrong patient (Patient A). Patient A called the pharmacy to complain. The pharmacist then realised the prescription was for a different patient with a similar name (Patient B). After contacting the courier, the unopened medication was collected and delivered to Patient B.

- A. Not a reportable data breach
- B. Reportable to supervisory authority only
- C. Reportable to data subjects only
- D. Reportable to both supervisory authority and data subjects



Is this a reportable data breach, if yes, who should have been informed?

An employee clicked a link to download a document from a phishing email, then inadvertently entered login credentials into what they believed was a legitimate website. A while later, the employee contacted the company's IT department as they noticed they were no longer receiving emails.

- A. Not a reportable data breach
- B. Reportable to supervisory authority only
- C. Reportable to data subjects only
- D. Reportable to both supervisory authority and data subjects





Undergraduate Diploma

Data Breaches



A pharmacy experiences a data breach where unauthorised individuals gain access to thousands of customer names and email addresses. The pharmacist quickly identifies and resolves the security vulnerability.

Should it be reported to the supervisory authority, the data subjects, or none of them?

Data Breaches



A financial institution experiences a data breach where cybercriminals gain unauthorised access to customer records, including names, home addresses and social security numbers. The institution immediately takes action to mitigate the breach and strengthen its security measures.

Should it be reported to the supervisory authority, the data subjects, or none of them?



Data Breaches



Your group is an investigating team of a company employing 523 employees. What action will you take on the following report and why?

Data Breach 1

An employee informs you that an email which was meant to be sent to your payroll service provider including an Excel attachment was sent to the wrong recipient. The excel sheet included the employees' company number, and overtime hours for that month.

Investigate and report



Data Breach 2

An employee informs you that an email which was meant to be sent to the social security department was sent to the wrong recipient. The email included the employees' sick leave certificates as an attachment .

Investigate and report

Suggest mitigation measures for non-repeat of the data breach

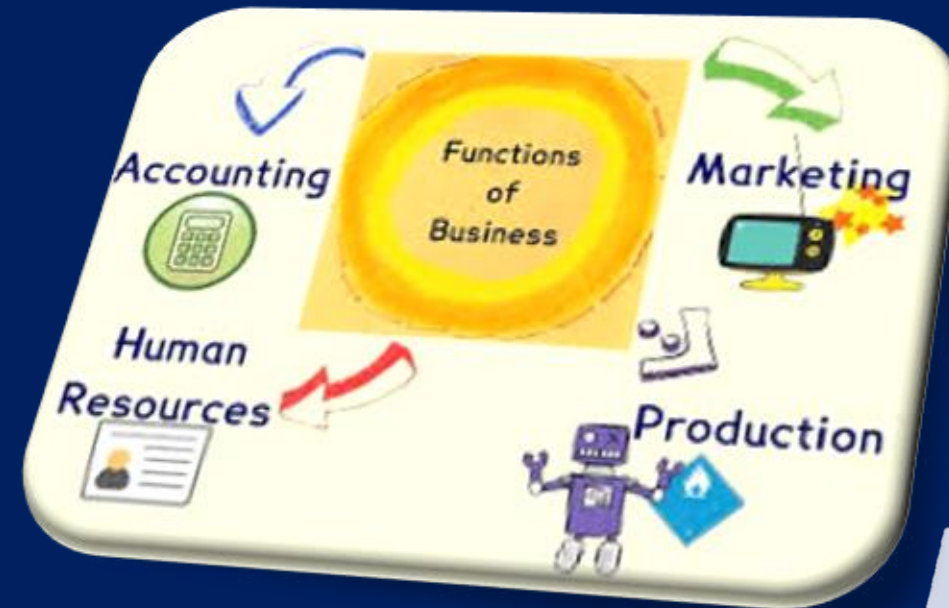




Undergraduate Diploma

Most effected departments in a company?

- IT
- Human Resources
- **Marketing** (Sales)
- Finance



Direct Marketing vs Indirect Marketing



What do we mean by “direct marketing” ?



Direct Marketing

- In the UK DPA 2018 :
- “the communication (by whatever means) of advertising or marketing material which is directed to particular individuals”



Direct Marketing

- Direct Marketing covers all advertising or promotional material.
- Including those promoting the aims or ideals of NGOs, charities and political parties.
- E-mails
- Print ads
- Telephone Calls
- Direct mail



Indirect Marketing

- News articles and press
- Sponsorships
- Blog posts
- Social media pages
- Social media influencers
- Product placements
- Word-of-mouth
- Referrals



Direct Marketing

- does not include “genuine market research”
- unless a survey includes promotional material



Direct Marketing

- Genuine routine customer-care service messages do not count as direct marketing.
- E.g. correspondence on current contracts, past purchases, service interruptions etc.



Direct Marketing

DATA PROTECTION LAW
cares about direct marketing



Direct Marketing

- ...How is direct marketing regulated?
- General Data Protection Regulation ('GDPR') - 2016/679
- Data Protection Act (Chap. 586)
- Processing of Personal Data (E-Communications Sector) Regulations (586.01)
- Processing of Child's Personal Data in relation to the Offer of Information Society Services Regulations (586.11)



GDPR | RECITAL 47

“The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.”

E.g. to profile your customers?

3-Part-Test must be documented



3-Part-Test

1 Purpose

Is it in Your Interests?
Is it Lawful?
Is it Ethical?

2 Necessity

Is it Proportionate?
Are There Alternatives?

3 Balance

Is it High-Risk?
What's the Impact?

GDPR | Article 21(2) | Right to Object

*“Where personal data are processed for direct marketing purposes, the data subject shall have the **right to object at any time** to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.”*

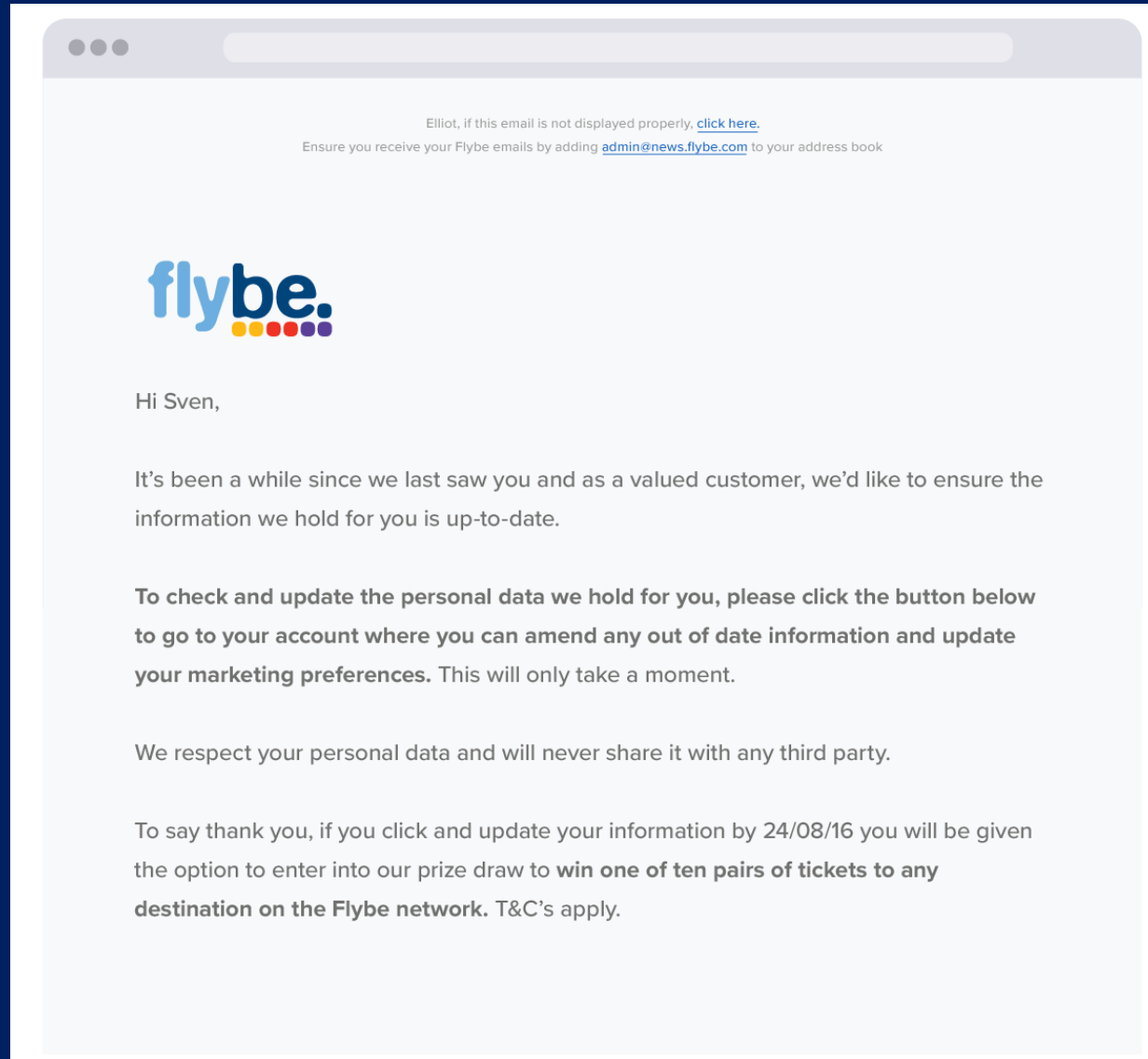


GDPR | Article 21(2) | Right to Object

“Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.”

>> Therefore >> NO possibility to contest





Processing of Personal Data (E-Communications Sector) Regulations

1. Transpose older EU Directives.
2. Is likely to be replaced by a new Regulation.



Processing of Personal Data (E-Communications Sector) Regulations

Includes key rules on:

1. Direct Marketing

2. Web Cookies - (essential tools for Online Behavioural Marketing)



(1) Direct Marketing

**DO
NOT
SPAM.**



(1) Direct Marketing

**DO
NOT
SPAM.**

... You cannot send unsolicited communication for the purpose of direct marketing by means of

- (a) an automatic calling machine; or
- (b) a facsimile machine; or
- (c) electronic mail

to a subscriber or user (including legal entities), unless with the prior consent in writing

(1) Direct Marketing

Unsolicited = a message that has not been specifically requested.

**DO
NOT
SPAM.**

... You cannot send **unsolicited** communication for the purpose of direct marketing by means of

- (a) an automatic calling machine; or
- (b) a facsimile machine; or
- (c) electronic mail

to a subscriber or user (including legal entities), unless with the prior consent in writing

(1) Direct Marketing

*It applies also to **marketing leads** which might not include actual product/services info.*

**DO
NOT
SPAM.**

... You cannot send unsolicited communication for the purpose of **direct marketing** by means of

- (a) an automatic calling machine; or
- (b) a facsimile machine; or
- (c) electronic mail

to a subscriber or user (including legal entities), unless with the prior consent in writing

(1) Direct Marketing

**DO
NOT
SPAM.**

... You cannot send unsolicited communication for the purpose of direct marketing by means of

- (a) an automatic calling machine; or
- (b) a facsimile machine; or
- (c) electronic mail

to a subscriber or user (including legal entities), unless with the prior consent in writing



What do we mean by “electronic mail” ?



Electronic Mail

"electronic mail" means **any text, voice, sound or image** message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient;



(1) Direct Marketing

**DO
NOT
SPAM.**

... You cannot send unsolicited communication for the purpose of direct marketing by means of

- (a) an automatic calling machine; or
- (b) a facsimile machine; or
- (c) electronic mail

to a **subscriber or user (including legal entities)**, unless with the prior consent in writing



(1) Direct Marketing

**DO
NOT
SPAM.**

... You cannot send unsolicited communication for the purpose of direct marketing by means of

- (a) an automatic calling machine; or
- (b) a facsimile machine; or
- (c) electronic mail

to a subscriber or user (including legal entities), **unless with the prior consent in writing**



Consent

.... GDPR

- freely given + informed + clear + specific
- positive action
- Generic consent covering “any third party” = very likely insufficient

Consent - expires?

- The law doesn't impose time-limits
- Consent does not remain valid for ever.
- Must be assessed on a case-by-case basis : is it still reasonable to treat it as an ongoing indication of the person's wishes?
- e.g. was consent given in the context of a specific campaign or service that might have ended?



(1) Direct Marketing

BUT
[soft-opt-in]

Where a person has obtained from his customers their contact details for electronic mail in relation to the sale of a product or a service, in accordance with the Act, that same person may use such details for direct marketing of its own similar products or services;



In Malta It is still not clear whether the exception applies to enquires by potential customers.

E.g. on a Web Form

E.g. by requesting a quotation

UK : Some form of negotiation is required showing interest, even asking for a quote.

BUT
[soft-opt-in]

Where a person has obtained **from his customers** their contact details for electronic mail in relation to the sale of a product or a service, in accordance with the Act, that same person may use such details for direct marketing of its own similar products or services;



This is specific. If you use other personal data, you would need to assess the grounds separately.

BUT
[soft-opt-in]

Where a person has obtained from his customers their **contact details** for electronic mail in relation to the sale of a product or a service, in accordance with the Act, that same person may use such details for direct marketing of its own similar products or services;



“Any text, voice, sound or image message”

NB The exception doesn't apply to FAX or Automated Calls

BUT
[soft-opt-in]

Where a person has obtained from his customers their contact details for **electronic mail** in relation to the sale of a product or a service, in accordance with the Act, that same person may use such details for direct marketing of its own similar products or services;



BUT
[soft-opt-in]

Where a person has obtained from his customers their contact details for electronic mail in relation **to the sale of a product or a service**, in accordance with the Act, that same person may use such details for direct marketing of its own similar products or services;



BUT
[soft-opt-in]

Where a person has obtained from his customers their contact details for electronic mail in relation to the sale of a product or a service, **in accordance with the Act**, that same person may use such details for direct marketing of its own similar products or services;



**PROVIDED
THAT** customers shall be given the opportunity to object, free of charge and in an easy and simple manner, to such use of electronic contact details at the time of their collection and on the occasion of each message where the customer has not initially refused such use;



**PROVIDED
THAT** customers shall be given the **opportunity to object**, free of charge and in an easy and simple manner, to such use of electronic contact details at the time of their collection and on the occasion of each message where the customer has not initially refused such use;



**PROVIDED
THAT** customers shall be given the opportunity to object, **free of charge** and in an easy and simple manner, to such use of electronic contact details at the time of their collection and on the occasion of each message where the customer has not initially refused such use;



**PROVIDED
THAT** customers shall be given the opportunity to object, free of charge and **in an easy and simple manner**, to such use of electronic contact details at the time of their collection and on the occasion of each message where the customer has not initially refused such use;



**PROVIDED
THAT** customers shall be given the opportunity to object, free of charge and in an easy and simple manner, to such use of electronic contact details **at the time of their collection and on the occasion of each message** where the customer has not initially refused such use;



Direct Marketing - Unlawful

- Disguising or concealing the identity of the e-mail sender
- e-mails that do not contain a valid email address for recipients to request that communications stop
- Marketing e-mails that encourage recipients to visit websites that contravene these rules



Direct Marketing Important

- Make sure you are very transparent & upfront (even with customers).
- If you rely on consent, make sure you get different opt-ins for different forms of communications.
- Make sure you keep clear records of consents.



Why is it important to keep a log of who opted out?



Direct Marketing Important

- Make sure you keep a 'do not contact' list of anyone who objects or opts out.
- Be sure to check applicable laws !! - Market research!!
- Look out for industry-specific rules. (e.g. igaming)



Direct Marketing Important

- If you pay someone to do your marketing..... you are both responsible to comply...
- If you apply Automated-Decision-Making (with legal or similar effects)
- ... double check your position.
- Look out for industry-specific rules. (e.g. igaming)



Marketing FAQs



Question 1

The GDPR obviously covers email and email communications - does it also include telephone and postal communication?

Postal communication - door to door

Robo calling

Consent and GDPR compliance by list vendor



Question 2

Is double opt-in a guidance or a law? Does GDPR include 'double opt-in'? i.e. A website visitor said "OK" passively, but do I need to confirm their consent? Surely single consent is enough?



Question 3

What about my contact database? Can I still email these people?



Question 4

How can I profile my data under GDPR to send personalised and targeted marketing material?

Automated Decision Making

Purpose Limitation



Question 5

How can you be sure to be compliant?

1	lawful, fair and transparent
2	specific, explicit and legitimate purpose
3	adequate, relevant and limited to what is necessary
4	accurate & up to date
5	storage limitation
6	integrity and confidentiality

Accountable



Question 6

Does GDPR Block Advertisers from Running Competitions? How Do Marketers Deal With Consent in a Random Prize Draw?

Highlight each piece of data collected during the competition and what you are doing with it.

An individual dropping their business card into a prize draw



Question 7

Can we still ask people to refer friends or does it go against GDPR?

Never:

- record a referred friend's personal data
- send any message to a referred friend
- record any data about a referred friend until they have become your user and provided clear consent
- use cookies or beacons to build profiles of referred friends or to track their behaviour in any way



Question 8

What happens to the mailing list in the case of sale or acquisition of a business? Can I sell or buy the data?

- Information to data subjects
- New owner obliged to use that data according to Privacy Notice
- Otherwise data subjects to be informed with change of purpose



Question 9

Can you buy a marketing list/database ?

Yes (but with lots of caution), if the list was lawfully obtained for that purpose.

[consent is the ground to rely on]



Question 10

Can you sell a marketing list/database ?

Yes (but with lots of caution), if the list was lawfully obtained for that purpose.

[consent is the ground to rely on]



Question 11

Can a company use the same list for multiple brands?

Yes (with caution), if the list was lawfully obtained for that purpose + the customers are fully aware at the time of consent.

[do not rely on exception]



Question 12

Can I send emails about points to members of my loyalty scheme?

Opinion : You should be able rely on legitimate interest or contract to send periodic updates on points/vouchers to members.



Question 13

Can I send marketing emails to members of my loyalty scheme?

Opinion : You should be able rely on the soft-opt-in in relation to marketing on your similar products and customers.





Undergraduate Diploma



Undergraduate Diploma

Data Protection Impact Assessment

- DPIA or Risk Assessment
- Used to identify and assess the potential risks and impacts on individuals' privacy and data protection rights.
- Help to understand and mitigate privacy risks



Data Protection Impact Assessment

- Compliance with data privacy legislation
- Protection of data subjects' rights
- Accountability and transparency
- Minimisation of negative Impacts
- Business reputation and competitive advantage



Data Protection Impact Assessment

- GDPR
 - processing operations that are likely to result in **high risks** to individuals' rights and freedoms, such as systematic and extensive profiling or processing of sensitive data on a large scale.
 - Article 35 of the GDPR - the evaluation of potential risks to individuals' rights and freedoms, the use of new technologies, and processing involving special categories of data.



High Risks

- Article 35(3) sets out three types of processing which always require a DPIA
 - Systematic and extensive profiling with significant effects
 - Large scale use of sensitive data
 - Public monitoring



High Risks

- Evaluation or scoring.
- Automated decision-making with legal or similar significant effect.
- Systematic monitoring.
- Sensitive data or data of a highly personal nature.
- Data processed on a large scale.



High Risks

- Matching or combining datasets.
- Data concerning vulnerable data subjects.
- Innovative use or applying new technological or organisational solutions.
- Preventing data subjects from exercising a right or using a service or contract.



Can you mention typical high-risk processing in a company?



High Risk Examples



Data Protection Impact Assessment

Facial recognition in school renders Sweden's first GDPR fine

📅 22 August 2019 Sweden

The Swedish DPA has fined a municipality 200 000 SEK (approximately 20 000 euros) for using facial recognition technology to monitor the attendance of students in school.

A school in northern Sweden has conducted a pilot using facial recognition to keep track of students' attendance in school. The test run was conducted in one school class for a limited period of time.

The Swedish DPA concluded that the test violates several articles in GDPR and has imposed a fine on the municipality of approximately 20 000 euros. In Sweden public authorities can receive a maximum fine of 10 million SEK (approximately 1 million euros). This is the first fine issued by the Swedish DPA.

The school has processed sensitive biometric data unlawfully and **failed to do an adequate impact assessment** including seeking prior consultation with the Swedish DPA.

The school has based the processing on consent but the Swedish DPA considers that consent was not a valid legal basis given the clear imbalance between the data subject and the controller.

Read the full press release in Swedish below or [here](#)

For further information, please contact the Swedish DPA: imy@imy.se



Data Protection Impact Assessment

The four elements of a DPIA

1. a systematic description of the processing operations and purposes
2. an assessment of proportionality and necessity
3. an assessment of risk to rights and freedoms of an individual
4. what measures are in place to ensure personal data of individuals remains protected



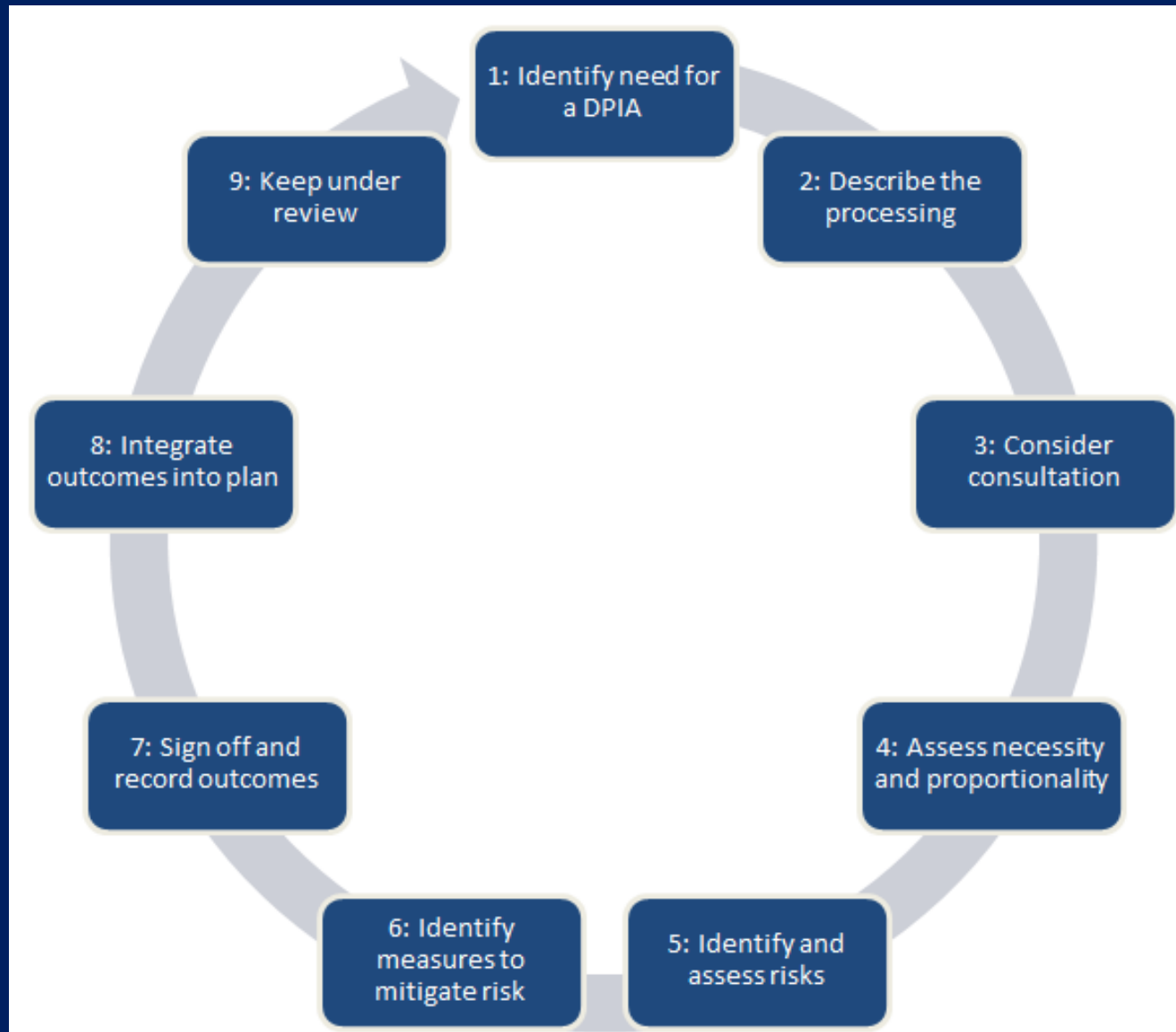
Data Protection Impact Assessment

will indicate

- if the processing is necessary and proportionate and
- if the security measures are adequate
- what are the risks
 - accept those risks
 - mitigate risks
 - reduce risks



Data Protection Impact Assessment



Questions to be asked in a DPIA

- What is the purpose and scope of the data processing activity?
- What types of personal data will be processed, and from what sources will it be obtained?
- How will the personal data be collected, stored, used, and shared?



How it is done

- Collaboration between multiple people
 - Business
 - Legal
 - Data Protection
 - Third Party Provider
 - The Department Implementing the processing
 - Legal advisor
 - Information Technology Department
 - Vendor



How it is done

The Data Protection Office is not involved in the compilation

BUT

Consulted once the DPIA is completed



Questions to be asked in a DPIA

- What are the legal grounds or justifications for processing the personal data?
- Who will have access to the personal data, both within the organisation and to external parties?
- Are there any potential risks or harms to individuals' privacy or data protection rights?



Questions to be asked in a DPIA

- What security measures are in place to protect the personal data against unauthorised access, loss, or breaches?
- Are there any special categories of personal data involved, such as health data or biometric data?
- Will the processing involve cross-border transfers of personal data?



Questions to be asked in a DPIA

- What are the retention periods for the personal data and how will it be securely disposed of after the processing is complete?
- Are there any specific data protection requirements or safeguards that need to be implemented, such as data minimisation, purpose limitation, or data subject rights?
- Have data subjects been provided with sufficient information about the processing activities and their rights



Questions to be asked in a DPIA

- Have measures been taken to ensure transparency and accountability in the processing activities?
- Have any mitigating measures or safeguards been identified to address the identified risks and protect individuals' rights?
- Are there any alternative approaches or less privacy-intrusive methods to achieve the same purpose?



Managing Data and its Implications

Lecture Title: Internal Procedures



Lecturer: Angelito Sciberras

Date: 20 June 2026

Undergraduate Diploma