Managing Data and its Implications

Lecture Title: Compliance with Data Privacy Legislation

Lecturer: Angelito Sciberras

Date: 26 February 2025

Undergraduate Diploma

Last Lecture

- Introduction to GDPR
- Data Breaches
- Identity Theft
- GDPR Fines
- 6 Principles of GDPR and Accountability
- Data vs Personal Data
- Special Category of Data
- Definitions of Processing, Pseudonymisation, Controller, Joint Controllers, Processor
- Data Protection Officer

1. Which of the following can be considered personal data? (Select all that apply)

a) Phone number

b) Recipe for chocolate cake

c) Social security number

d) Weather conditions

e) Home address

2. Which of the following can be considered personal data? (Select all that apply)

a) Favorite colour

b) Publicly available news article

c) Passport expiration date

d) Financial market trends

e) Email newsletter

3. Which of the following can be considered personal data? (Select all that apply)

a) Historical landmark coordinates

b) Bank account number

c) Social media post

d) Publicly available court ruling

e) Traffic light sequence

4. Which of the following can be considered personal data? (Select all that apply)

a) Movie review

b) Public transportation schedule

c) Passport number

d) Publicly available song lyrics

e) Social media profile picture

5. Which of the following can be considered personal data? (Select all that apply)

a) Publicly available scientific research abstract

b) Credit card transaction record

c) Clothing size chart

d) Social media direct message

e) Historical facts about a country

Compliance

Compliance vs Non Compliance

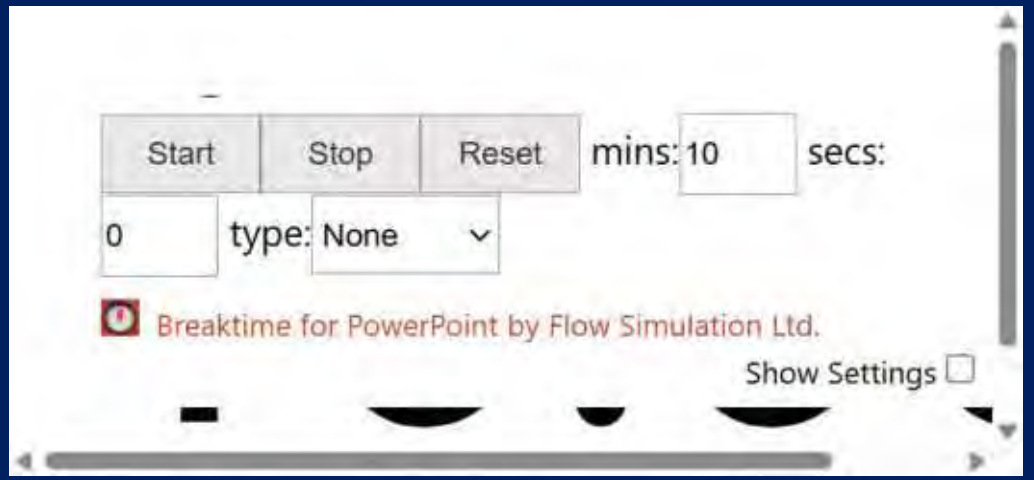
Salesforce reasearch: *"State of the Connected Customer"*

Compliance vs Non Compliance

Most organizations are seeing positive returns on their privacy investments.

More than 40% are seeing benefits at least twice that of their privacy spend

Most effected departments in a company?



Most effected departments in a company?

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

Principles - from lecture 03

Lawfullness

- Consent
- Contract
- Legal Obligation
- Vital Interest
- Public Interest
- Legitimate Interests

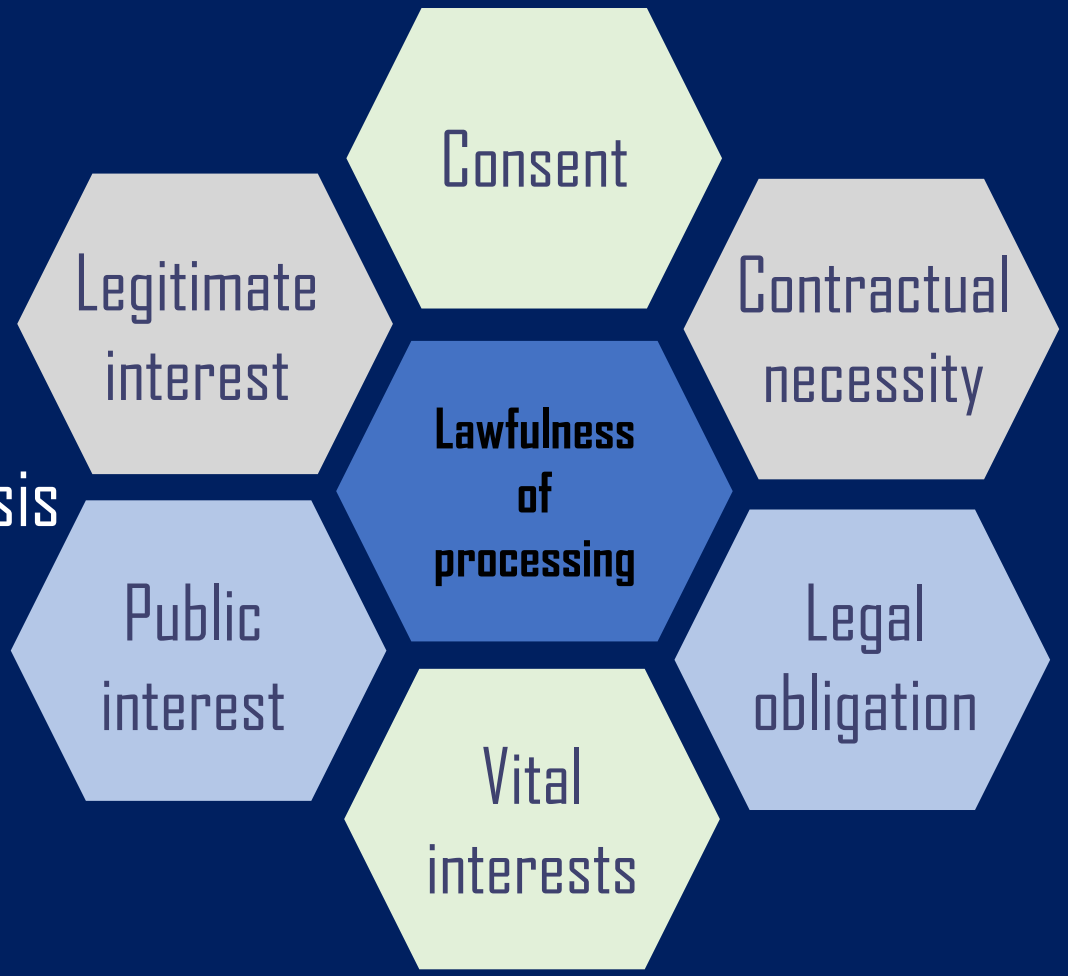
Fairness

- Cannot mislead
- Keep data honest

Transparency

- What is the data
- Why data is needed
- How data is processed
- Not shared with others

Processing is lawful if based on at least one of the following lawful basis

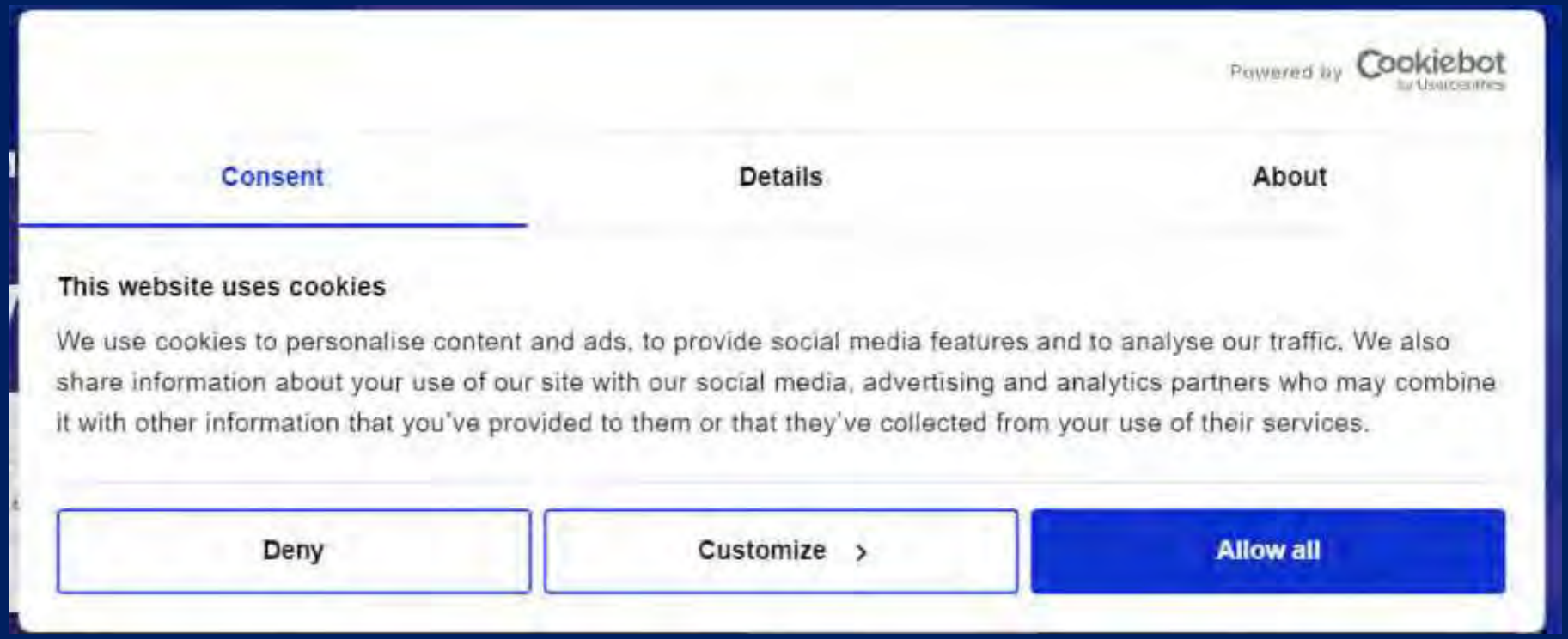


Consent

- The weakest to rely on
- It can be withdrawn at any time
- It has to be explicit
- Obligatory in Marketing
- Cannot be used in HRM

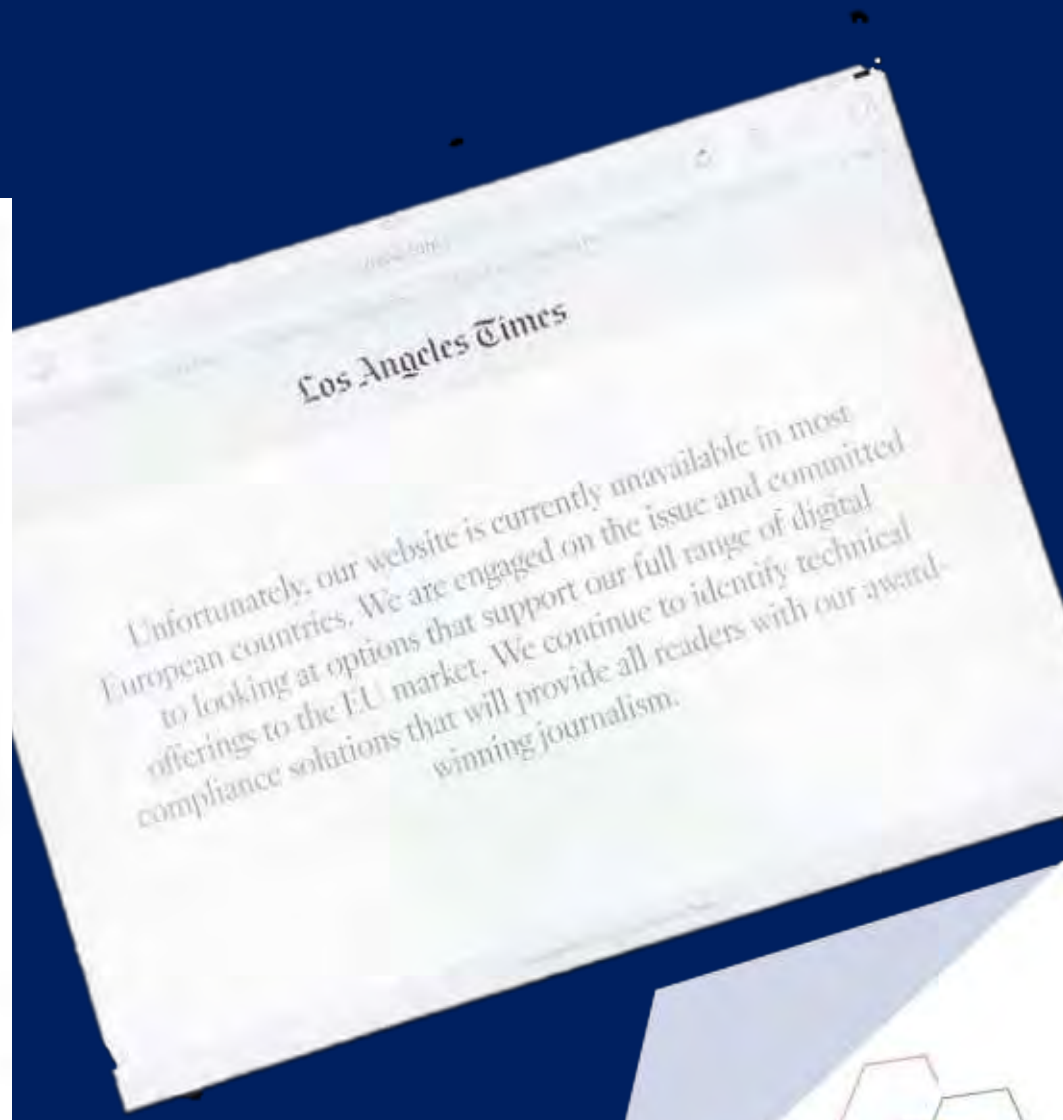
Consent

Cookie Banners



Consent


Visitor from European Union
We have detected that you are visiting us from a country located within the European Union.
Global Data Protection Regulation (GDPR)
Due to requirements placed upon ANA as a result of the EU's Global Data Protection Regulation (GDPR), we are not permitting internet traffic to our website from countries within the European Union at this time. If you believe you've received this message in error or would like more information about our position, please email us at eugdpr@ana.net.
No tracking or performance measurement cookies were served with this page.


Los Angeles Times
Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism.

Consent

€390 million
Forced Consent

€27.8 million
No Consent

€150,000
Use of consent in HRM

Consent

Acceptable in HRM only when

Contractual Necessity

- You have a contract with someone and need to process their personal data to comply with your obligations as part of that contract.

- You don't yet have a contract with someone, but they've asked you to do something as an initial step (for example, provide a quote) and you need to process their personal data to do so.

Legal Obligation

- if you need to process personal data to comply with a common law or statutory obligation.

Vital Interest

- It is unlikely to apply except in cases of emergency medical treatment.

- if it's necessary to process personal data to protect someone's life.

Public interest

- for the performance of a task carried out in the public interest or in the exercise of official authority
- administration of justice is an example

Legitimate interests

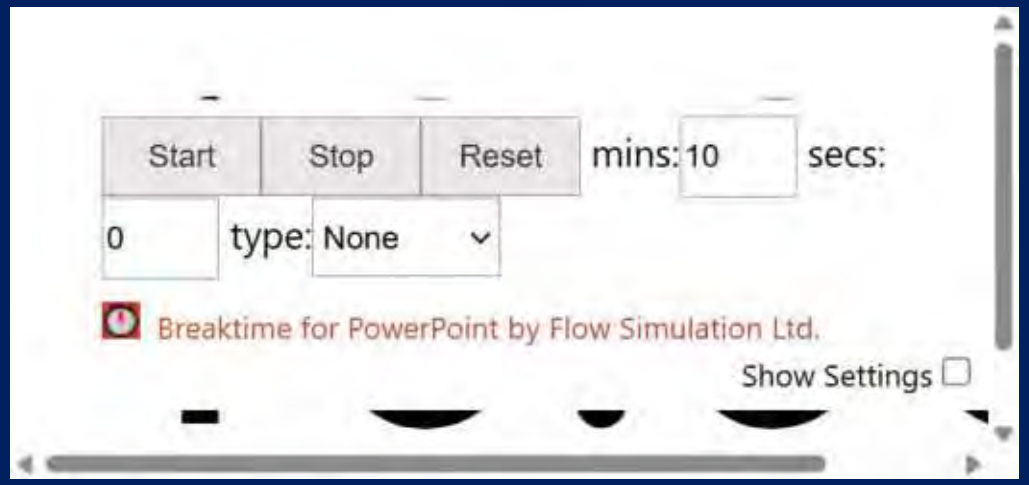
- the most flexible
- burden is on you to determine whether or not your interests in processing the personal data are legitimate
- if you are using an individuals' data in a way that they would expect or otherwise deem reasonable - and where the processing has a minimal impact on their privacy

Legitimate interests

- Fraud prevention
- Network and information security
- Indicating possible criminal acts or threats to public security

21 ACADEMY

Undergraduate Diploma

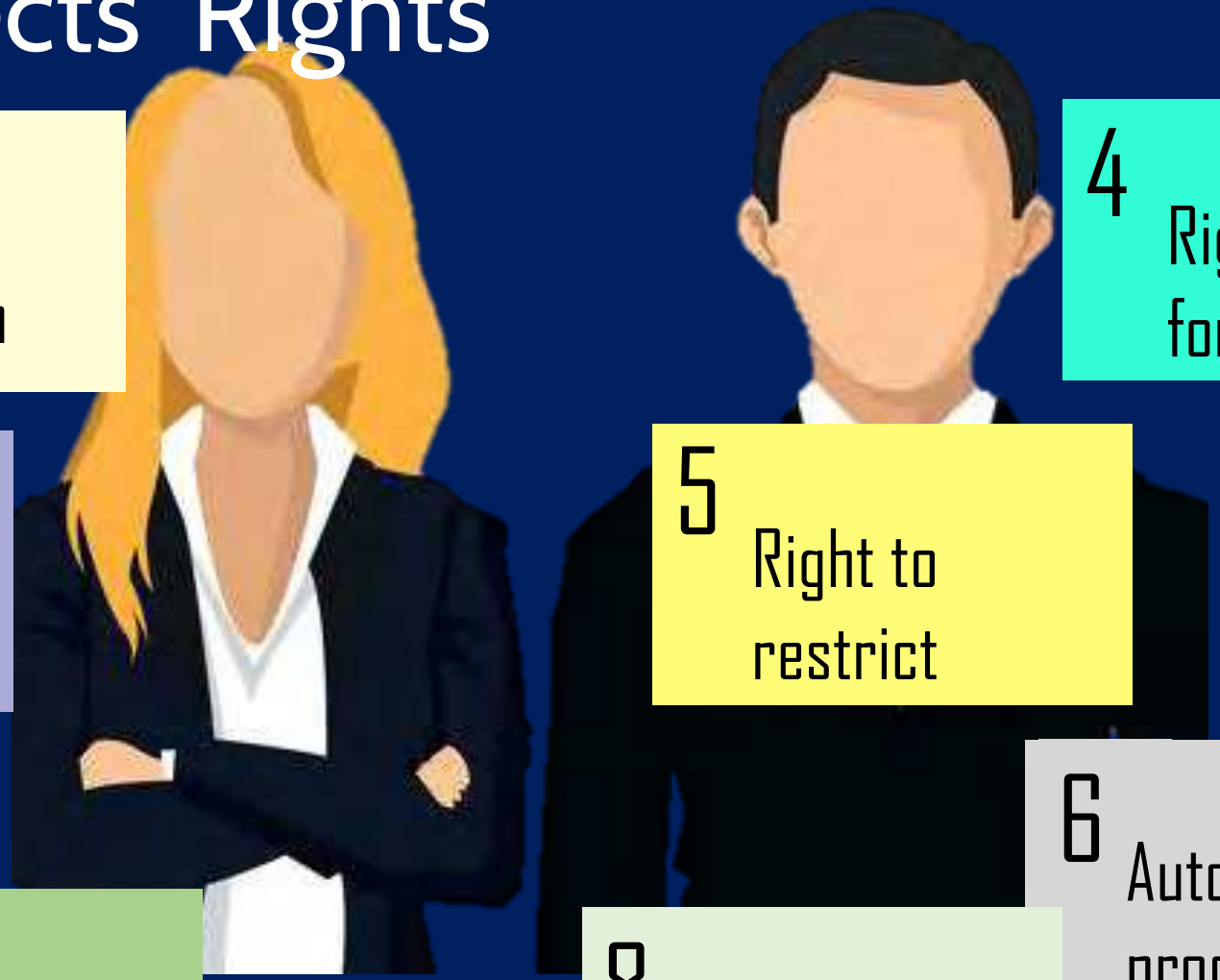


21 ACADEMY

Undergraduate Diploma

Data Subjects' Rights

Data Subjects' Rights



1 Right to information

2 Right of access

3 Right to rectify

4 Right to be forgotten

5 Right to restrict

6 Automated processing

7 Right to object

8 Data portability

21 ACADEMY

Undergraduate Diploma

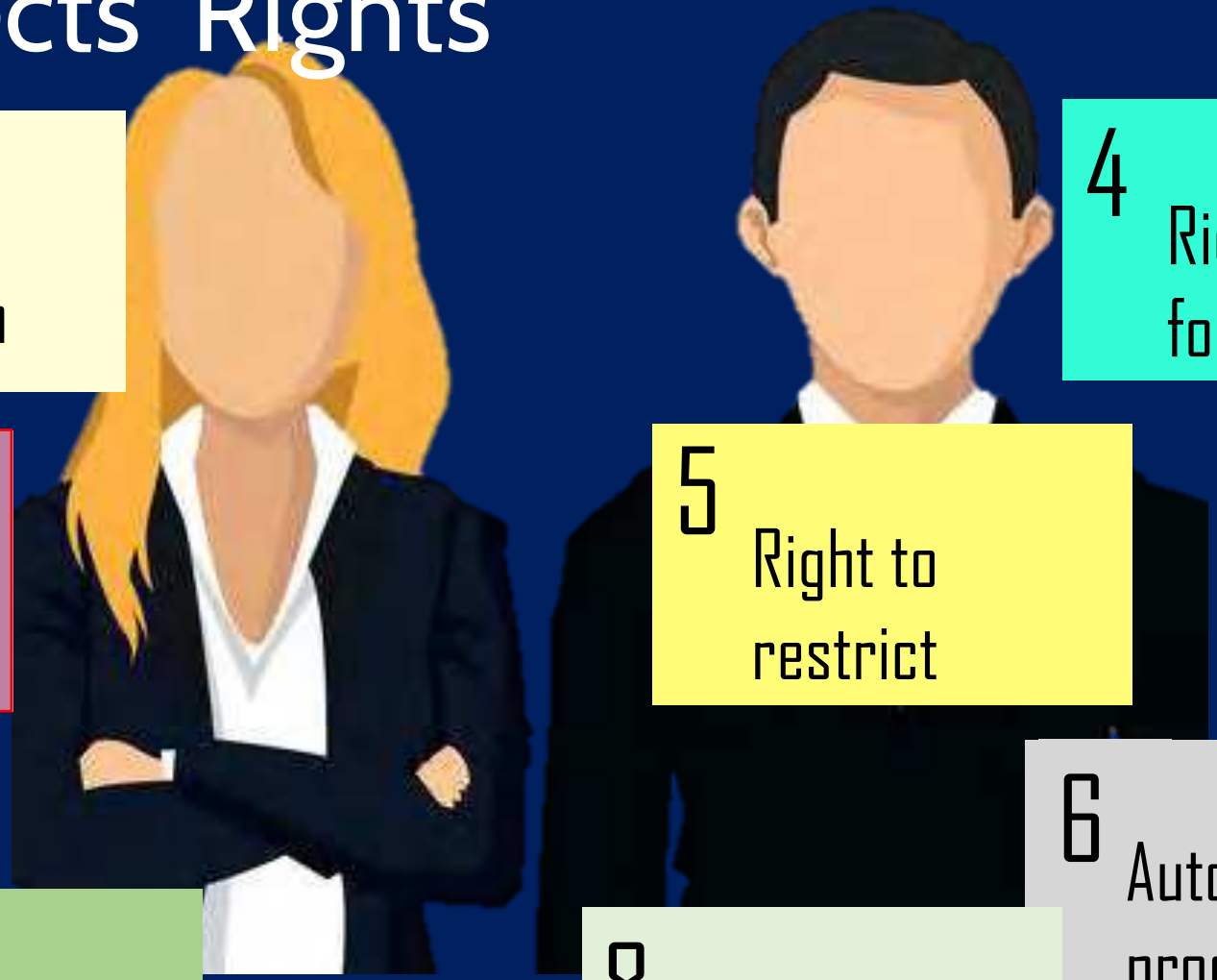
Subject Access Requests

The Right to SAR

A fundamental right under the Charter of Fundamental Rights of the European Union (2012/C 326/02)

Article 8(2) of the Charter states that "*everyone has the right of access to data*" which is collected about them.

Data Subjects' Rights



1. Right to information
2. Right of access
3. Right to rectify
4. Right to be forgotten
5. Right to restrict
6. Automated processing
7. Right to object
8. Data portability

Summary of rights

An employee has the right to obtain from an employer information as to whether or not personal data is being processed about him or her.

What's being advised to employees?

Alex Monaco
Senior Employment Solicitor

Summary of rights

If personal data is being processed, the employee is entitled to be given a copy of his or her personal data together with the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom data has been or will be disclosed;
- the period during which personal data will be retained

Summary of rights

- information on the source of the data;
- information regarding complaints and disputes;
- transfer of data outside the EEA (if any);

Transfer of Data outside the EEA

- Countries in the EEA
  - EU + Iceland, Liechtenstein and Norway
- Adequacy Decisions
  - Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom under the GDPR and the LED, the United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay .
- Standard Contractual Clauses
- Binding Corporate Rules

Highest Fines

Meta

€1.2 billion

- Ireland's Data Protection Commission
- Transfer of data to the United States
- Meta used basis to transfer data which do not comply with EU Law - Privacy Shield

Summary of rights cont.

The information must be provided free of charge (Article 12.5).

The employer must provide the information without undue delay and, in any event, within one month of receipt of the request.

Approach

Employer should approach compliance in a positive and helpful way:

- The employer must facilitate the exercise of the subject access right (Article 12.2).
- The request must be handled fairly and transparently (Article 5.1(a)).
- Information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language (Article 12.1).

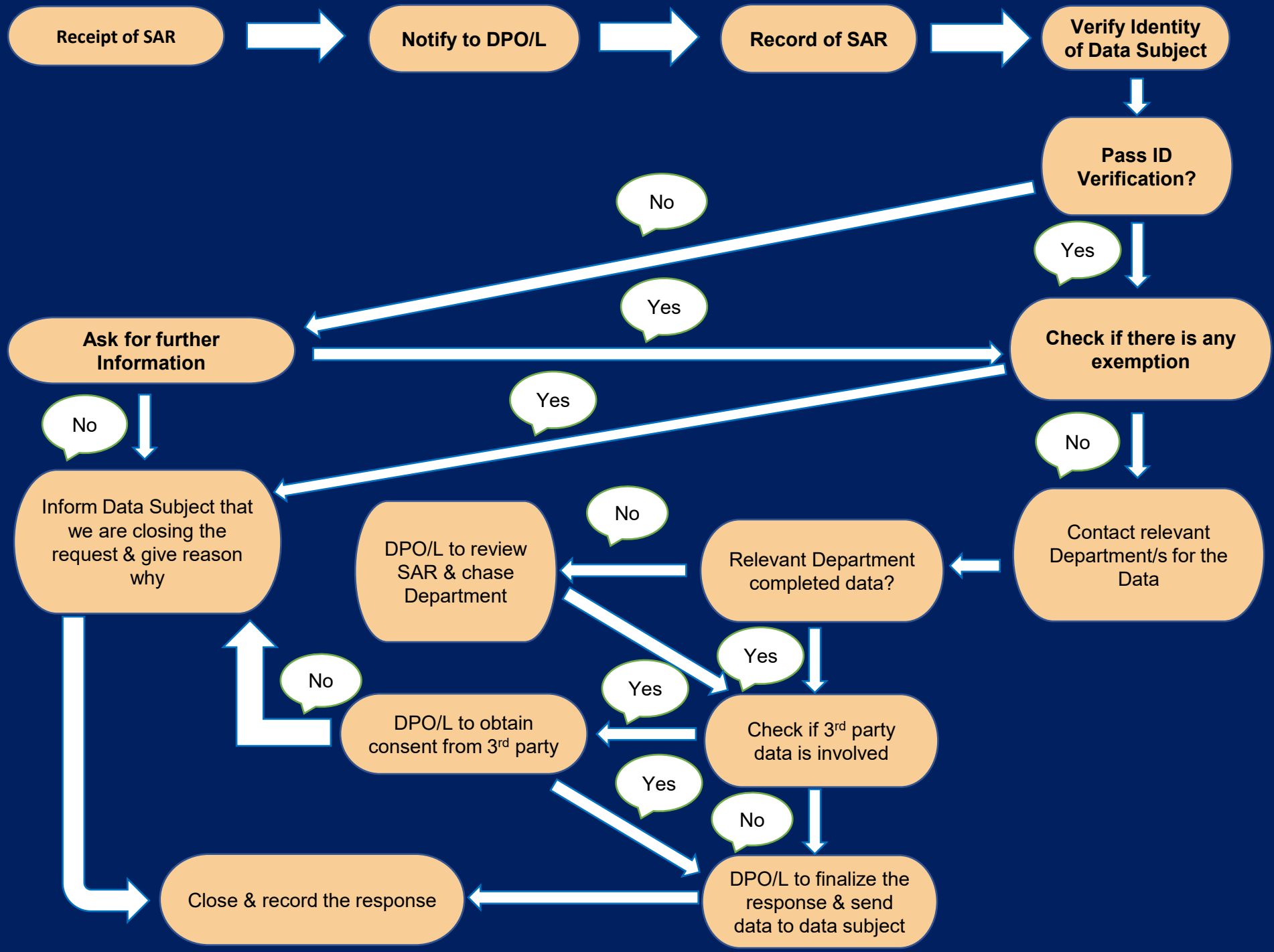
Receiving a SAR

A SAR may be made:

- in writing
- email
- other electronic means and,
- verbally

Employer should provide means for requests to be made electronically

Set out a preferred method of contact


Receipt of SAR
Notify to DPO/L
Record of SAR
Verify Identity of Data Subject
Pass ID Verification?
No
Yes
Ask for further Information
Yes
Check if there is any exemption
No
Yes
No
Inform Data Subject that we are closing the request & give reason why
DPO/L to review SAR & chase Department
No
Relevant Department completed data?
Contact relevant Department/s for the Data
Yes
No
Yes
DPO/L to obtain consent from 3rd party
Check if 3rd party data is involved
Yes
No
Close & record the response
DPO/L to finalize the response & send data to data subject

Responding to a request

Initial assessment

- Is data concerning the employee processed?
- Respond or not?
- Scope behind the request?
- Approach to find the data and response.

Responding to a request

Checking identity of person making request

- make sure that a person is lawfully authorised to act on behalf a data subject
- no exceptions for family members

Responding to a request

Timing

- basic rule is that requests must be handled without undue delay and, in any case, within one month of the receipt of the request
- (may) extend by 2 months were necessary (complexity and number of requests)
- inform data subject within a month

Responding to a request

Understanding what the data subject wants

- ask the data subject in more detail what information he or she is after
- aim of the request should not be to narrow the scope

Responding to a request

Manifestly unfounded or excessive requests

- Charge a reasonable fee.
- Refuse to act on the request.

Need to demonstrate that the request is indeed manifestly unfounded or excessive

Responding to a request

Form of response

- Writing
- Electronic means
- Orally (following a request by employee)

Ideal Scenario

- Policy on handling a SAR
- Response procedure
- Form (one for each subject right)
- Tracking form
- Letters
- Logbook

21 ACADEMY

Undergraduate Diploma

Managing Data and its Implications

Lecture Title: Compliance with Data Privacy Legislation

Lecturer: Angelito Sciberras

Date: 26 February 2025

Undergraduate Diploma