Managing Data and Its Implications

Tutorial Title: Tutorial 01

Lecturer: Angelito Sciberras

Date: 24 March 2025

Undergraduate Diploma

Today's Session

- Self Assessment 30 minutes
- The Group Presentation

Today's Session

- Self Assessment 30 minutes

The group presentation question

Question

Prepare and deliver a presentation that explains how a digital marketing agency should respond to and investigate a personal data breach in compliance with the General Data Protection Regulation (GDPR).

Your presentation must:

1. Explain What a Data Breach Is

- Define a personal data breach under GDPR
- Provide digital marketing examples of three data breaches that occurred in 2025

Question

2. Develop a Step-by-Step Data Breach Investigation Procedure

Your procedure must begin from the moment the breach is discovered and end when the investigation is formally closed.

3. Include a Visual Flowchart

Create a clear process flowchart showing each stage of the investigation from detection to closure.

Presentation Question

KEY POINTS
Data Breach

Detail
What is a Data Breach?
Examples of 3 digital marketing data breaches that happened in 2025?

Step by Step procedure - flow chart

Reflective Notes

- Friday 27 March at 23.59hrs
  - What did I Learn? (100 words)
  - What went well? (100 words)
  - What could I have done better? (100 words)
  - Long-term implications (200 words)

21 ACADEMY

Undergraduate Diploma

Data Breaches

a breach of security leading to the accidental or unlawful

- destruction,
- loss,
- alteration,
- unauthorised disclosure of, or
- access to,

personal data transmitted, stored or otherwise processed.

Data Breaches

Access to data by unauthorised individuals

Lost or stolen devices

Sending an email with multiple recipients not in BCC

Email sent to the wrong recepient

Accidental destruction of data

Unintended publication

Data of wrong person shown

Types of Data Breaches - CIA

- **Confidentiality breach** - where there is an unauthorised or accidental **disclosure** of, or **access** to, personal data; or

- **Integrity breach** - where there is an unauthorised or accidental **alteration** of personal data

- **Availability breach** - where there is an accidental or unauthorised **loss** of access to, or **destruction** of, personal data.

Data Breach Policy

- Identification of suspected breach
- Reporting a security incident
- Response to security incident
- Investigating Team members
- Establishing a personal data breach
- Notifying the Supervisory Authority
- Notifying the data subjects
- Evaluation and response

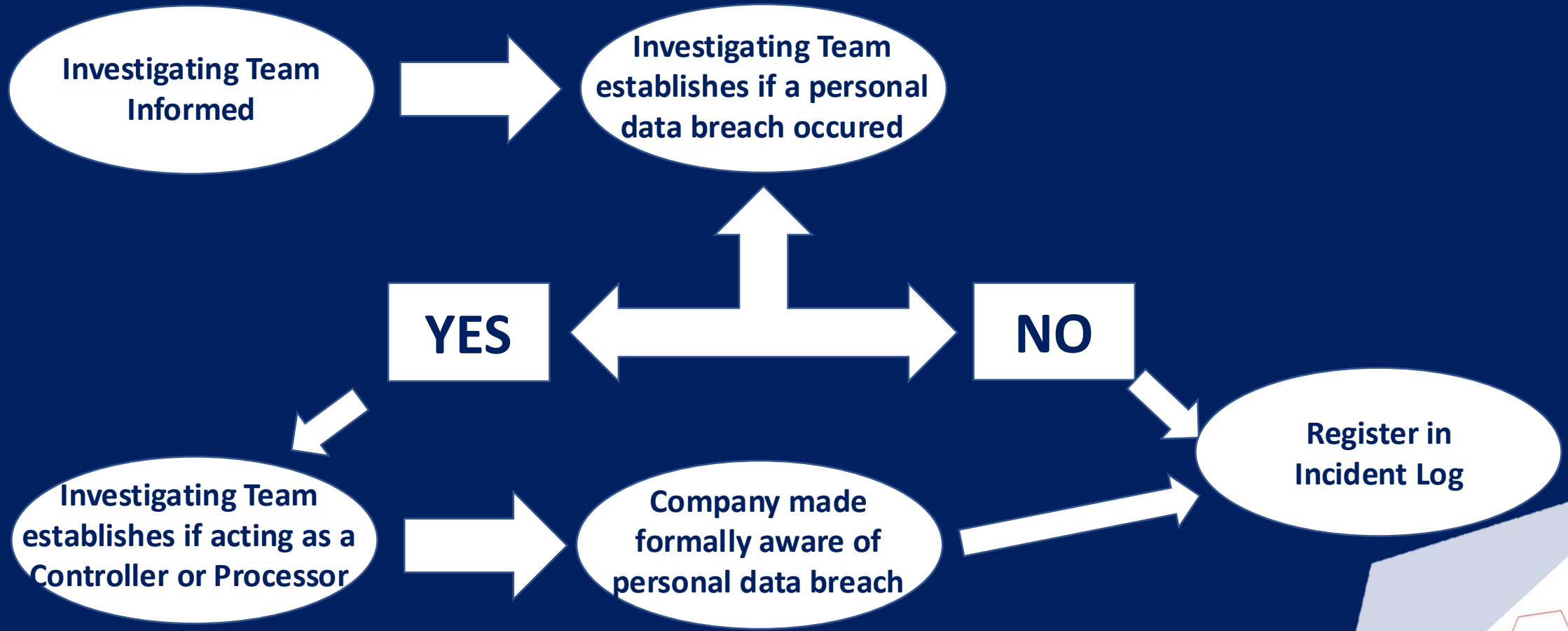
Data Breach Policy

- Reporting a security incident
  - Make it easy
  - Identify who has to report to who reporting chain
  - Have a form

Data Breach Policy

- Incident form
  - Date of incident
  - Time of Incident
  - Date the incident was discovered
  - Identification of person reporting the incident
  - Incident description - including type of data
  - Number of involved data subjects
  - Action taken at time of discovery

Data Breach Policy



Data Breach Policy

Data Breach Assessment

Factors	Reasoning	Conclusion (No/Low/Medium/High Risk)
Type of breach		
Nature, sensitivity and volume of personal data		
Ease of identification of individuals		
Severity of consequences for individuals		
Special characteristics of the individual		
Special characteristics of the controller		
Number of affected individuals		
Overall conclusion*	Likelihood of risk = No/Low/Medium/High Risk Severity of risk = No/Low/Medium/High Risk Conclusion = No/Low/Medium/High Risk	

Data Breach Assessment

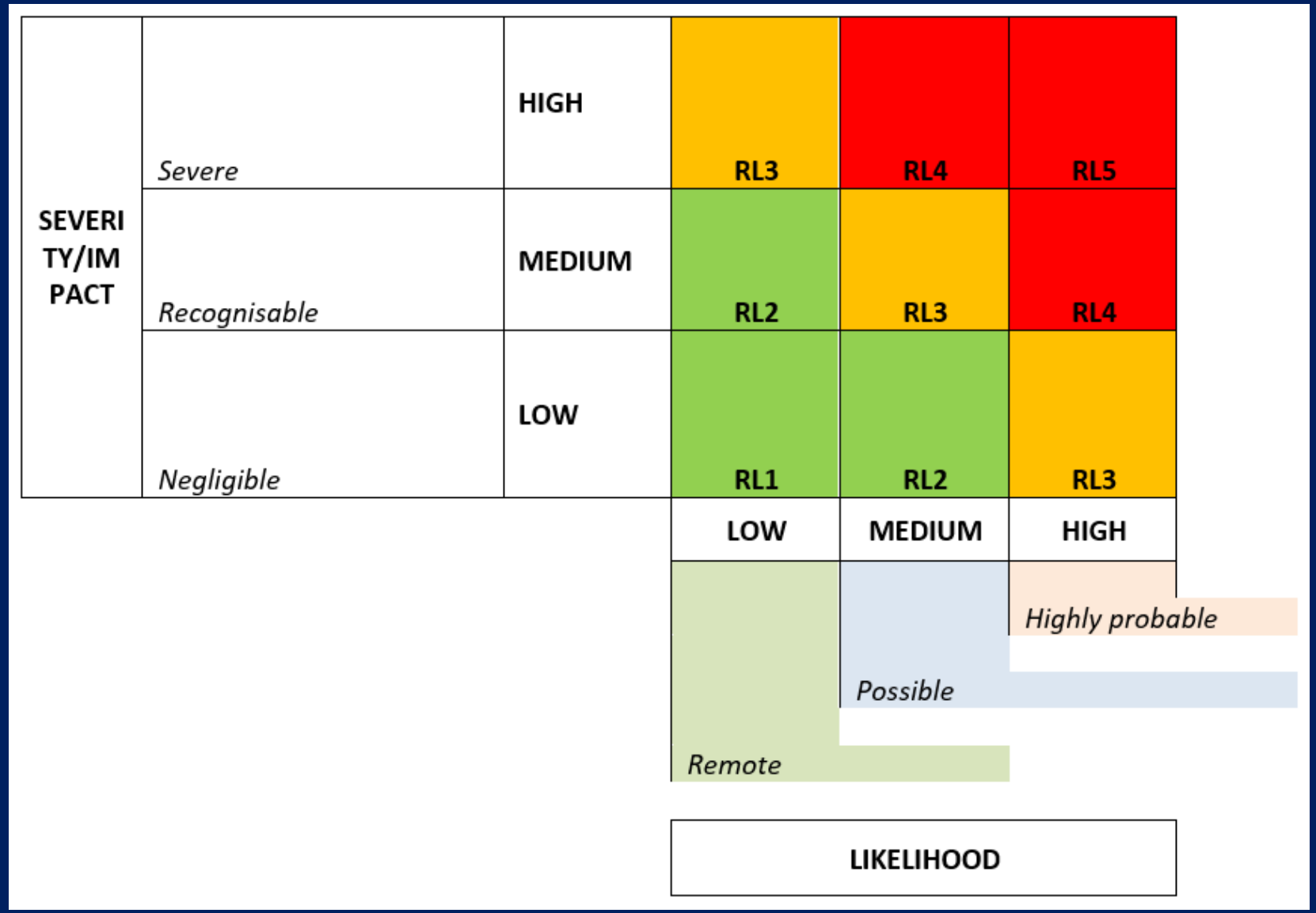
Severity of the Impact

- Negligible
- Recognisable
- Severe

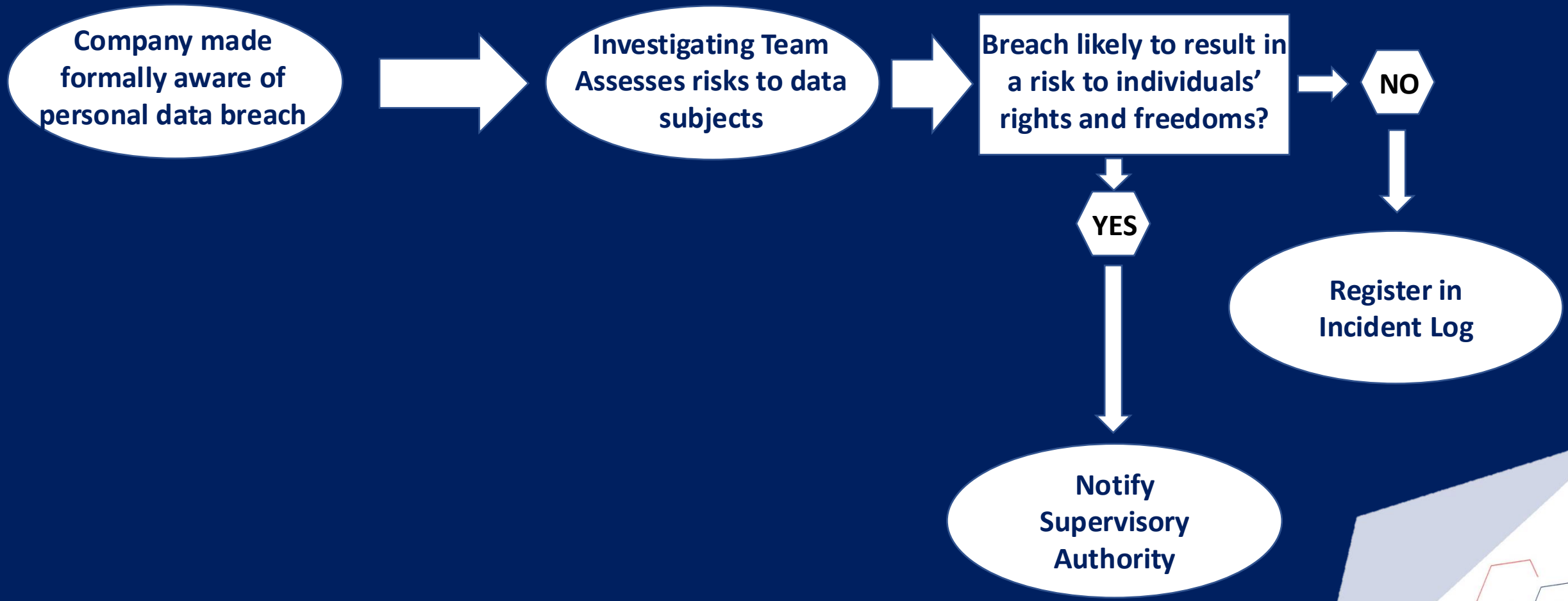
Likelihood of risk occuring

- Remote
- Possible
- Highly Probable

Data Breach Assessment



Data Breach Policy



Notifying Supervisory Authority

- Description of what happened?
- How did the incident occur?
- How was it discovered?
- What preventative measures where in place?
- Was breach caused by a cyber incident?
- Data and Time of breach?
- Data and time of discovery?

Notifying Supervisory Authority

- Categories of personal data included in the breach
- Number of personal records
- Number of affected data subjects
- Categories of data subjects
- Describe detriment
- If you anticipate high risk give details

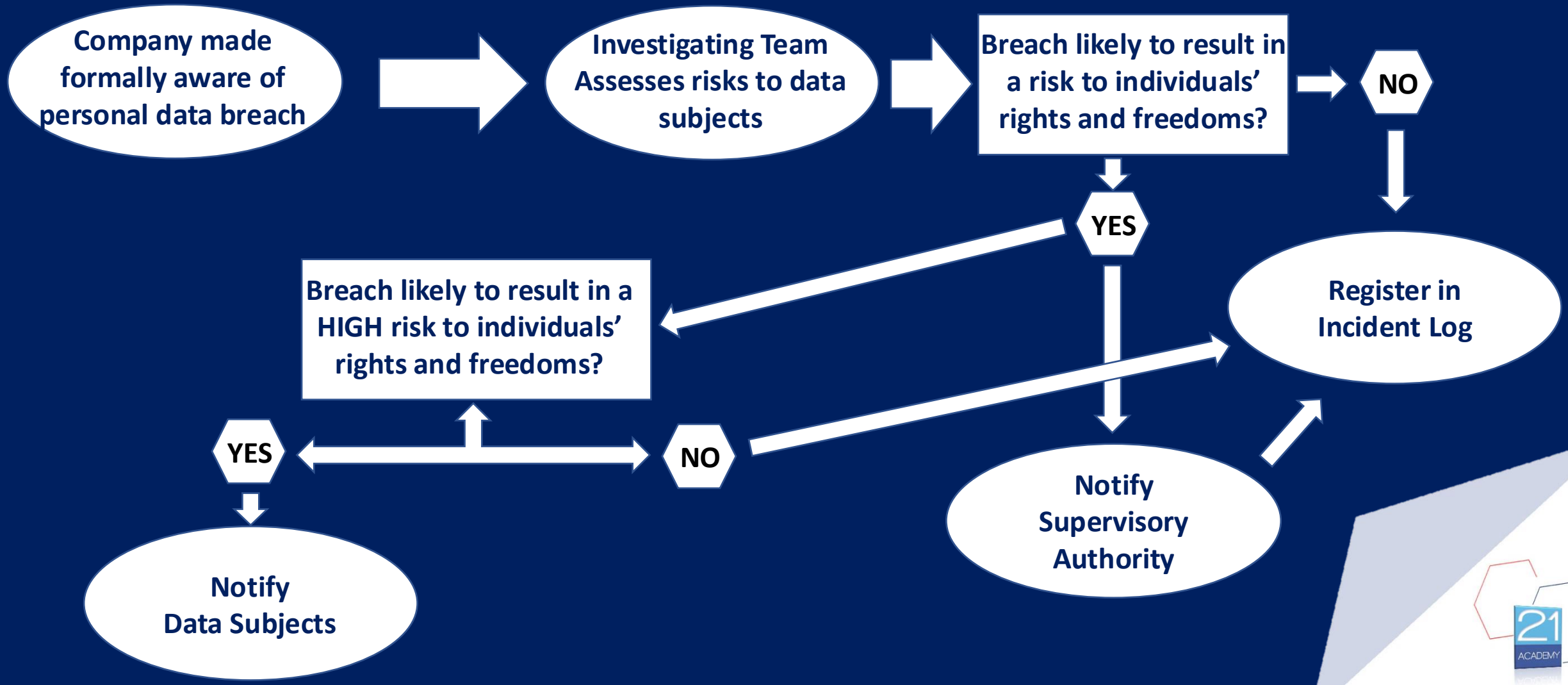
Notifying Supervisory Authority

- Cyber Incidents
  - Was the data recovered, can be recovered or unable to restore
- Were the employees involved trained in the last years
- Describe training
- In case of a delayed report explain why
- Action taken to contain breach
- Action taken or to be taken to avoid a repeat - timeline

Notifying Supervisory Authority

- Any anticipated further action
- Informed or planning to inform any other organisation and why
- Were data subjects informed? Why?

Data Breach Policy



Notifying the Data Subjects

- Describe, in clear and plain language, the nature of the personal data breach
- Name and contact details of DPO, or other contact point
- Description of the likely consequences of the personal data breach
- Description of the measures taken or proposed to deal with the personal data breach
- Description of the measures taken to mitigate any possible adverse eff

Notifying the Data Subjects

- Give specific and clear advice to individuals on the steps they can take to protect themselves, and what you are willing to do to help them.

  - forcing a password reset;
  - advising individuals to use strong, unique passwords; and
  - telling them to look out for phishing emails or fraudulent activity on their accounts.

Notifying the Data Subjects

Notice of cyber security incident – be alert to phishing emails

Dear Customer,

I wanted to write to you personally in regards to a recent cyber security incident at easyJet.

As you may have heard, we announced on 19th May 2020 that we were the target of an attack from a highly sophisticated source. As soon as we became aware of the attack, we took immediate steps to manage and respond to the incident, closing off the unauthorised access. We engaged leading forensic experts to investigate the issue and we also notified the National Cyber Security Centre and the Information Commissioner's Office (ICO).

Our investigation found that your name, email address, and travel details were accessed for the easyJet flights or easyJet holidays you booked between 17th October 2019 and 4th March 2020. **Your passport and credit card details were not accessed**, however information including where you were travelling from and to, your departure date, booking reference number, the booking date and the value of the booking were accessed.

We are very sorry this has happened.

Please be extra careful about phishing attacks

There is no evidence that personal information of any nature has been misused but please do be extra careful if you receive any unsolicited communications, particularly if they claim to be from either easyJet or easyJet holidays. Please note that we will never contact you unprompted to ask for your account details or security information, and we will never ask you to disclose your passwords, or to change your passwords on your easyJet account.

You do not need to take any action apart from continuing to be alert as you would normally be, especially with any unsolicited communications. To help you stay safe online, please remember:

- Do not open emails or attachments if you have any questions on the source
- Make sure you know who you are dealing with before disclosing any personal information online
- Always check links before clicking on them – you can do this by hovering over the link to see whether the source is recognisable. Do not click any link if you are unsure

The ICO has very helpful information on its website, including an article related to phishing posted on 31st March 2020 entitled 'Stay One Step Ahead of the Scammers'. The National Cyber Security Centre likewise has useful guidance, including an article entitled 'Phishing attacks: dealing with suspicious emails and messages'.

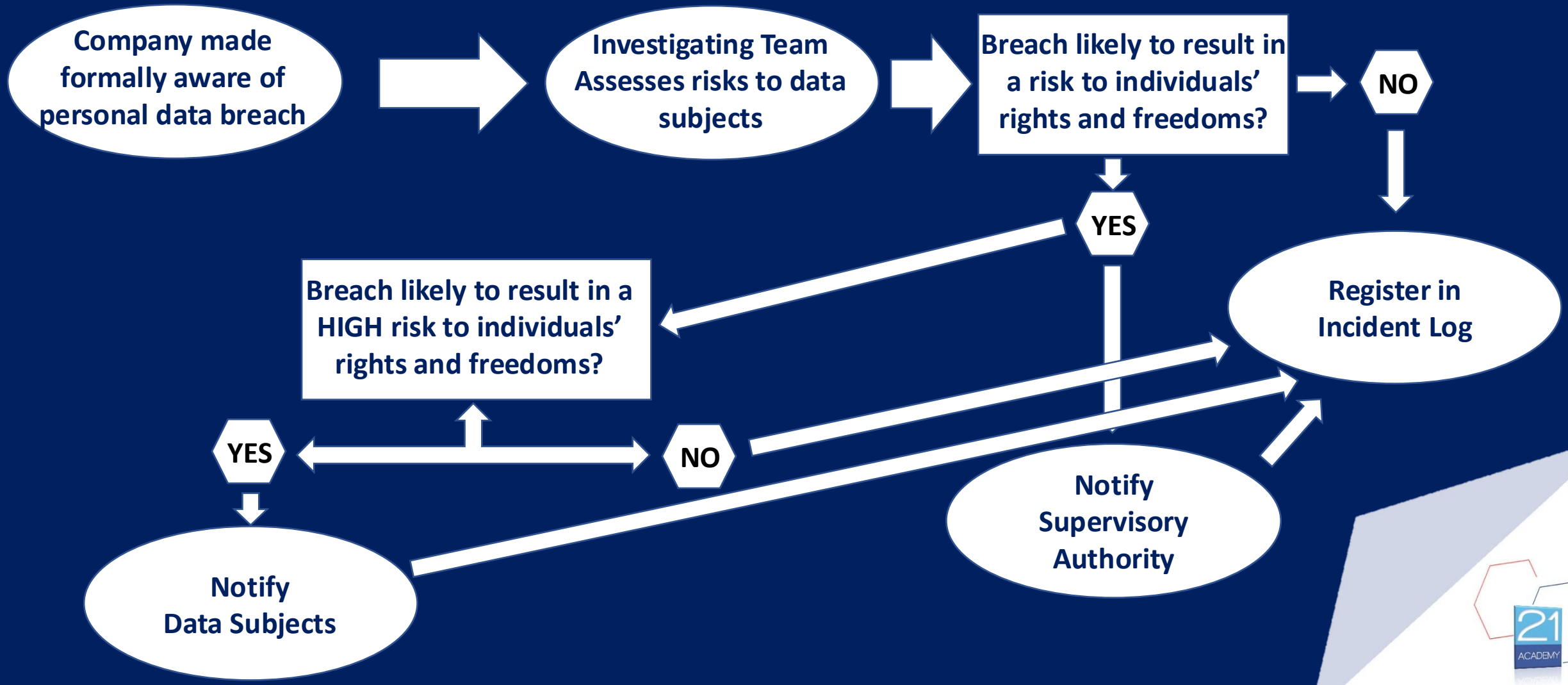
More information on the cyber incident with easyJet can be found on our website. Additionally, if you have any further questions, please email us at infoalert@easyjet.com

Once again, we're sorry that this attack has happened. We do take the safety and security of our customers' information very seriously and will continue to take every action to protect it against any future attacks.

Yours sincerely,

Johan Lundgren
CEO, easyJet

Data Breach Policy



21 ACADEMY

Undergraduate Diploma

Managing Data and Its Implications

Tutorial Title: Tutorial 01

Lecturer: Angelito Sciberras

Date: 24 March 2025

Undergraduate Diploma