

Managing Data and its Implications

Lecture Title: Implications on Business Part II



Lecturer: Angelito Sciberras

Date: 17 March 2026

Undergraduate Diploma

The assignment questions



Question 01

Explain how the General Data Protection Regulation (GDPR) affects digital marketing activities.

In your answer, describe:

What personal data is in a digital marketing context

The lawful bases for processing marketing data

The role of consent in email and online marketing

The importance of transparency and privacy notices

The risks of non-compliance for businesses

Provide practical examples from digital marketing to support your explanation.



Question 02

Create a detailed checklist that a business can use to make sure it follows European data protection laws. Clearly explain why each item on the checklist is important.



Question 03

Explain what a Subject Access Request (SAR) is and why it is important for both individuals and organisations.

Include examples relevant to a business context.

Develop a step-by-step procedure that a business should follow when processing a SAR, starting from the point the request is received until the individual receives a copy of the requested data.



Question 03

Your procedure should cover: How the request is recorded and acknowledged

Verification of the requester's identity

Assessment and clarification of the request (if needed)

Locating and reviewing the relevant personal data

Handling exemptions or third-party data

Responding within GDPR time limits

Securely providing the data to the requester

Recording and documenting the process

Present your procedure visually using a flowchart or diagram to clearly show the sequence of steps from receipt of the SAR to completion.

Reflect briefly on the challenges an organisation might face when handling SARs and how these can be mitigated.



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.



Managing Data and its Implications

Lecture Title: Implications on Business Part II



Lecturer: Angelito Sciberras

Date: 17 March 2026

Undergraduate Diploma

Last Lecture

- Most effected departments in a business
- Checklist
- Policies and Procedures a company shoud have
- Monitoring
- Data Inventory
- Data Processing Agreement
- Technical vs Organisational Measures
- IT Department



Which of the following is a must-have from the GDPR compliance checklist?

- a) Conduct regular employee training sessions on data protection
- b) Conduct regular customer satisfaction surveys
- c) Update the company logo on the website
- d) Organise team-building activities for employees



Which of the following is a must-have from the GDPR compliance checklist?

- a) Review and update company social media policies
- b) Review and update privacy notices and policies
- c) Schedule regular team meetings
- d) Conduct customer market research



Which of the following is a must-have from the GDPR compliance checklist?

- a) Implement measures to increase data collection
- b) Implement measures to ensure data accuracy and minimize data collection
- c) Implement measures to track employee attendance
- d) Implement measures to increase data sharing



Which of the following is a must-have from the GDPR compliance checklist?

- a) Review and update data processing agreements with third-party service providers
- b) Review and update the company's vacation policy
- c) Review and update employee dress code
- d) Review and update company mission statement



Which of the following is a must-have from the GDPR compliance checklist?

- a) Implement measures to ensure data security
- b) Implement measures to improve office decor
- c) Implement measures to enhance employee benefits
- d) Implement measures to increase marketing efforts



Which of the following is a must-have from the GDPR compliance checklist?

- a) Appoint a Chief Executive Officer (CEO)
- b) Appoint a Data Protection Officer (DPO)
- c) Appoint a Chief Financial Officer (CFO)
- d) Appoint a Chief Marketing Officer (CMO)



Which of the following is a must-have from the GDPR compliance checklist?

a) Establish procedures to respond to customer complaints only

b) Establish procedures to respond to data subject requests and complaints

c) Establish procedures to respond to employee complaints only

d) Establish procedures to respond to supplier complaints



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.



CIA

What's CIA Triad



What type of data breach is this?



Due to a technical glitch, a company's server crashes, making customer data temporarily inaccessible to authorised personnel.

- A. Confidentiality breach
- B. Integrity Breach
- C. Access Breach

What type of data breach is this?



A company's employee accidentally sends an email containing sensitive customer data to the wrong recipient.

- A. Confidentiality breach
- B. Integrity Breach
- C. Access Breach

What type of data breach is this?



An external attacker gains unauthorised access to a company's system and steals sensitive employee information, including social security numbers and bank account details.

- A. Confidentiality breach
- B. Integrity Breach
- C. Access Breach

What type of data breach is this?



A hacker gains unauthorised access to a database and modifies customer information, changing their addresses and contact details.

- A. Confidentiality breach
- B. Integrity Breach
- C. Access Breach

What type of data breach is this?



A company's employee mistakenly deletes a critical file containing customer records, rendering the data irretrievable

- A. Confidentiality breach
- B. Integrity Breach
- C. Access Breach

What type of data breach is this?



A malicious insider intentionally alters financial records of customers, modifying transaction amounts to divert funds.

- A. Confidentiality breach
- B. Integrity Breach
- C. Access Breach

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

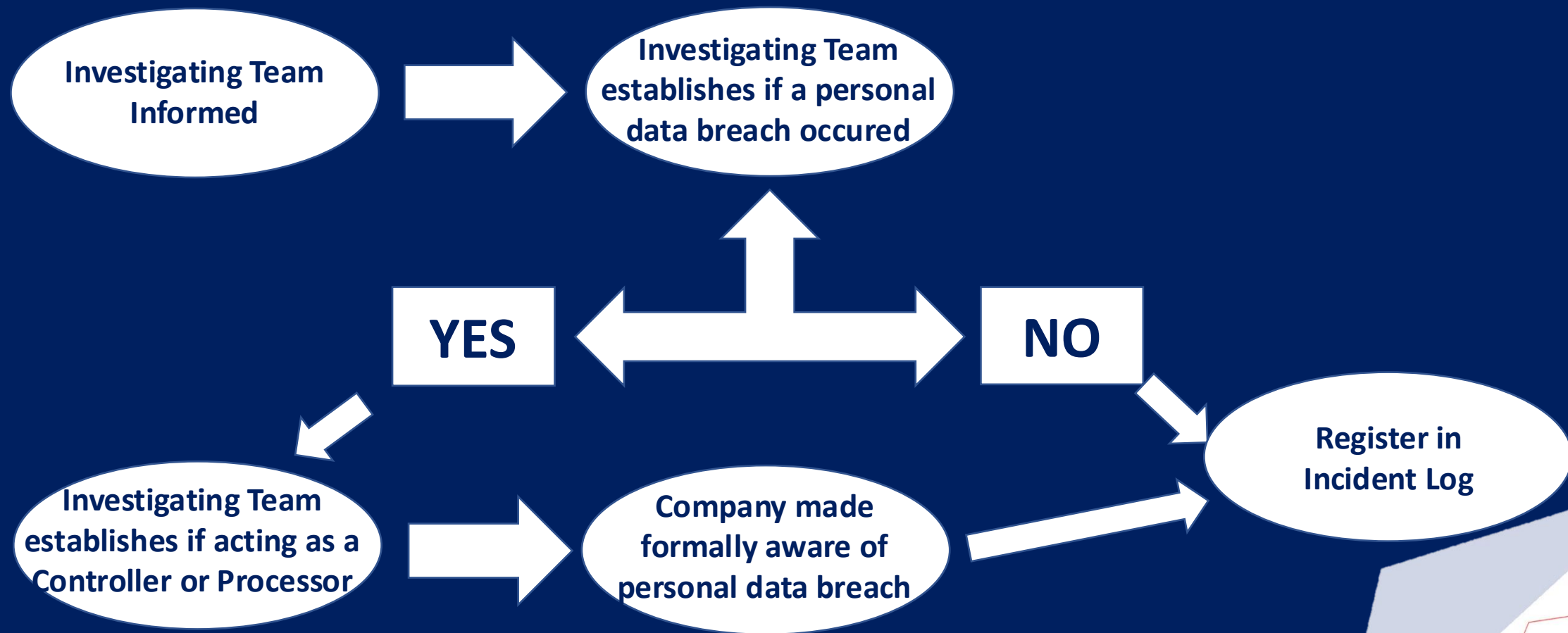


Data Breach Policy

- 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

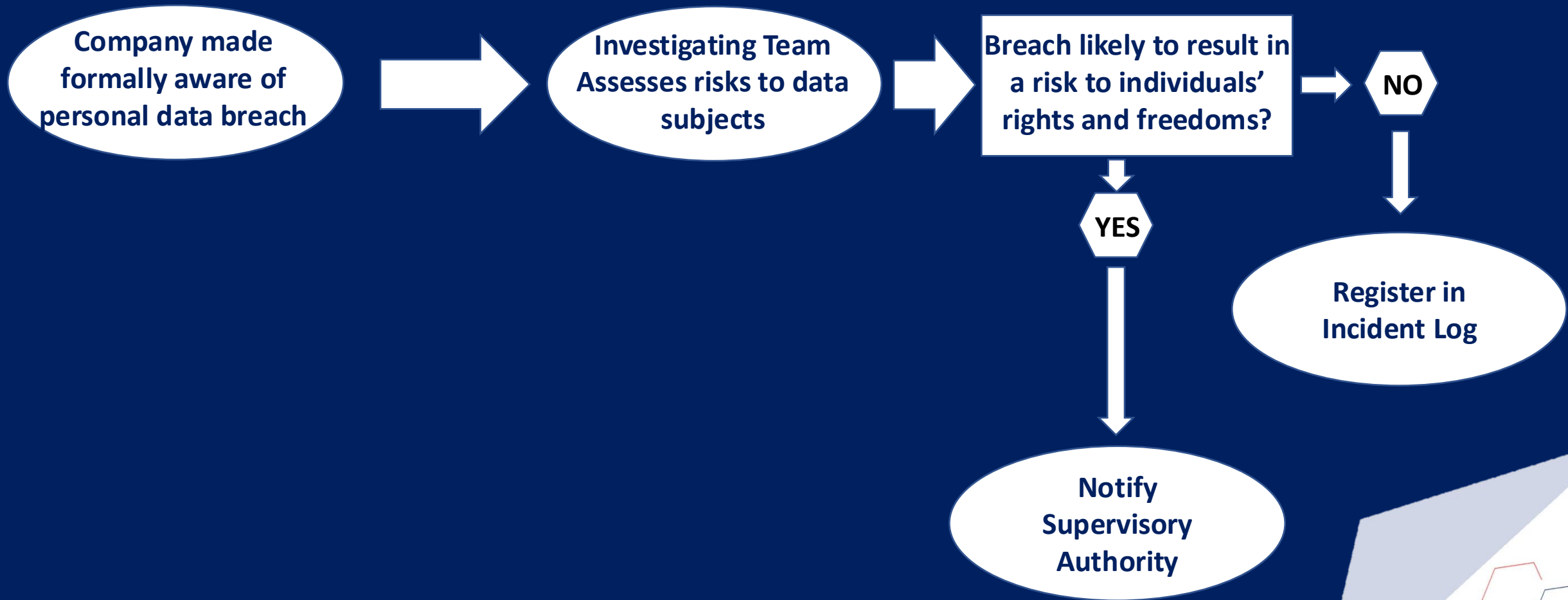
Likelihood of risk occurring

- Remote
- Possible
- Highly Probable

Data Breach Assessment

SEVERITY/IMPACT		HIGH	RL3	RL4	RL5
	Severe				
	Recognisable	MEDIUM	RL2	RL3	RL4
	Negligible	LOW	RL1	RL2	RL3
			LOW	MEDIUM	HIGH
			Remote	Possible	Highly probable
			LIKELIHOOD		

Data Breach Policy



Notifying Supervisory Authority

- Description of what happened?
- How did the incident occur?
- How was it discovered?
- What preventative measures were 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

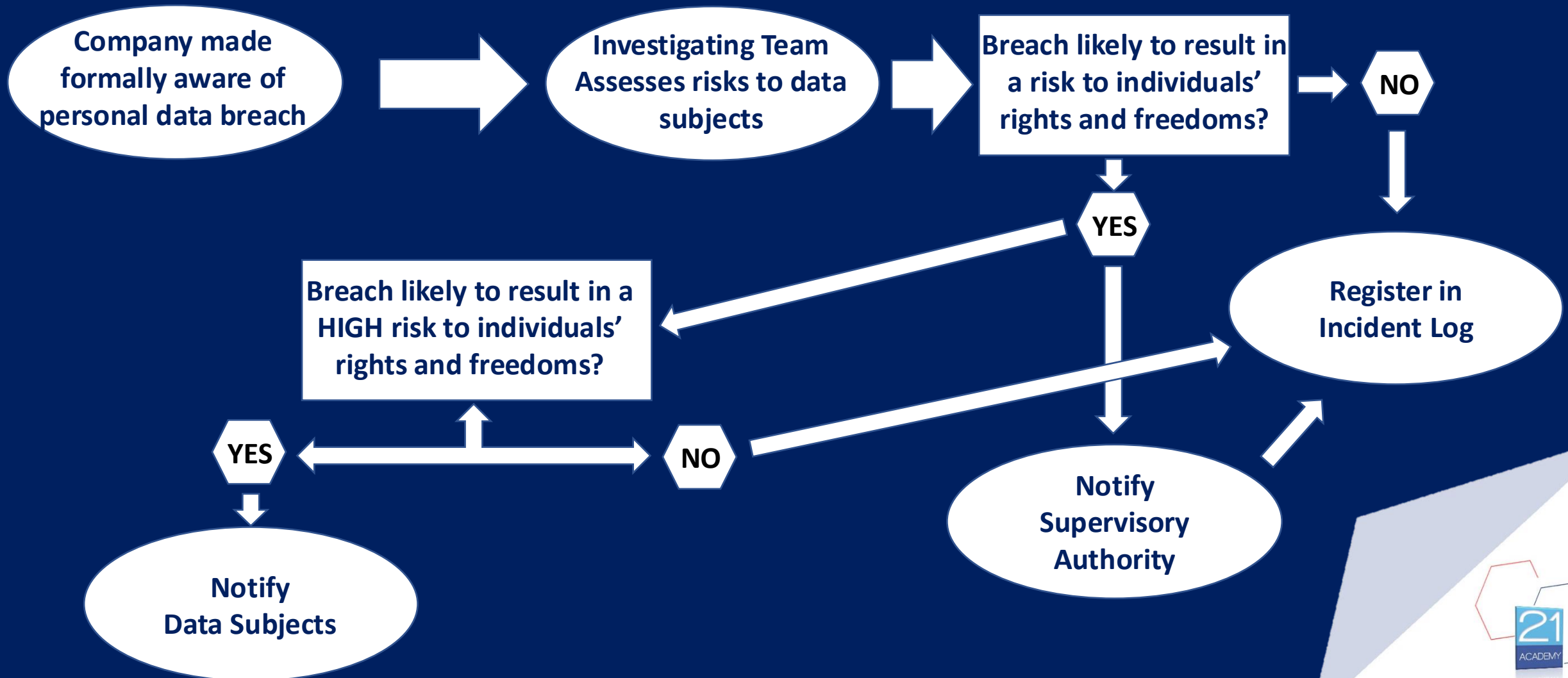


Notifying Supervisory Authority

- 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 effects



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

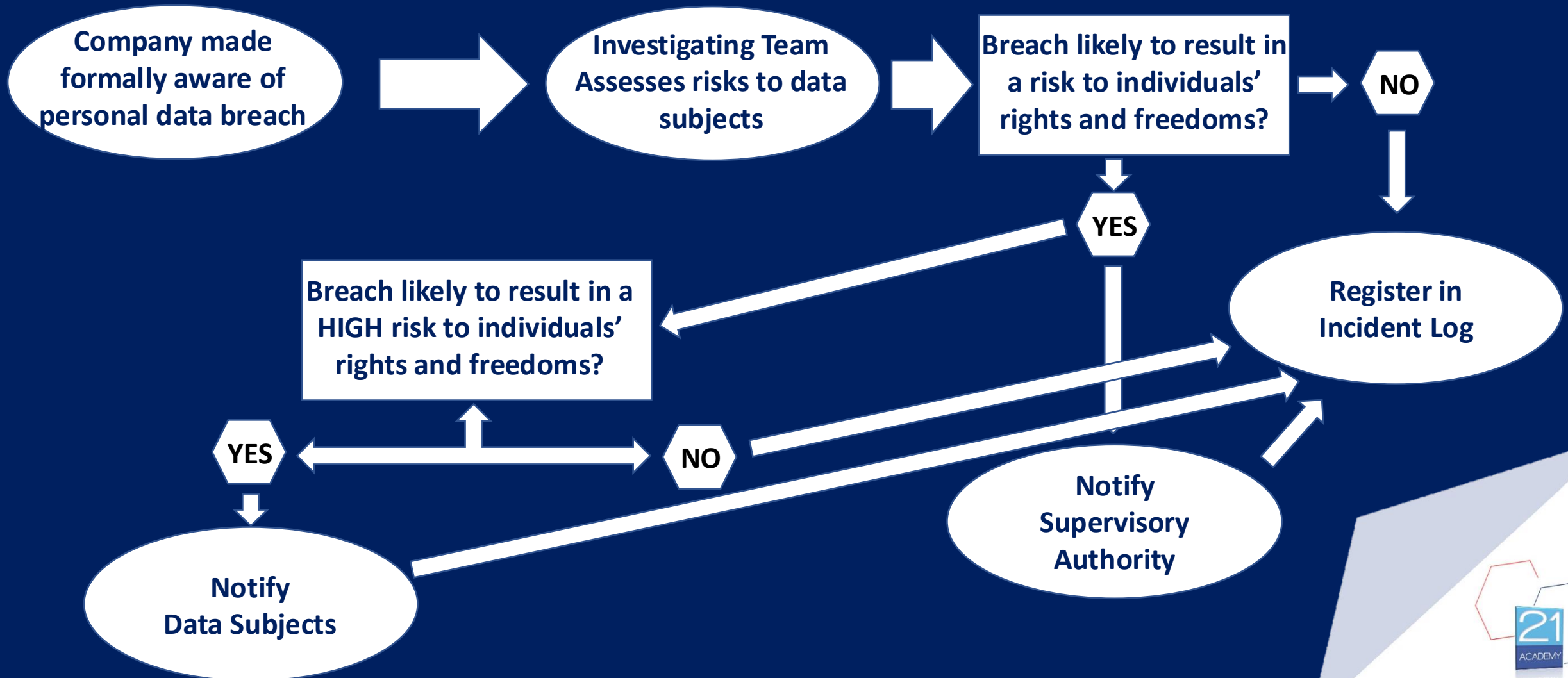
Once again, we're sorry that this attack has happened. We do take the safety and security of our customers' information very seriously and will continue to take every action to protect it against any future attacks.

Yours sincerely,

Johan Lundgren
CEO, easyJet



Data Breach Policy



Data Breaches



A small business experiences a data breach where unauthorised individuals gain access to customer names and email addresses. However, the breach does not include any sensitive personal information or financial data. The business 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, 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?



Undergraduate Diploma

Managing Data and its Implications

Lecture Title: Implications on Business Part II



Lecturer: Angelito Sciberras

Date: 11 March 2026

Undergraduate Diploma