

Managing Data and its Implications

Lecture Title: Internal Procedures



Lecturer: Angelito Sciberras

Date: 27 April 2024

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
- HR Department
- Marketing and Sales Department



For which purposes do employers process employees' personal data?

- A) To track employees' social media activities
- B) To enhance workplace diversity and inclusion
- C) To sell personal data to third-party companies

D) To comply with legal obligations and manage employment contracts



For which purposes do employers process employees' personal data?

- A) To monitor employees' political affiliations
- B) To provide personalised advertising
- C) To assess job applicants for unrelated positions
- D) To manage payroll and benefits administration



For which purposes do employers process employees' personal data?

- A) To influence their personal lifestyle choices
- B) To conduct market research
- C) To ensure workplace safety and security
- D) To access employees' personal financial information



Which of the following scenarios represents a flaw in marketing compliance with GDPR?

- A) Obtaining explicit consent from individuals before sending marketing emails
- B) Providing individuals with an option to unsubscribe from marketing communications
- C) Collecting and using personal data only for specified and legitimate purposes
- D) Purchasing email lists from third-party vendors without verifying the consent of individuals



Which of the following scenarios represents a flaw in marketing compliance with GDPR?

- A) Implementing strong security measures to protect personal data from unauthorised access
- B) Maintaining clear records of individuals' consent to receive marketing communications
- C) Obtaining explicit consent from individuals for each marketing communication channel used
- D) Sharing individuals' personal data with marketing partners in the absence of data sharing agreements



Which of the following scenarios represents a flaw in marketing compliance with GDPR?

A) Retaining individuals' personal data for longer than necessary for the intended purposes

B) Providing individuals with the right to access and rectify their personal data

C) Encrypting personal data to ensure its confidentiality during storage and transmission

D) Implementing strict data protection policies and procedures for marketing campaigns



Which of the following practices is considered a good IT practice to prevent data breaches?

A) Sharing passwords with colleagues for easier collaboration

B) Using strong and unique passwords for each online account

C) Leaving sensitive information on unencrypted devices

D) Disabling firewalls and antivirus software for better system performance



Which of the following practices is considered a good IT practice to prevent data breaches?

- A) Ignoring software updates and patches
- B) Allowing employees to use personal devices for work purposes without any security measures
- C) Regularly conducting vulnerability assessments and penetration testing
- D) Storing sensitive data on public cloud servers without any encryption



Which of the following practices is considered a good IT practice to prevent data breaches?

- A) Sharing confidential information through unsecured email accounts
- B) Allowing unrestricted access to sensitive data for all employees
- C) Enforcing strict access controls and user permissions
- D) Using the same login credentials for multiple online accounts



Internal Procedures

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



Data Breaches

15:00



Give examples of data breaches

How do they happen?

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 recipient

Accidental destruction of data

Unintended publication

Data of wrong person shown



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

15:00



Undergraduate Diploma

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.



What type of data breach is this?



Due to a technical glitch, a company's server crashes, making customer data temporarily inaccessible to authorized 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 unauthorized 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

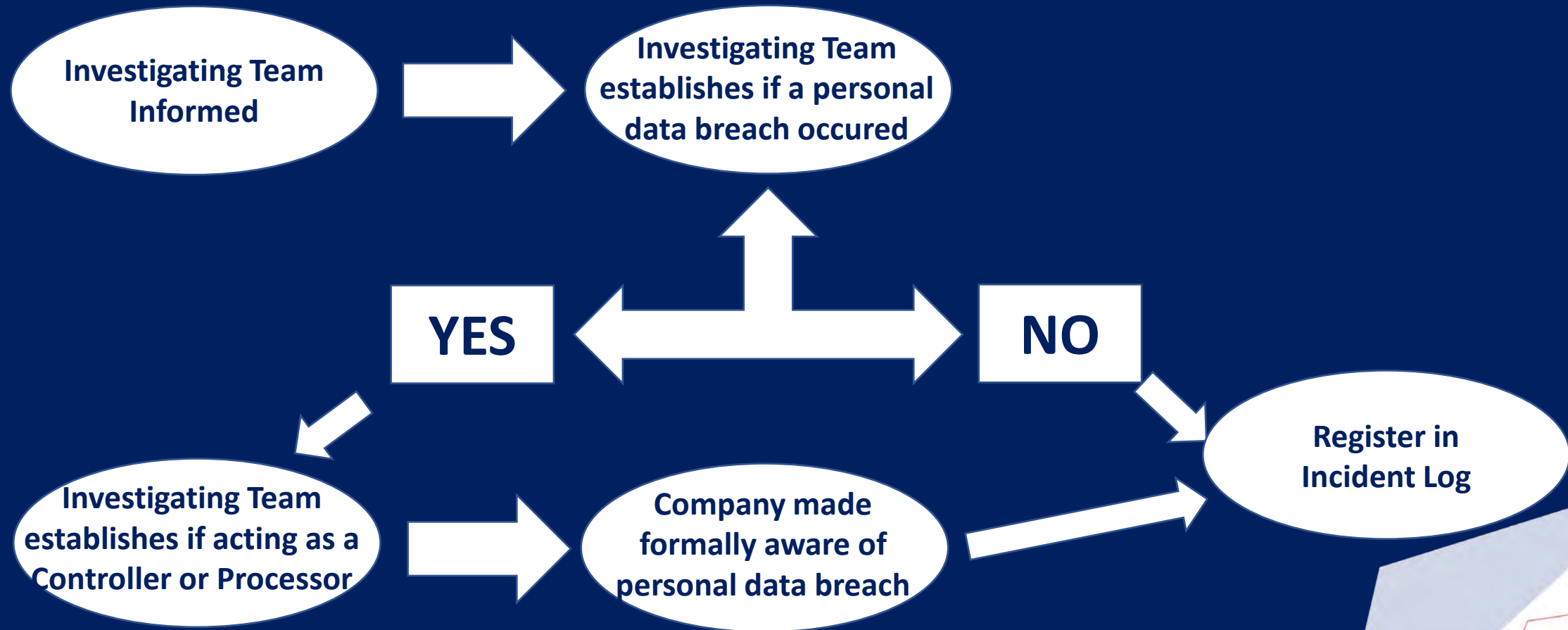


Data Breach Policy

- Incident form
 - Date of incident
 - Time of Incident
 - Date the incident was discovered
 - Identification of person reporting the incident
 - Incident description - incl. 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	Severe	HIGH	RL3	RL4	RL5
	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

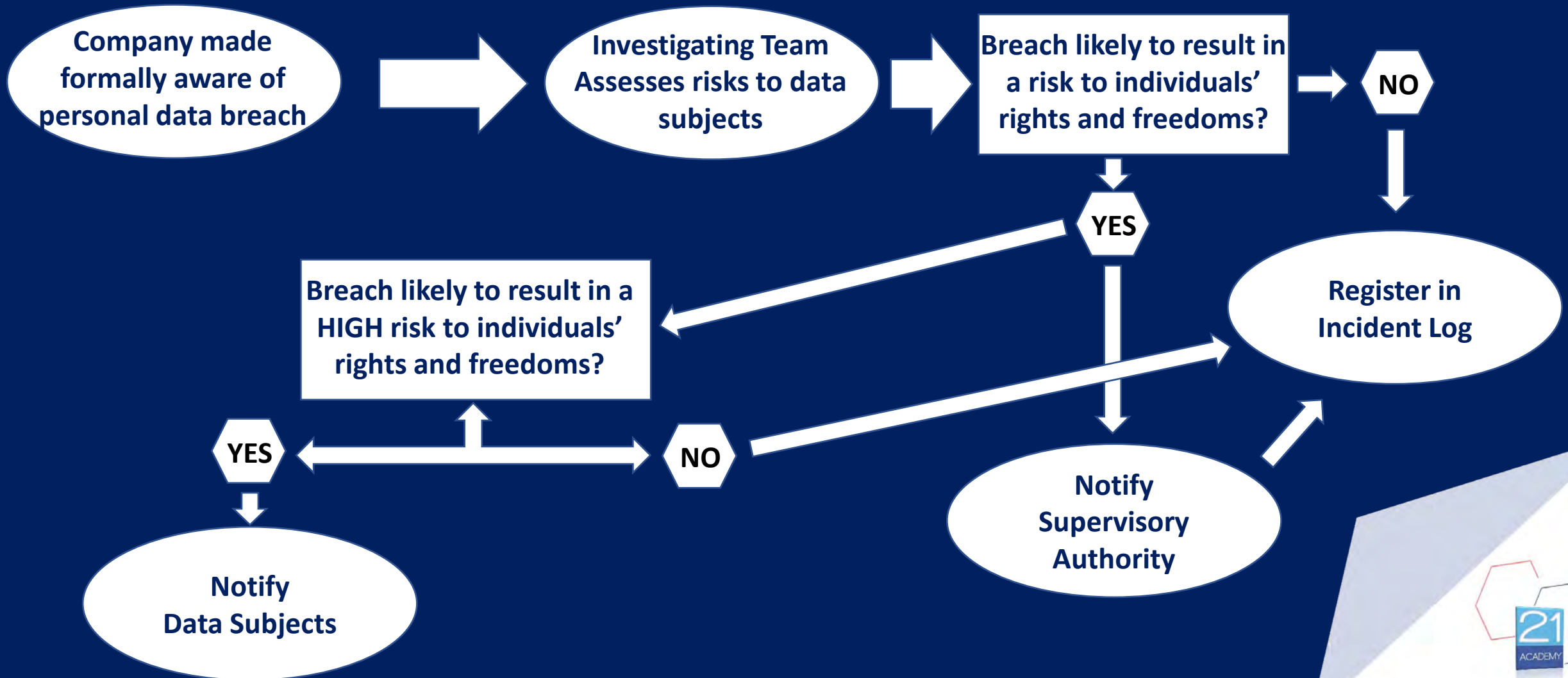


Notifying Supervisory Authority

- 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

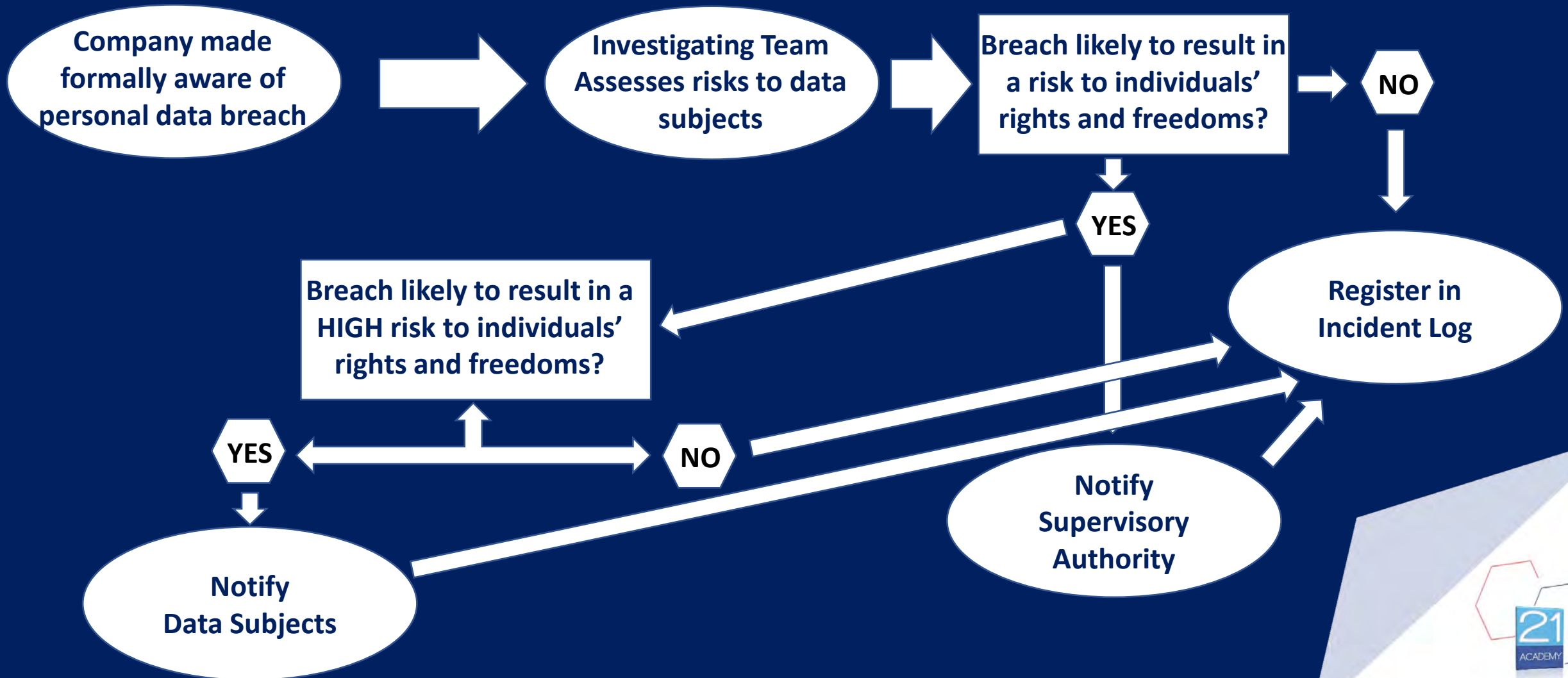
Once again, we're sorry that this attack has happened. We do take the safety and security of our customers' information very seriously and will continue to take every action to protect it against any future attacks.

Yours sincerely,

Johan Lundgren
CEO, easyJet



Data Breach Policy



Data Breaches

10:00



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

10:00

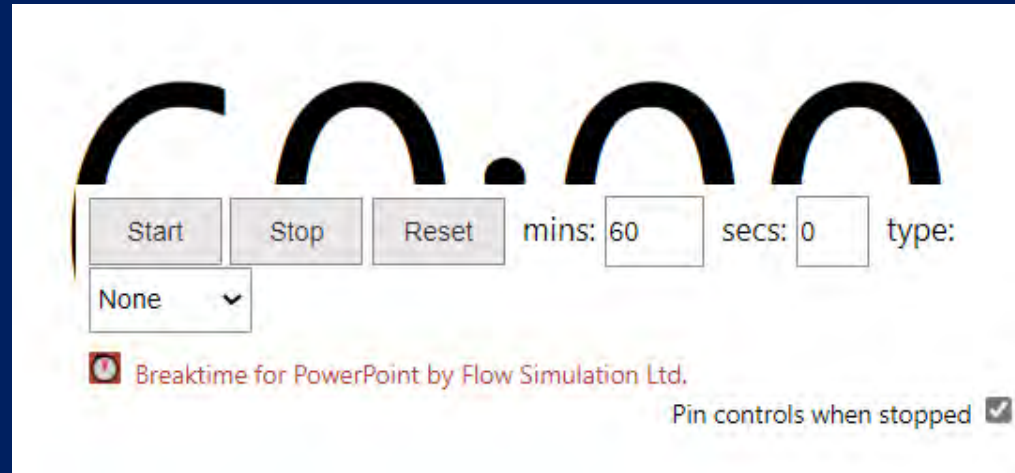
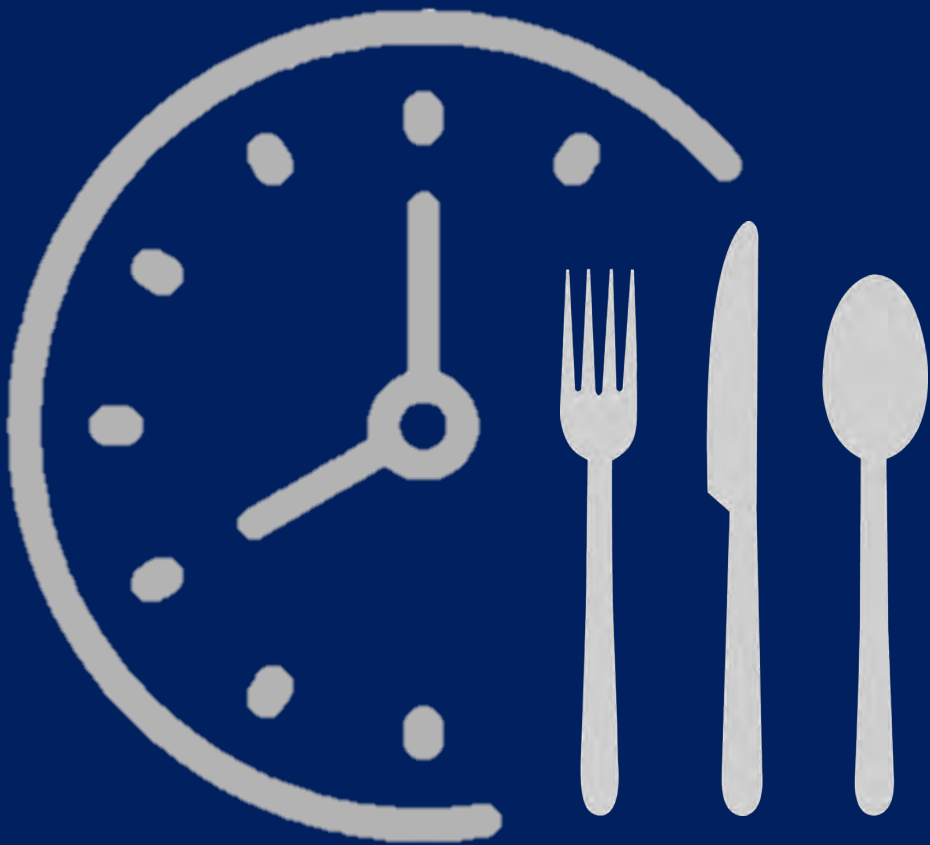


A financial institution experiences a data breach where cybercriminals gain unauthorised access to customer records, including names, addresses and social security numbers. The institution immediately takes action to mitigate the breach and strengthen its security measures.

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



Undergraduate Diploma



Undergraduate Diploma

Data Breach 1



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

15:00



Data Breach 2



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 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 .

15:00

Investigate and report

Suggest mitigation measures for non-repeat of the data breach



15:00



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?



1 0.00

Start Stop Reset mins: 10 secs: 0 type:

None ▾

 Breaktime for PowerPoint by Flow Simulation Ltd.

Pin controls when stopped

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 organization 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 unauthorized 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 minimization, 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: 27 April 2024

Undergraduate Diploma