Managing Data and its Implications

Lecture Title: Implications on Business

21 ACADEMY

Undergraduate Diploma

Lecturer: Angelito Sciberras
Date: 20 April 2024

Last Lecture

- Introduction to GDPR
- Data Breaches & Identity Theft
- GDPR Fines
- Data, Personal Data & Special Category of Data
- Definitions
- Data Protection Officer
- 6 Principles of GDPR and Accountability
- Lawfulness of processing
- Data Subject Rights
- Subject Access Requests

Which of the following is a principle of GDPR?

A) Data Encryption

B) Secure Socket Layer (SSL)

C) Purpose Limitation

D) Firewall Protection

E) Two-Factor Authentication

Which of the following is a principle of GDPR?

A) Data Breach Notification

B) Right to Erasure

C) Data Minimisation

D) Accuracy

E) Consent

Which of the following is a principle of GDPR?

A) Right to Access

B) Lawfulness, Fairness, and Transparency

C) Storage Limitation

D) Integrity and Confidentiality

E) Profiling

Which of the following is a principle of GDPR?

A) Purpose Limitation

B) Individual Rights

C) Consent

D) Accountability

E) Data Minimisation

Which of the following is a principle of GDPR?

A) Storage Limitation

B) Right to Rectification

C) Data Portability

D) Lawfulness, Fairness, and Transparency

E) Two-Factor Authentication

Which of the following is a principle of GDPR?

A) Data Breach Notification

B) Purpose Limitation

C) Accountability

D) Data Encryption

E) Right to Erasure

Which of the following is a principle of GDPR?

A) Accuracy

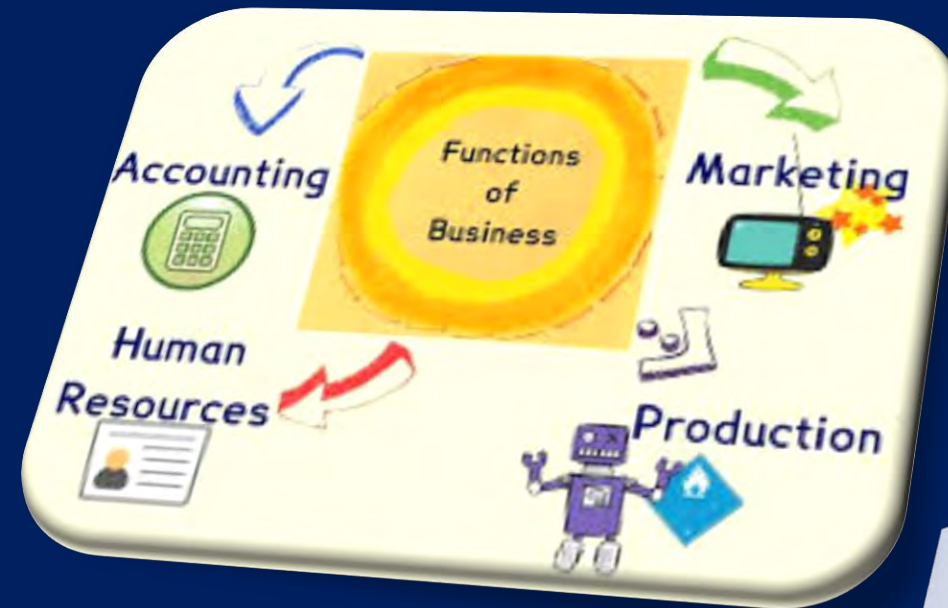B) Data Minimisation

C) Purpose Limitation

D) Lawfulness, Fairness, and Transparency

E) Profiling

Most effected departments in a company?

- IT

- Human Resources

- Marketing (Sales)

- Finance

Undergraduate Diploma

Checklist

Ensure all employees are aware of GDPR regulations and their responsibilities

Awareness

15:00

How can you create GDPR awareness within an organisation?

Creating Awareness

- Conduct GDPR training
- Communicate GDPR policies
- Create GDPR champions
- Display GDPR posters
- Encourage reporting of GDPR incidents
- Conduct GDPR audits
- Provide GDPR resources

Undergraduate Diploma

Checklist

Review and update privacy notices and policies

Policies and Procedures

15:00

What GDPR Policies and Procedures should a company have in place?

Policies and Procedures

- Privacy Standard (Data Protection Policy)
- Privacy Notices
  - Shareholders
  - Employees
  - Clients
  - Website
  - Directors
  - Job Applicants
  - Suppliers

Policies and Procedures

- Data Retention Guidelines
  - HRM
  - Business related
- Data Breach
  - Policy
  - Procedure
- Subject Access Requests
  - Policy
  - Procedure

Policies and Procedures

- CCTV Policy/Notice/Signage
- Data Protection Impact Assessment
- Image Consent Forms
- IT Systems Policies
  - IT and Communications System Policy
  - Disposal of IT Equipment Policy
  - Email Usage Policy
  - Bring Your Own Device Policy

Privacy Standard

- A privacy standard is an 'inward-looking' document, recently replacing what was previously known as a "privacy policy".

- Today, this has become an essential document which regulates an organisation's handling of personal data (whether obtaining, controlling, processing, transport, or storage) and also informs employees of their duties under data protection legislation.

Privacy Standard

- written in simple language and presented in an accessible form

- comprehensive

- easily accessible

Privacy Standard

- Having these duties set out in writing does not exempt the employer from being bound to educate & train employees on good data practices in order to comply with the law.

Notice to Data Subjects

- Shareholders

- Employees

- Clients

- Website

- Directors

- Job Applicants

- Suppliers

Notice to Data Subjects

- Who is processing the data

- What legal basis allow you to collect user data

- What are the purposes of collecting the personal data

- What types of personal data you collect

Notice to Data Subjects

- How long you're going to store the data

- The contact details of the data protection officer, where applicable;

- The right to lodge a complaint with a supervisory authority;

- Whether you transfer the data internationally

Notice to Data Subjects

- Whether you use the data in automated decision-making

- With what third parties you share the data

- What are the data subject rights

- How you'll inform users that your policy has changed

Secure IT Policy

- Equipment Security and Passwords
- Systems and Data Security
- Email
- Using the Internet
- Personal Use of Systems
- Monitoring
- Prohibitive use of systems
- Disposal of IT equipment

Undergraduate Diploma

15:00

www.21Academy.education

21
ACADEMY

Undergraduate Diploma

Email Use Policy

- Prevents Phishing

- Abide with privacy legislation

- Personal Data

Email Use Policy

- Standards users must follow when using the Work Email

- Ensuring availability by protecting it from unauthorised or accidental modification

- Preserving confidentiality and protect against unauthorised disclosure

- Making the Users aware of what is acceptable and unacceptable use of the Work Email.

Emails

15:00

Identify bad practices in email use that may lead to a data breach?

Email Use – bad practices

• Sending email to the wrong recipient

• Sending email to multiple recepients with all in copy

• Sending attachments which are not password protected

• Using work email for personal use

• Sharing of email login credentials

• Not monitoring of incoming emails

• Auto forwarding emails to another account

• No backup

Can you give examples of employees' monitoring?

05:00

Monitoring of Employees

- Computer and Internet Monitoring
- Video Surveillance
- Telephone Monitoring
- GPS Tracking
- Email Monitoring
- Time and Attendance Monitoring
- Performance and Productivity Monitoring
- Keystroke Logging
- Social Media Monitoring
- Data Movement
- Mystery Shopping

Monitoring of Employees

"Employers have legitimate interests in monitoring in order to improve efficiency and protect company assets. However, workplace monitoring becomes intrusive and unjustifiable if it is not limited or transparent."

- Working Party 29

Monitoring of Data Subjects

- Data Subjects must be informed:

- of the existence of monitoring;

- about the purposes for which their data is processed; and

- of any other information necessary to guarantee fair processing.

Monitoring of Data Subjects

This sign is affixed in an office. It is informing employees & visitors that monitoring is being carried out

Is this enough? Why?

Monitoring of Data Subjects

Monitoring of Data Subjects

05:00

CCTV IN OPERATION

IMAGES ARE BEING MONITORED AND MAY BE RECORDED FOR THE PURPOSE OF CRIME PREVENTION AND PUBLIC SAFETY

This scheme is operated by:

YOUR COMPANY NAME HERE

For further information contact
The Data Controller

TEL: YOUR NUMBER HERE

What is missing in this notice from an HR perspective?

Undergraduate Diploma

Checklist

Ensure all data processing activities have a lawful basis

Ensure all data processing activities have a lawful basis

How?

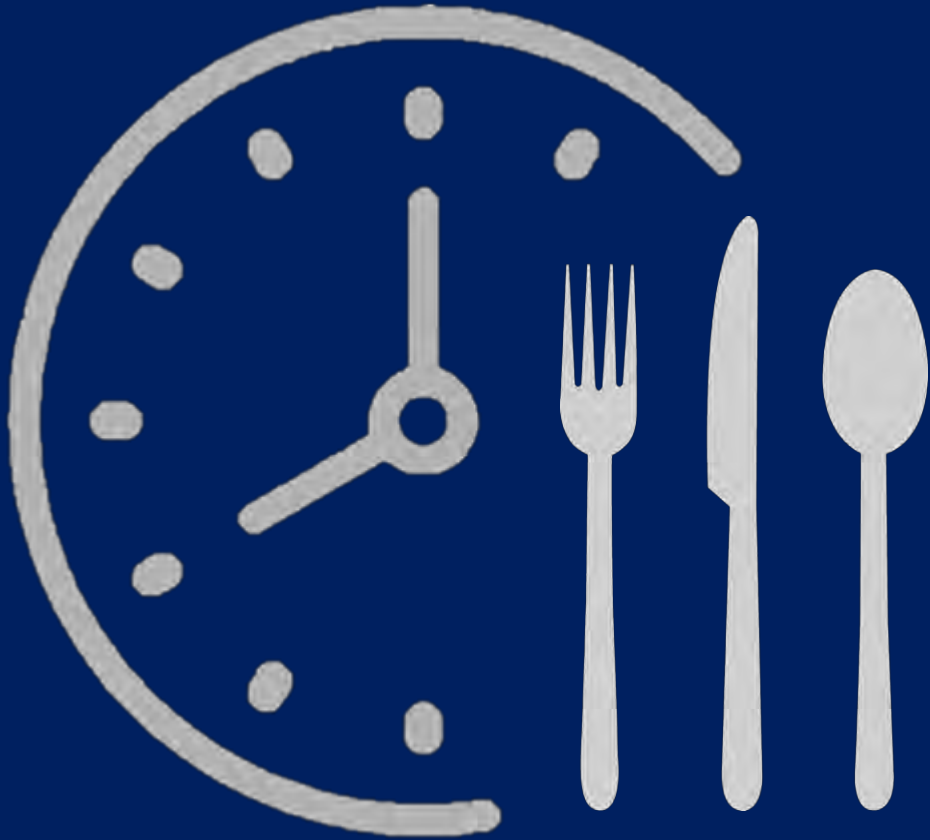05:00

Undergraduate Diploma

Checklist

Implement measures to ensure data accuracy and minimise data collection

Undergraduate Diploma in
Business Administration

60:00

21
ACADEMY

Undergraduate Diploma

Checklist

Review and update data processing agreements with third-party service providers

Data Processing Agreement

- Subject matter and duration
  - the nature,
    - types of personal data
    - categories of data subjects
  - scope, and
  - purpose of the processing activities, and
  - the duration of the processing

Data Processing Agreement

- Obligations of the data processor: including
  - measures taken to ensure data security,
  - confidentiality, and
  - compliance with GDPR

- Subcontracting
  - obtain the data controller's prior written consent and
  - impose the same obligations on any subcontractor

Data Processing Agreement

- Obligations of the data controller
  - contact points
  - transfer methods
  - within when to give written authorisarions
  - pre-notifications

Data Processing Agreement

- Data subject rights:
  - how data subjects can exercise their rights
    - right to access,
    - rectify,
    - erase,
    - restrict processing,
    - object, and
    - data portability

Data Processing Agreement

- Data breaches:
  - data processor's obligations in the event of a data breach
    - notifying the data controller
    - the supervisory authority
    - assisting with investigations
    - remedial actions.

Data Processing Agreement

- International transfers:
  - the safeguards implemented to ensure an adequate level of protection for personal data.

- Audit and compliance:
  - allow the data controller to conduct audits or inspections to ensure compliance with GDPR regulations.

Data Processing Agreement

- Termination:
  - specify the circumstances under which the agreement can be terminated, and
  - the consequences of termination.

- Governing law and jurisdiction.

Undergraduate Diploma

Checklist

Implement appropriate technical and organisational measures to ensure data security

Technical vs Organisational measures

Technical vs Organisational measures

Technical Measures

- Facility protection
- Firewalls
- VM Security
- Sys Admin
- and many more

- Data Encryption
  (at record-application level)
- Auth & Access Control
- Consent Tracking
- Immutable audit logs
- and many more

Organisational Measures

- Privacy Policies
- Terms & Conditions
- DPA
- DPIA & Risk Assess.
- and many more

Undergraduate Diploma

Checklist

Appoint a Data Protection Officer (DPO) if required by the GDPR

Appoint a Data Protection Officer

- Assess whether it is obligatory to have a DPO
  - What are the reasons you appoint a DPO?

- Check what member state law says
  - In Malta DPO has to be registered with the IDPC
  - Data Controller, Name of DPO, Mailing Address, Email Address, Contact Number, Nature of Business, and Date of Appointment.

Appoint a Data Protection Officer

- Always appoint someone responsible for data privacy

Undergraduate Diploma

Checklist

Establish procedures to respond to data subject requests and complaints

Lecture 4

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

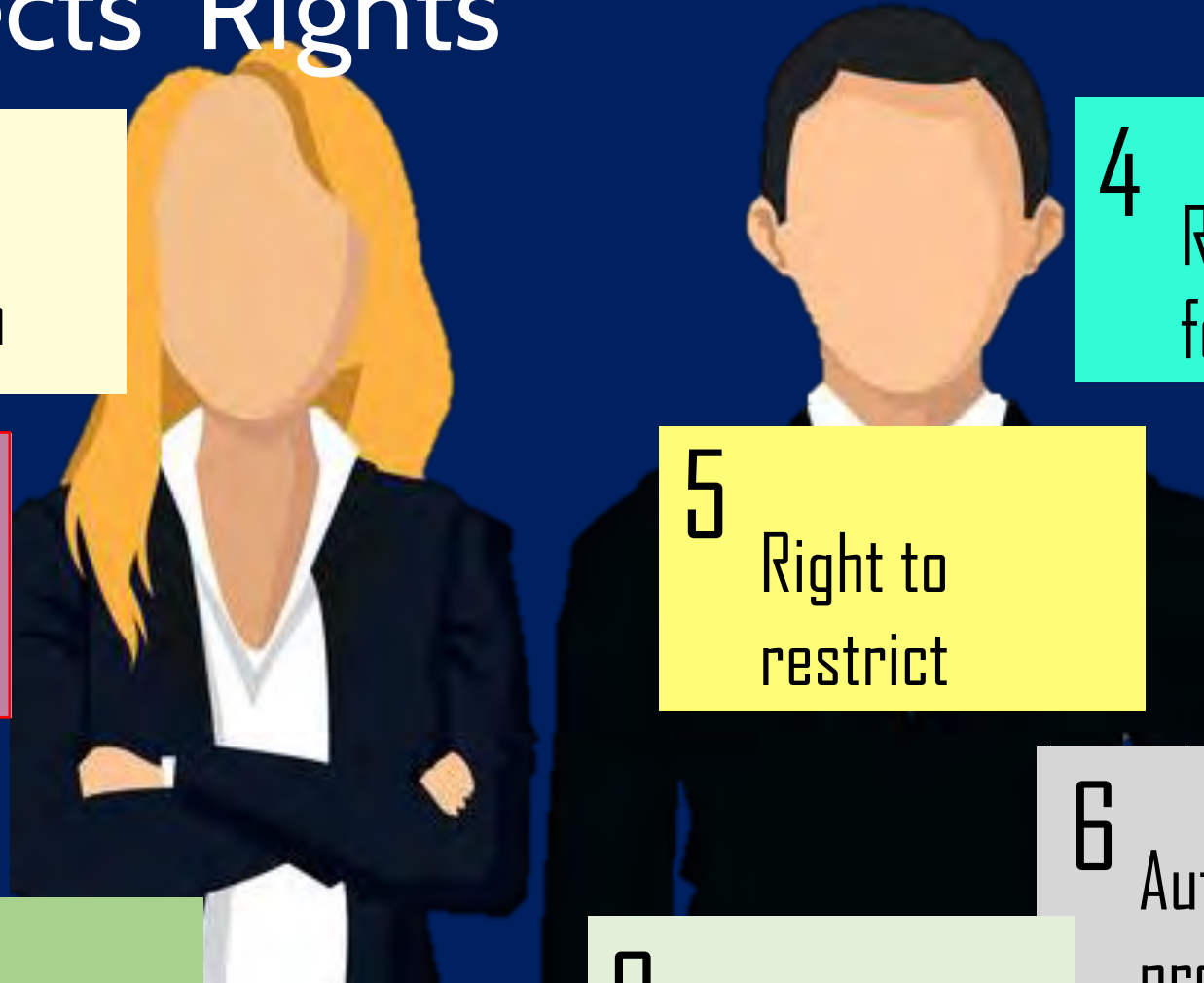2 Right of access

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.

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

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).
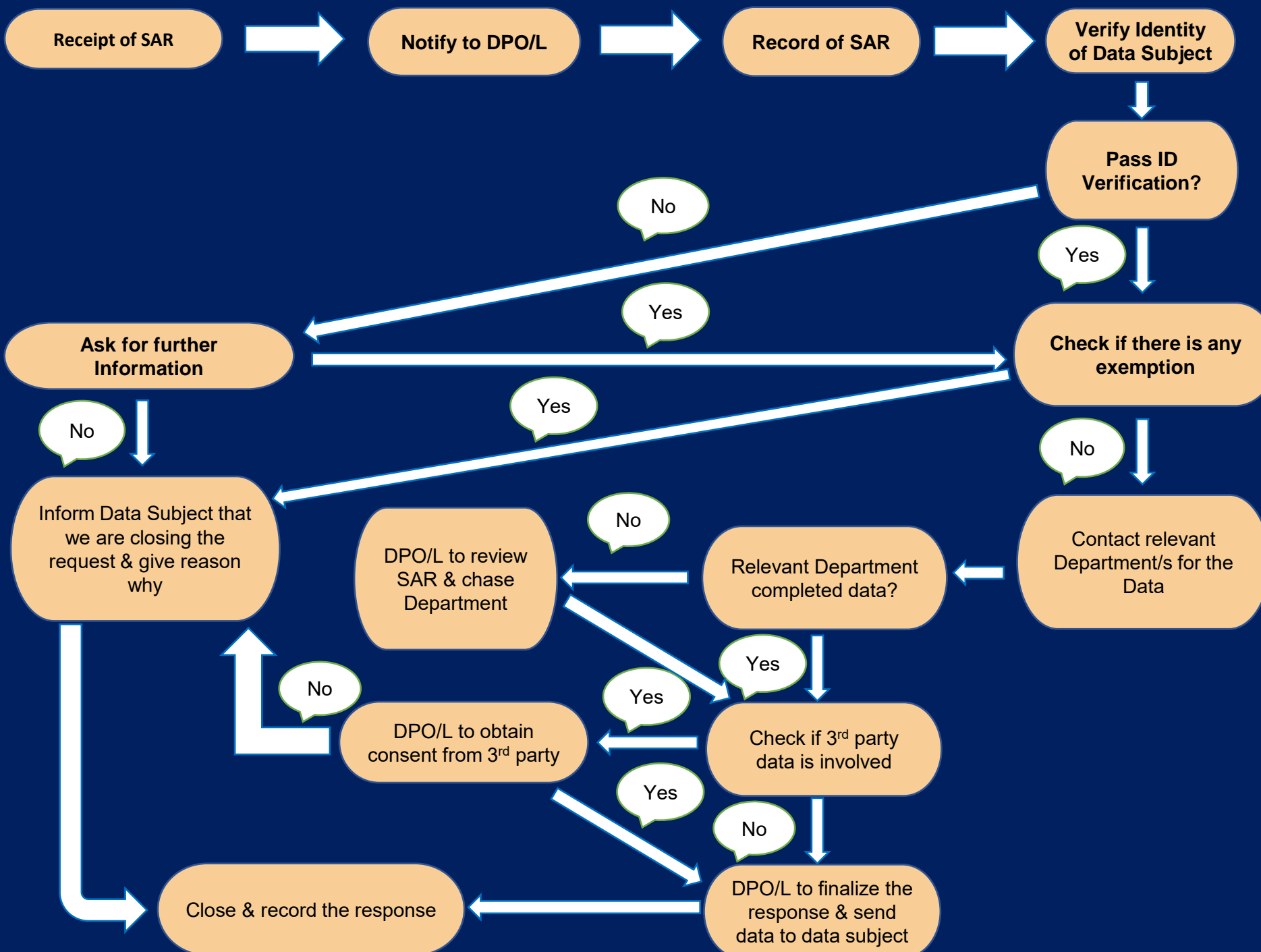
Receiving a SAR

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

Undergraduate Diploma

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

Checklist

Conduct regular data protection impact assessments (DPIAs) for high-risk processing activities

Lecture 7

Checklist

Establish procedures to report data breaches to the supervisory authority and affected individuals

Lecture 7

Checklist

Conduct regular GDPR compliance audits and reviews

Undergraduate Diploma

IT Department

10:00

Technical & Organisational Measures?

How can the IT department help with GDPR compliance?

Privacy By Design – Data Protection Impact Assessment (DPIA)

- Must be prior to processing;
- Must be continual (not a one time process);
- Processors should assist controllers;
- Recommended to seek independent expert advice.

ISO/IEC 29134:2017 : Information technology - Security techniques - Guidelines for privacy impact assessment

How can the IT department help with GDPR compliance?

Privacy By Default

The controller shall implement **mechanism**s for ensuring that, by **default**, only those personal data are processed which are necessary for each specific purpose of the processing,

(& not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage).

How can the IT department help with GDPR compliance?

Privacy By Default - Example

A social media platform should be encouraged to set users' **profile settings in the most privacy-friendly setting** by, for example, limiting from the start the accessibility of the users' profile so that it isn't accessible by default to an indefinite number of persons.

How can the IT department help with GDPR compliance?

GDPR, Article 5(1)f - the 6th Principle

"Personal Data shall be processed in a manner that ensures appropriate **security** of the personal data, including **protection against unauthorised or unlawful processing and against accidental loss, destruction or damage**, using appropriate technical or organisational measures"

How can the IT department help with GDPR compliance?

Security measures put in place should seek to ensure :

- the data can be **accessed, altered, disclosed or deleted** only by those you have **authorised** to do so (and that those people only act within the scope of the authority you give them);

- the data you hold is **accurate and complete** in relation to why you are processing it; and

How can the IT department help with GDPR compliance?

Security measures put in place should seek to ensure :

- the data remains accessible and usable, i.e. if personal data is accidentally **lost, altered or destroyed**, you **should be able to recover** it and therefore prevent any damage or distress to the individuals concerned

Physical vs Cyber Security

PHYSICAL SECURITY

CYBER SECURITY

- the quality of doors and locks, and the **protection of premises** by such means as alarms, security lighting or CCTV;

- **access control** to premises, and how **visitors** are supervised;

- Paper, waste and electronic **disposal**; and

- Security of **IT equipment,** particularly mobile devices

- **System/network security** – the security of network and information systems, including those which process personal data;

- **data security** – the security of the data held on systems, eg ensuring appropriate access controls are in place and that data is held securely;

- **online security** – eg the security of a website and any other online service or applications used; and

- **device security** – including policies on Bring-your-own-Device (BYOD).

Security

Use Firewalls to secure your internet connection

- This effectively creates a 'buffer zone' between your IT network and other, external networks.

- Incoming traffic can be analysed to find out whether or not it should be allowed onto your network.

Security

Choose the most secure settings for your devices and software

- Manufacturers often set the **default configurations** of new software and devices to be as open and multi-functional as possible. They come with 'everything on' to make them easily connectable and usable

- Check Settings. Change Passwords.

- For important accounts, use 2-factor authentication (2FA)

Security

Control who has access to your data and services

- Set admin accounts;

- Check privileges;

- Standard accounts should be used for general work. By ensuring that your staff don't browse the web or check emails from an account with administrative privileges you cut down on the chance that an admin account will be compromised

- only use software from official sources

Security

Protect yourself from viruses and
 other malware

- Anti-malware measures;

- Whitelisting;

- Sandboxing (isolates applications);

Security

Keep your devices and software
up to date

- Operating systems, programmes, phones and apps should all be set to 'automatically update' wherever this is an option;

- Replace unsupported hardware or software;

Security

Penetration Testing

- Obligation to carry out **'stress tests'** (vulnerability scanning and penetration testing) of networks and information systems, which are designed to reveal areas of potential risk and things that you can improve.

- ICO : The GDPR now makes this an obligation for all organisations.

Security

E-Mail Security

- Consider whether the content of the email should be encrypted or password protected.

- Make sure you choose the right address before you click send.

- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc).

- If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.

15:00

www.21Academy.education

21
ACADEMY

Undergraduate Diploma
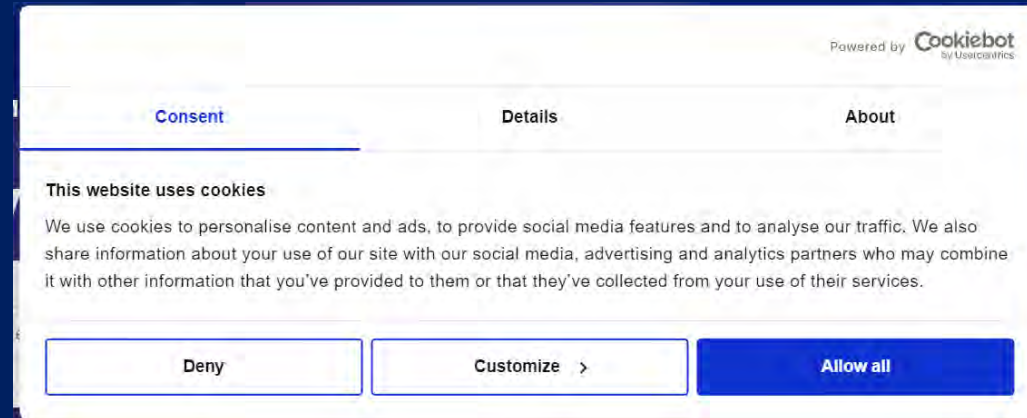
GDPR & Privacy Laws

Is your website GDPR Compliant?

Website Compliance

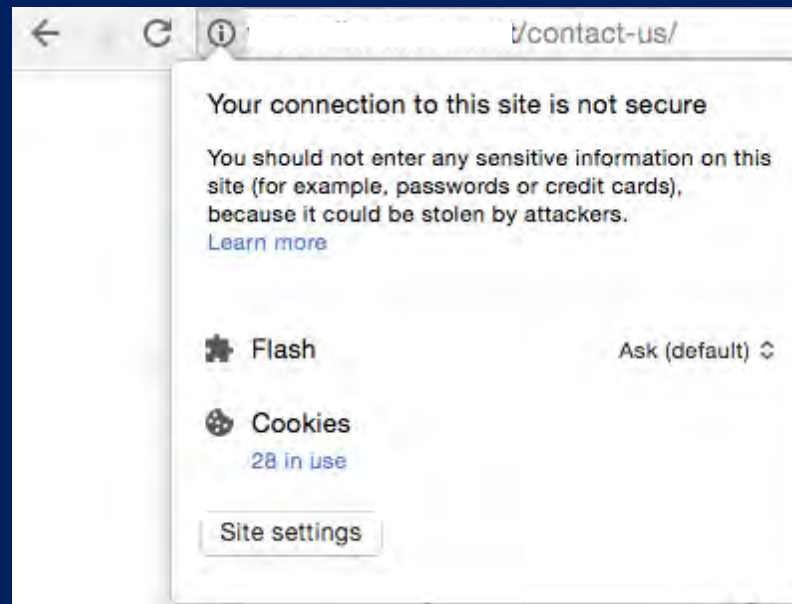## Cookie Notification
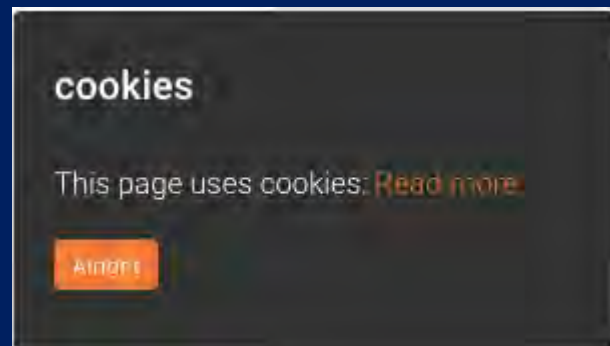
Website Compliance

Policies & Notices

Cookie Policy which is also accessible from your privacy notice and also link it to the policies of the third party cookie providers
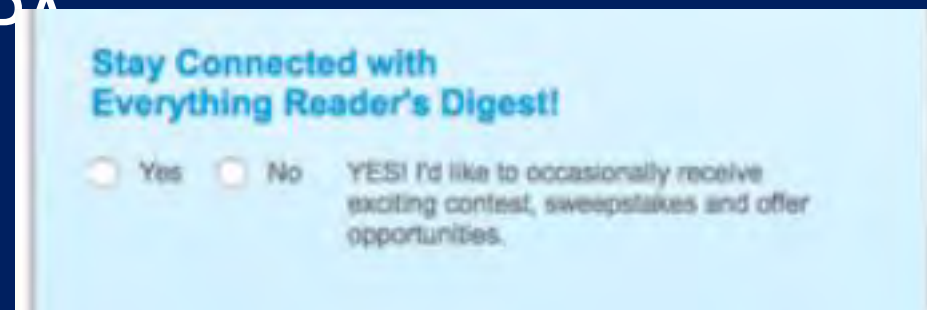
Privacy Notice

Website Compliance

Secure Socket Layer (SSL)

Website Compliance

Data Capturing Tools

- Consent

- Links to notice/s

- Do not store data which you don't need

- Service providers (mailing list etc) should also be GDPR compliant & DPPA

- No pre ticked boxes

- Not bundled

Stay Connected with Everything Reader's Digest!

Yes   No   YES! I'd like to occasionally receive exciting contest, sweepstakes and offer opportunities.

Website Compliance

Consent from all of those who show on photographs, videos and testimonials

including employees

Website Compliance

Payment Gateways

Make sure that they are GDPR compliant

Link Privacy Notice

Website Compliance

Web Chat

Is the chat stored?

Is data captured from the chat?

Is chat provider GDPR compliant?

Does your notice link to theirs?

Do you have a DPPA in place?

Undergraduate Diploma