Introduction to Business Law

Lecture Title: Data Protection - the Salient Features

Lecturer: Mr Angelito Sciberras

Date: 21 November 2023

Today's Session

- Personal Data
- Power of Data
- GDPR
  - Definitions
  - Principles, Rights, Lawful Basis for Processing
- Data Breaches, SARs & DPIAs
- Company Data
  - IT
  - HR
  - Marketing

Data vs Personal Data

60sec

Data vs Personal Data

facts and statistics collected together for reference or analysis

vs

any information relating to an identified or identifiable individual

Data Privacy vs Data Protection

60sec

Data Privacy vs Data Protection

Data Privacy defines who has authorised access

Data Protection is focused on protecting assets from unauthorised use.

21 ACADEMY

The Power and Value of Personal Data

"The world's most valuable resource is no longer oil, but data"

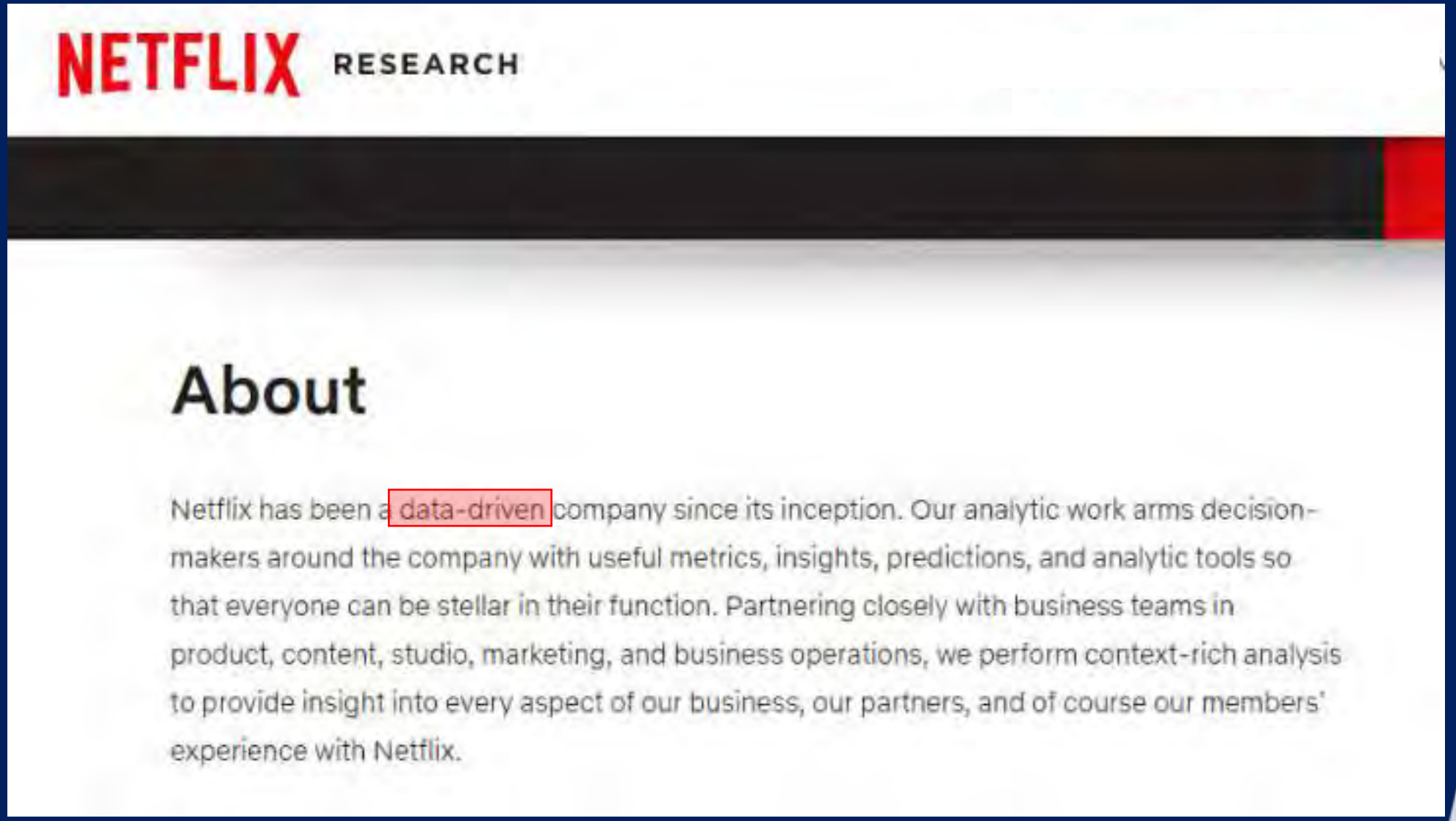
- The Economist, May 2017

Personal Data

How would you describe Netflix?

60sec

Data



NETFLIX RESEARCH

About

Netflix has been a data-driven company since its inception. Our analytic work arms decision-makers around the company with useful metrics, insights, predictions, and analytic tools so that everyone can be stellar in their function. Partnering closely with business teams in product, content, studio, marketing, and business operations, we perform context-rich analysis to provide insight into every aspect of our business, our partners, and of course our members' experience with Netflix.

Personal Data

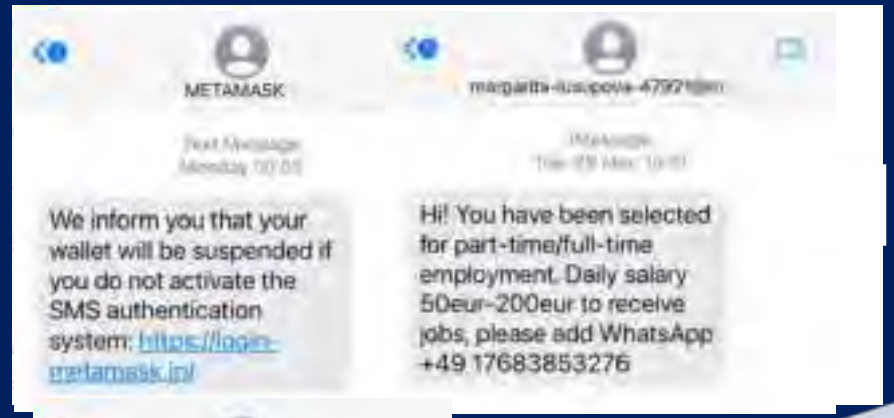
Value of Personal Data

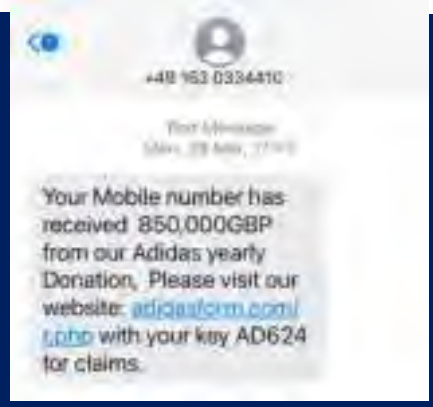
What value does company data have?

- Email addresses
- Mobile numbers

Do you keep copies of ID cards?

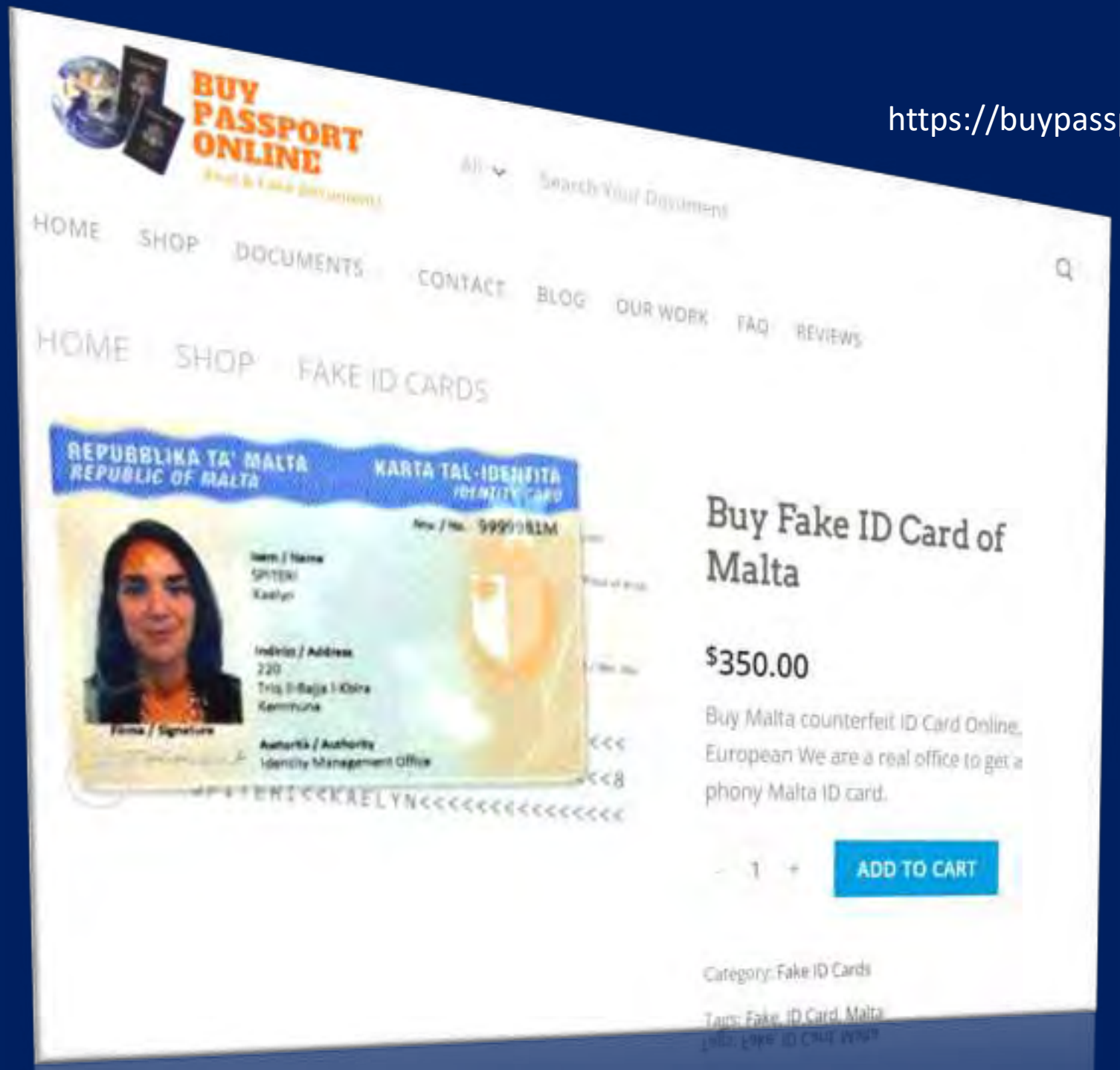
For what purpose?



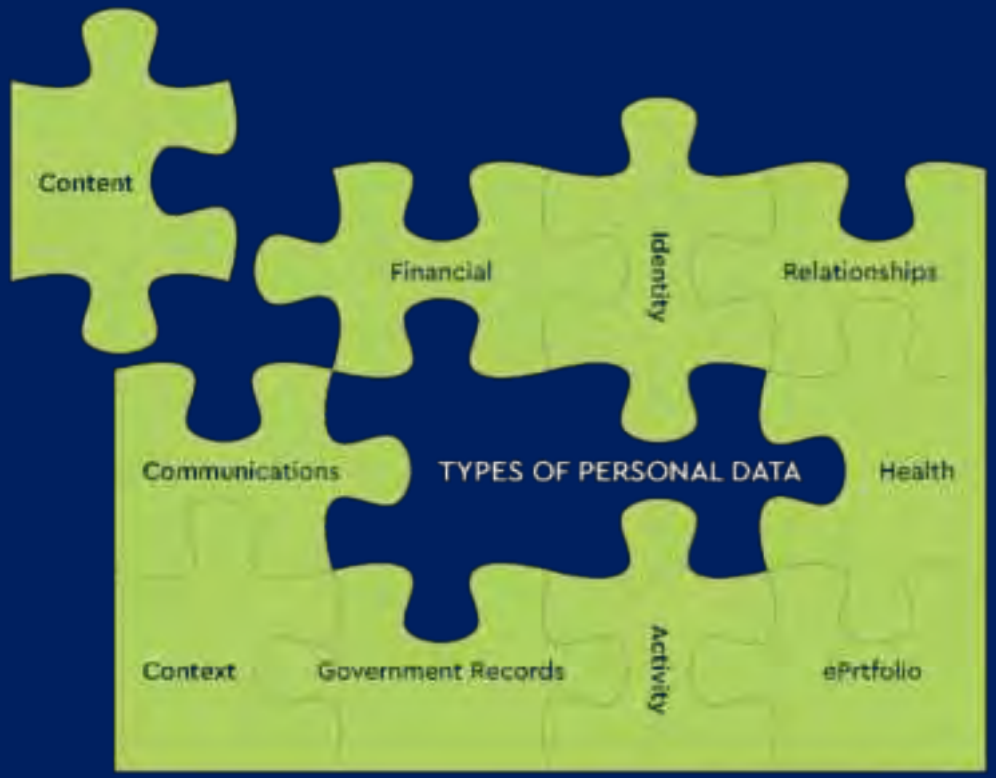


Award in Introduction to Business Law

https://buypassportsonline.com/shop/buy-fake-id-card-of-malta



Why do fraudsters want access to your company's personal data?



Award in Introduction to Business Law

Why GDPR?

Personal Data misuse

21 ACADEMY

The need for new legislation

Legislation

Directive 95/46/EC

GDPR

What changed on a Company Level?

Directive 95/46/EC

Macintosh Performa 6200

IBM Personal Communicator

Kodak DCS 460 Camera

Iomega Zip Drive

Motorola Tango Pager

IBM ThinkPad 701C

DVDs

Sony Handycam DCR-VX1000

Legislation

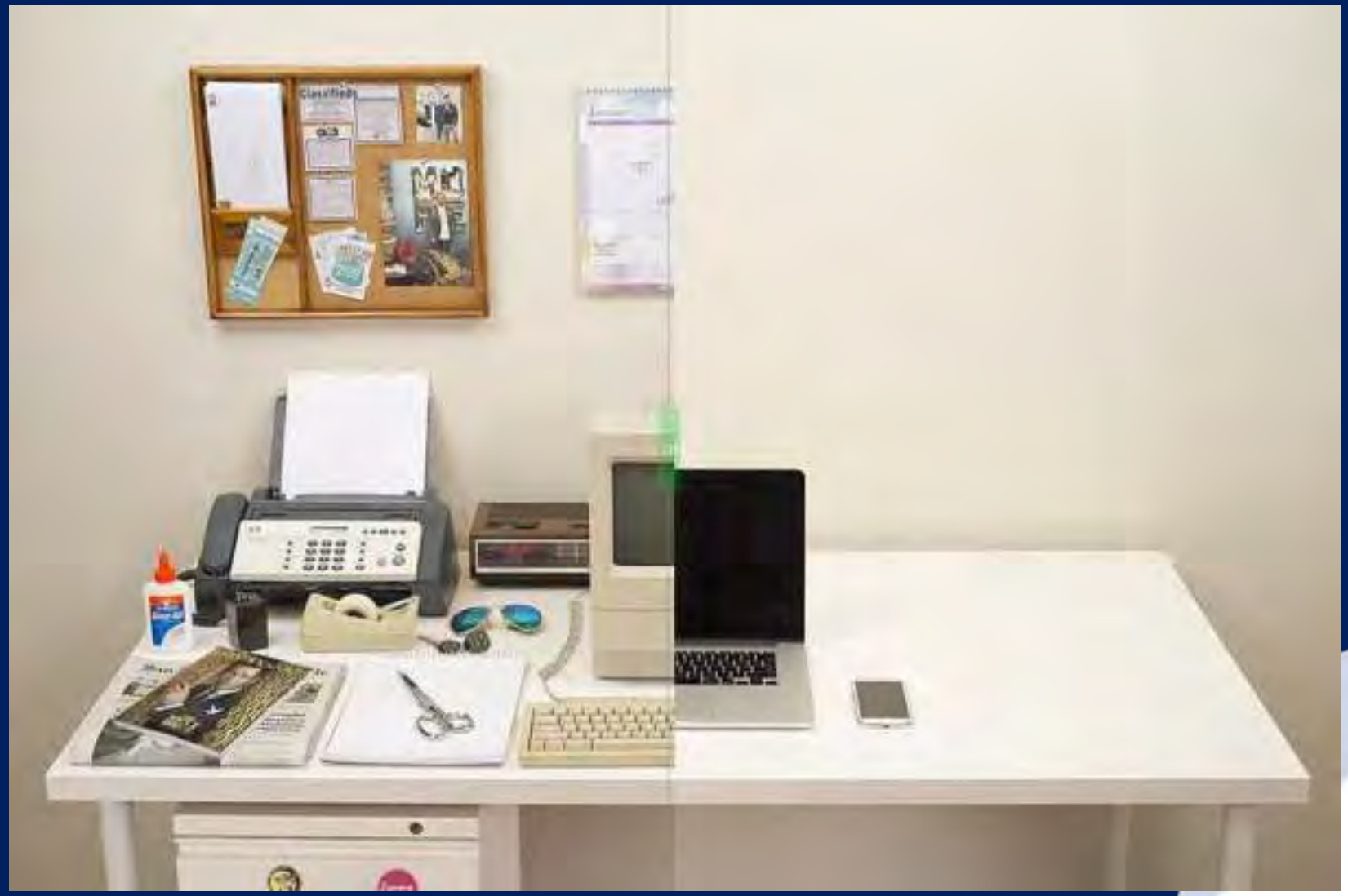
Directive 95/46/EC

GDPR

What changed on a Company Level?

Company Tools Evolution

Company Tools Evolution



Company Tools Evolution

21 ACADEMY

GDPR

"What must be recognised is that GDPR is an evolution in data protection, not a total revolution... GDPR is building on foundations already in place for the last 20 years."

- Steve Wood - Deputy Commissioner for Policy, ICO

25 August 2017

Award in Introduction to Business Law

Problems solved?

www.21Academy.education

Fines

€746 million

- Luxembourg National Commission for Data Protection (CNDP)
- how Amazon processes personal data of its customers
- complaint filed by 10,000 people in 2018
- infringements regarding Amazon's advertising targeting system that was carried out without proper consent

Fines - Malta

What was the highest fine under GDPR in Malta so far?

60sec

Fines - Malta

€250,000

- 2022
- Information and Data Protection Commissioner
- Controller infringed principles of security regarding personal data of data subjects and failed to implement appropriate technical and organisational measures
- Infringements of Articles 32(1) and 32(2) of the GDPR

21 ACADEMY

Definitions

Processing

Means *any* operation or set of operations which is performed on personal data or on sets of personal data,

- *whether or not by automated means*,
- *such as* collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal Data

- ***any information*** relating to an identified or identifiable natural person **('DATA SUBJECT');**
- an identifiable natural person is one who can be identified, directly or indirectly, ***in particular*** by reference to an identifier ***such as*** a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Special Categories of Data

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

Special Categories of Data

[B] Criminal Convictions & Offences

Exercise

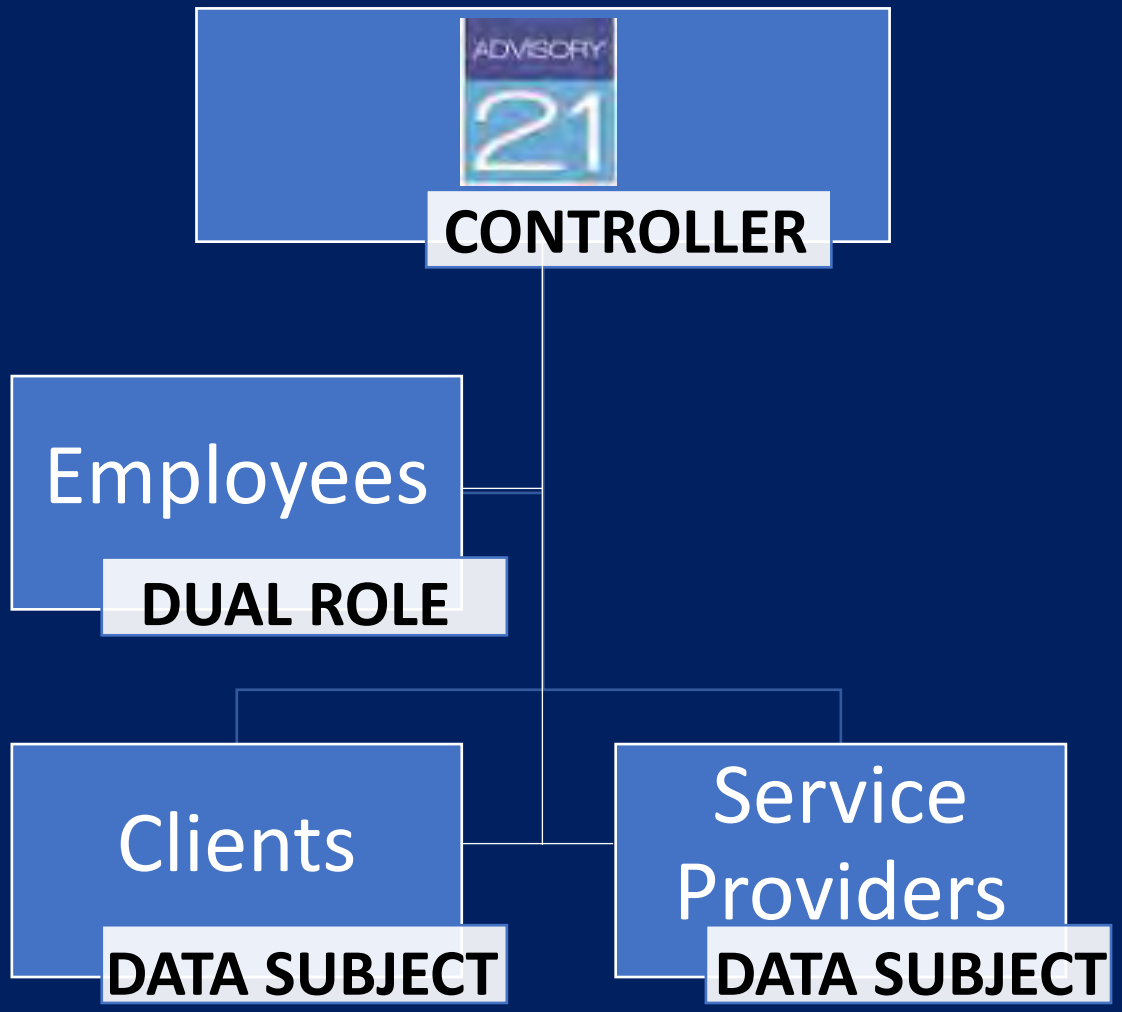
Identify (a) personal data, (b) sensitive data and (c) out of scope

- Mr J. Borg
- High blood pressure
- 21 Academy
- info@21academy.education
- Police conduct certificate
- +356 2099 5486

Controller

‘Controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

Controller


CONTROLLER
Employees
DUAL ROLE
Clients
DATA SUBJECT
Service Providers
DATA SUBJECT

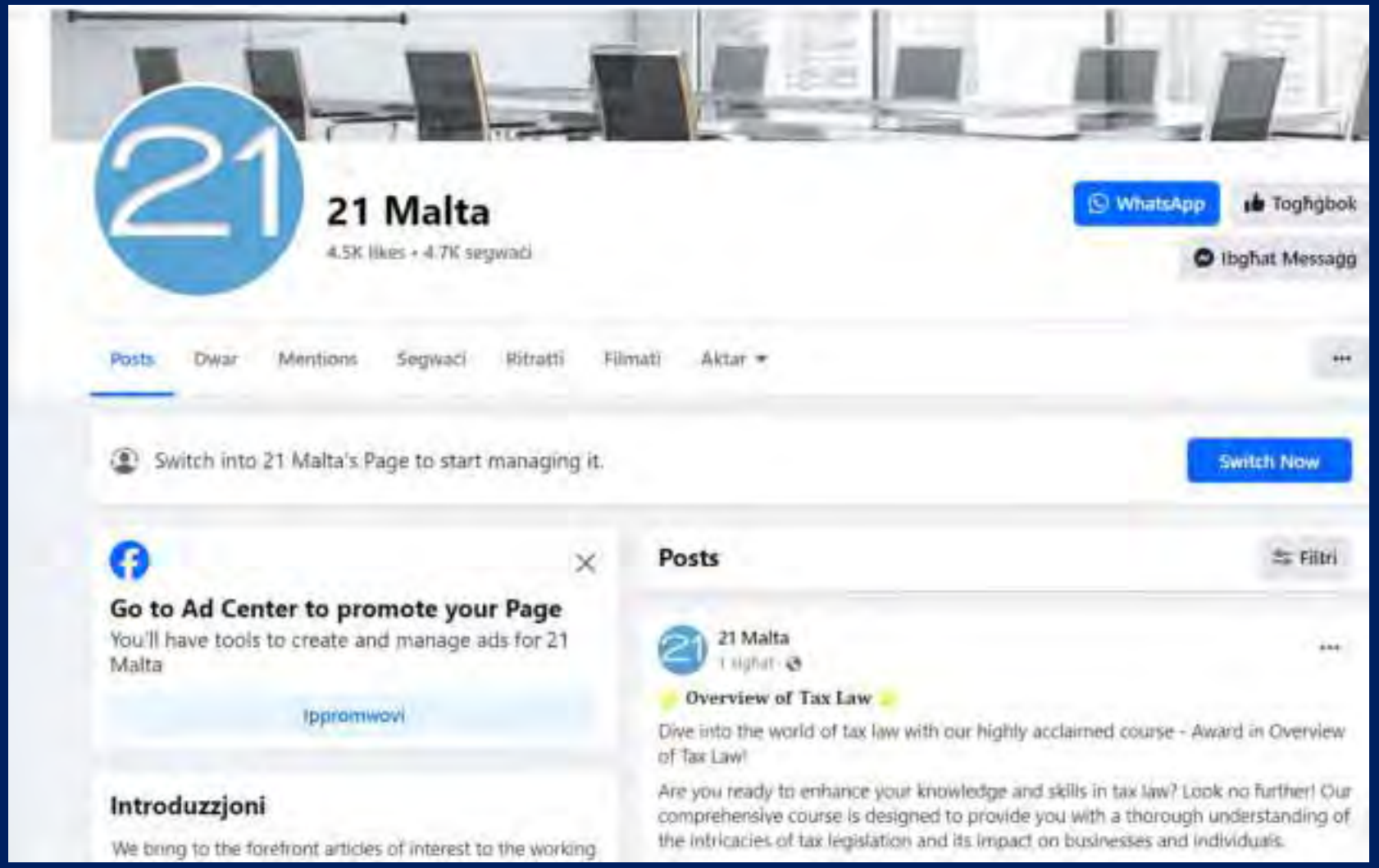
Joint Controllers

Where two or more controllers jointly determine the purposes and means of processing

Reflect the respective roles and relationships vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

The data subject may exercise his or her rights in respect of and against each of the controllers.

Joint Controllers



Processor

‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Controller & Processor

Controller

Processors

Controller & Processor

Employee
(DATA SUBJECT)

Advisory 21 Ltd
(CONTROLLER)

External Payroll Service Provider
(PROCESSOR)

Dakar
(SUB-PROCESSOR)

Principles Legal Grounds and Rights

Principles

1	lawful, fair and transparent
2	specific, explicit and legitimate purpose
3	adequate, relevant and limited to what is necessary
4	accurate & up to date
5	storage limitation
6	integrity and confidentiality

Legal Grounds

Processing is lawful if based on one of the following legal basis

1 Right to information

2 Right of access

3 Right to rectify

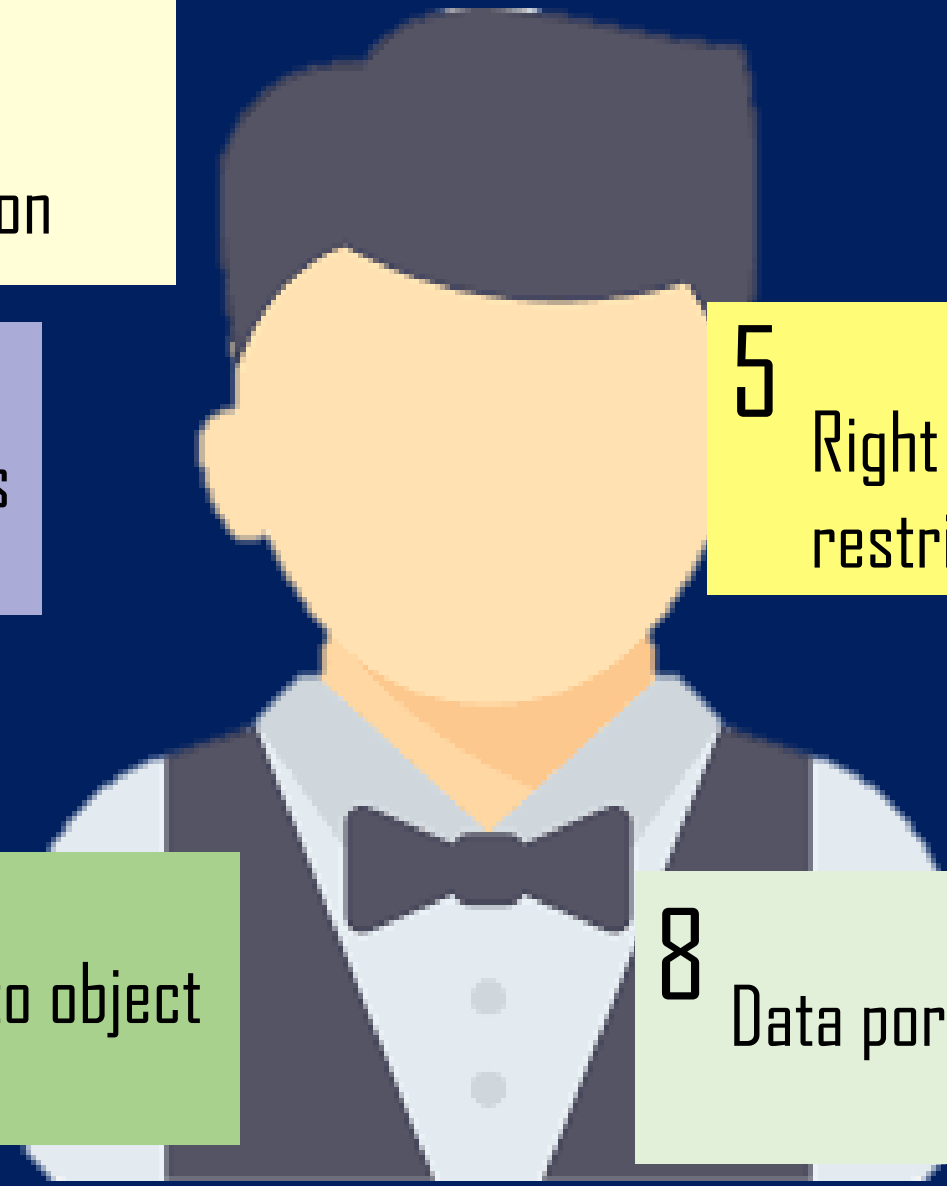
4 Right to be forgotten

5 Right to restrict

6 Automated processing

7 Right to object

8 Data portability

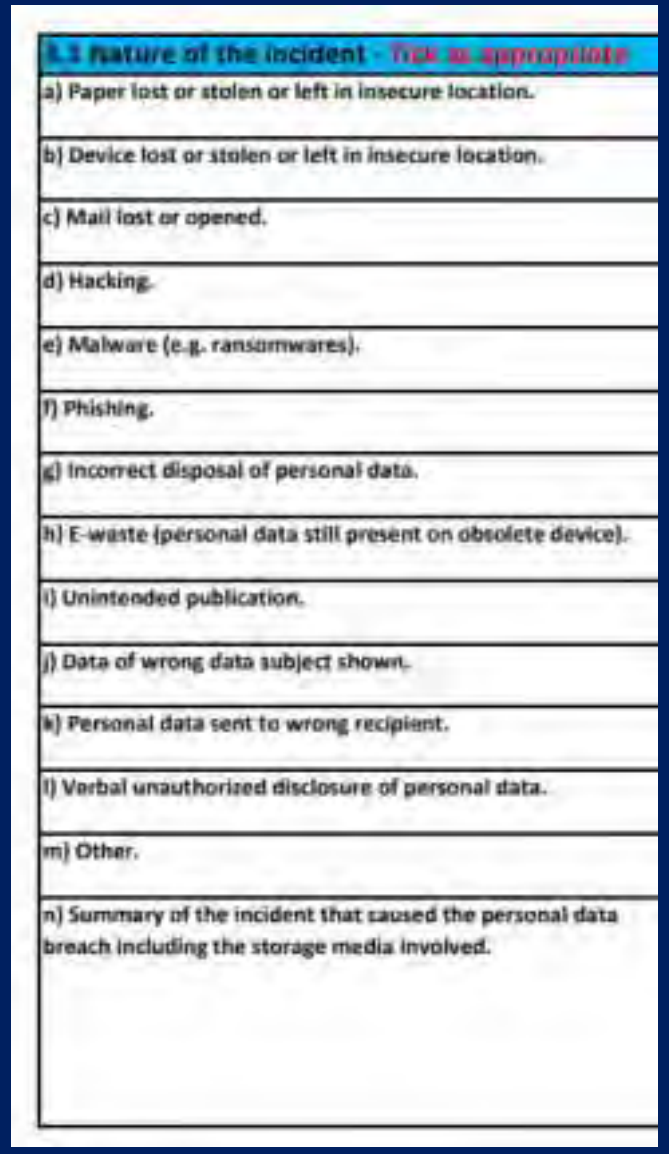


21 ACADEMY

21
ACADEMY

Data Breaches, SARs and DPIAs

Data Breach



3.1 Nature of the incident - Tick as appropriate
a) Paper lost or stolen or left in insecure location.
b) Device lost or stolen or left in insecure location.
c) Mail lost or opened.
d) Hacking.
e) Malware (e.g. ransomwares).
f) Phishing.
g) Incorrect disposal of personal data.
h) E-waste (personal data still present on obsolete device).
i) Unintended publication.
j) Data of wrong data subject shown.
k) Personal data sent to wrong recipient.
l) Verbal unauthorized disclosure of personal data.
m) Other.
n) Summary of the incident that caused the personal data breach including the storage media involved.

A breach is not hacking only

- Sending personal data to the wrong recipient
- Sending emails to multiple recepients who are not in BCC
- Losing employee data
- Others

Data Breach

- Policy
- Procedure
- Assessment

Data Breach

Assessment

- Step one: Check if personal data is involved.
- Step two: Establish what personal data has been breached.
- Step three: Consider who might have the personal data.
- Step four: Work out how many people might be affected.
- Step five: Consider how seriously it will affect people.
- Step six: Document everything else you know about the breach
- Step seven: Assess the risk

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.

The Right to SAR

GDPR - 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

If personal data is being processed, the data subject 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**;
- information on the **source** of the data;

Summary of rights

- information regarding complaints and disputes;
- transfer of data outside the EEA (if any);
- the recipients or categories of recipients to whom data has been or will be **disclosed**;
- the period during which personal data will be **retained**;
- information on the **source** of the data;

Summary of rights

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

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

Receiving a SAR

A SAR may be made:

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

Controller should provide means for requests to be made electronically

Set out a preferred method of contact

Ideal Scenario

Policy on handling a SAR

Response procedure

Form (one for each subject right)

Tracking form

Letters

Logbook

Data Protection Impact Assessment

- A process to help you identify and minimise the data protection risks of a project

- Must be done for processing that is likely to result in a high risk to individuals

- Must:
  - describe the nature, scope, context and purposes of the processing;
  - assess necessity, proportionality and compliance measures;
  - identify and assess risks to individuals; and
  - identify any additional measures to mitigate those risks.

21 ACADEMY

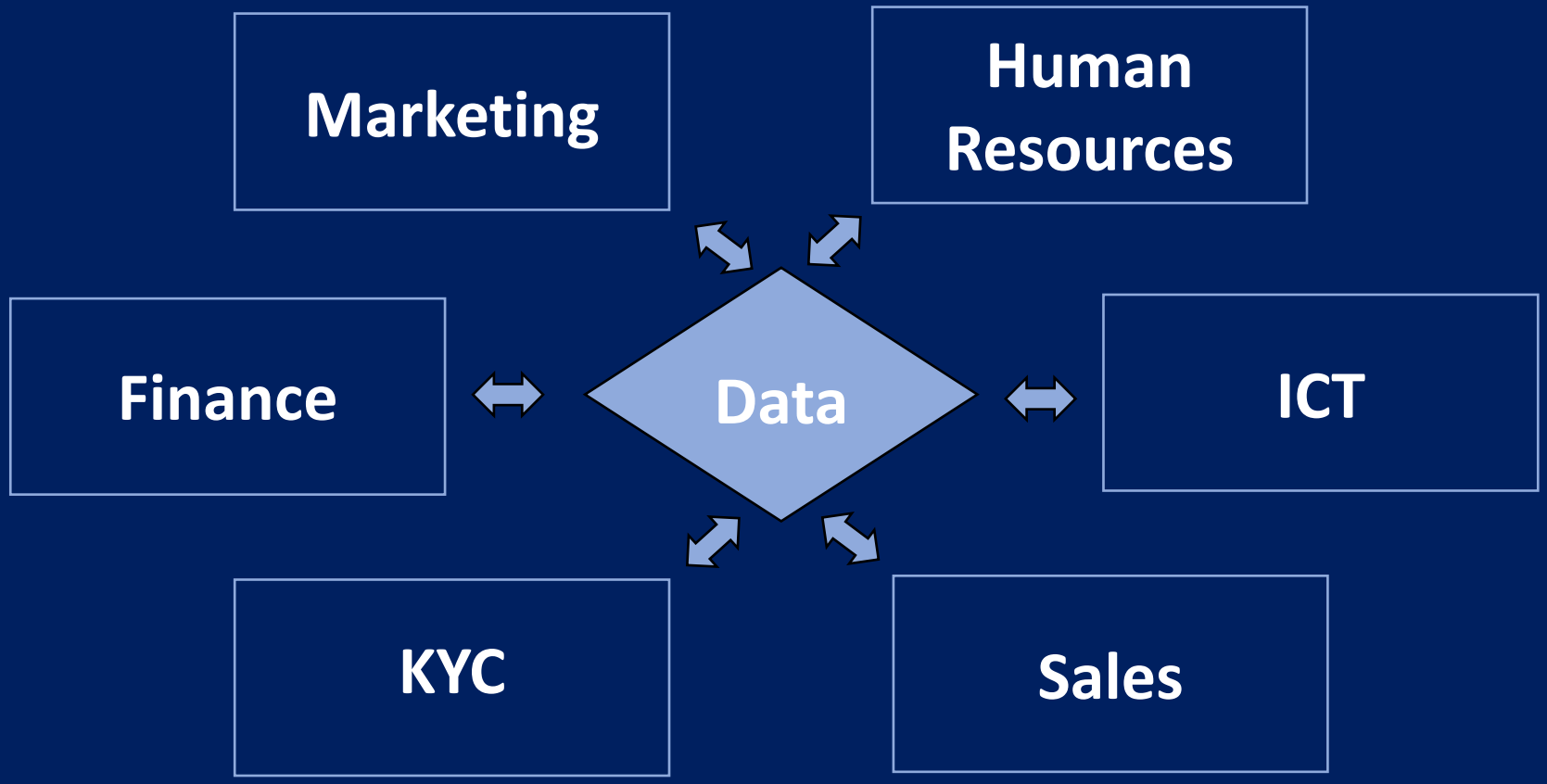
Company Data

Business/Office Data

Which typical Departments/Sections within a business/office generate/use/handle data?

60sec

Company/Office Data



Documentation

- Privacy Standard
- Privacy Notices (Clients, Candidates, Employees, Website)
- Data Processing Agreements
- Joint Controllers Agreements
- SAR Forms and Procedures
- Data Breach Procedure
- Data Protection Impact Assessment Template

21 ACADEMY

Information & Communication Technology Dept.

Physical vs Cyber Security

PHYSICAL 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

CYBER SECURITY

- **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

- 3-2-1 Backup
- Firewalls
- Most Secure Settings
- Access Control
- Malware Protection
- Up to Date
- Multi Factor Authentication
- Penetration Testing
- E-mail Security

21 ACADEMY

Human Resources Dept.

*"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."*

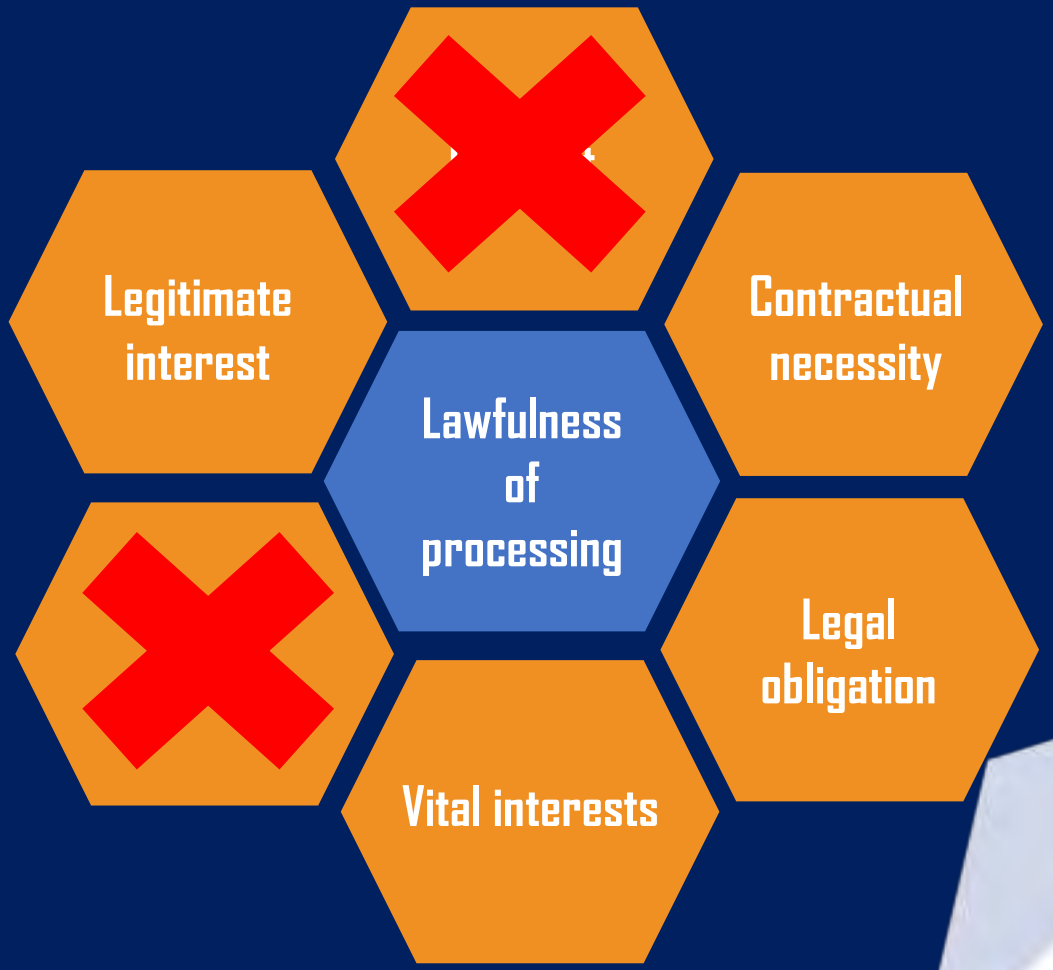
- Working Party 29

Types of Monitoring

- Email use
- Internet Use
- Telephone Use & Recordings
- CCTV
- Biometric
- Vehicles
- Automation
- Mystery Shopping
- Device

Legal Grounds

Processing is lawful if based on one of the following legal basis



Transparency

Employees must be informed:

- of the existence of monitoring;
- about the purposes for which their data are processed; and
- of any other information necessary to guarantee fair processing.

Transparency

Always have available:

- Acceptable use policy
- Privacy policies/information
- Signage

Transparency

What is missing in this notice from an HR perspective?

60sec

Transparency

- Privacy Notice to Candidates
- Privacy Notice to Employees

Transparency

ALWAYS

- The name and contact details of your organisation
- The purposes of the processing
- The lawful basis for the processing
- The retention periods for the personal data
- The rights available to individuals in respect of the processing
- The right to lodge a complaint with a supervisory authority

Transparency

IF APPLICABLE

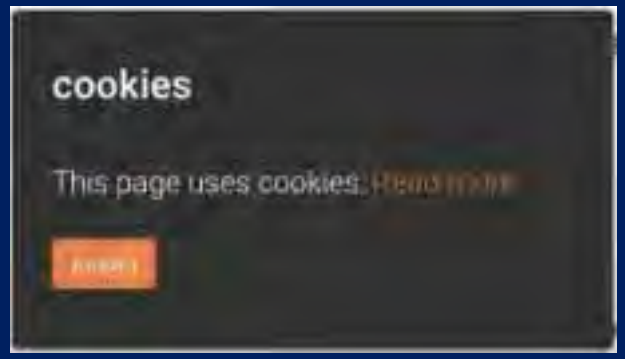
- The name and contact details of your representative
- The contact details of your data protection officer
- The legitimate interests for the processing
- The recipients, or categories of recipients of the personal data
- The details of transfers of the personal data to any third countries or international organisations
- The right to withdraw consent
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data
- The details of the existence of automated decision-making, including profiling

21 ACADEMY

Marketing Dept.

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

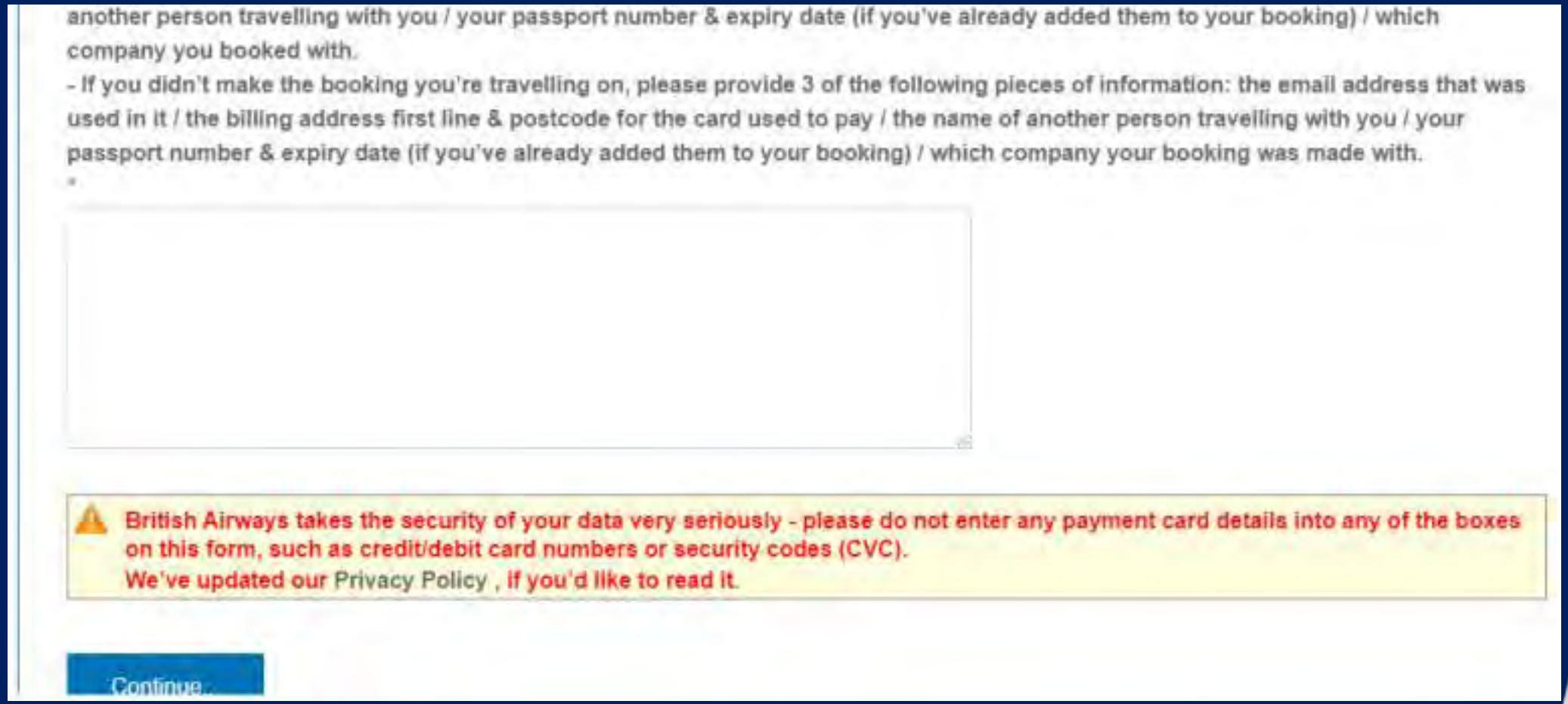
Secure Socket Layer (SSL)

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

Website Compliance



Website Compliance

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

including employees

Website Compliance

Payment Gateways

Make sure that they protect the personal data
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 DPA in place?

Question 1

The GDPR obviously covers email and email communications - does it also include telephone and postal communication?

Postal communication - door to door

Robo calling

Consent and GDPR compliance by list vendor

Question 2

Is double opt-in a guidance or a law? Does GDPR include 'double opt-in'? i.e. A website visitor said "OK" passively, but do I need to confirm their consent? Surely single consent is enough?

Guidance as good practice

Question 3

What about my contact database? Can I still email these people?

Who are the data subjects on your list?

Do you have their consent?

Question 4

How can you be sure to be compliant?

1	lawful, fair and transparent
2	specific, explicit and legitimate purpose
3	adequate, relevant and limited to what is necessary
4	accurate & up to date
5	storage limitation
6	integrity and confidentiality

Question 5

Does GDPR Block Advertisers from Running Competitions? How Do Marketers Deal With Consent in a Random Prize Draw?

Highlight each piece of data collected during the competition and what you are doing with it.

An individual dropping their business card into a prize draw

Question 6

Can we still ask people to refer friends or does it go against GDPR?

Never:

- record a referred friend's personal data
- send any message to a referred friend
- record any data about a referred friend until they have become your user and provided clear consent
- use cookies or beacons to build profiles of referred friends or to track their behaviour in any way

Question 7

What happens to the mailing list in the case of sale or acqusition of a business? Can I sell or buy the data?

- Information to data subjects
- New owner obliged to use that data according to Privacy Notice
- Otherwise data subjects to be informed with change of purpose

Question 8

Can you buy or sell a marketing list/database ?

Yes (but with lots of caution), if the list was lawfully obtained for that purpose.

[consent is the ground to rely on]

Question 9

Can a company use the same list for multiple brands?

Yes (with caution), if the list was lawfully obtained for that purpose + the customers are fully aware at the time of consent.

[do not rely on exception]

Question 10

How can a website be, or not be, compliant with data privacy legislation?

- Cookies
- Privacy Notices
- SSL
- Data Capturing Tools
  - Forms
  - Web Chat
  - Payment Gateways
- Photographs/videos

21 ACADEMY

Introduction to Business Law

Lecture Title: Data Protection - the Salient Features

Lecturer: Mr Angelito Sciberras

Date: 21 November 2023