www.21Academy.education

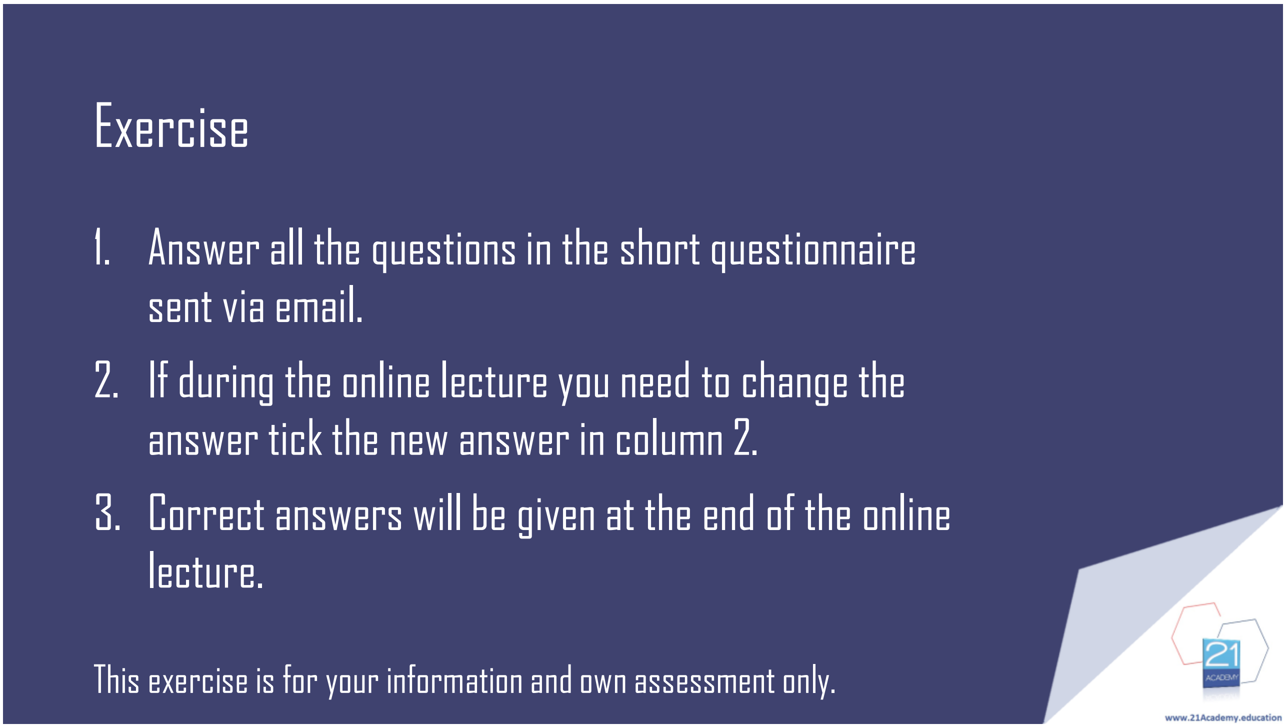
1

GDPR & Payroll Implications

Angelito Sciberras
June 2021

www.21Academy.education

2



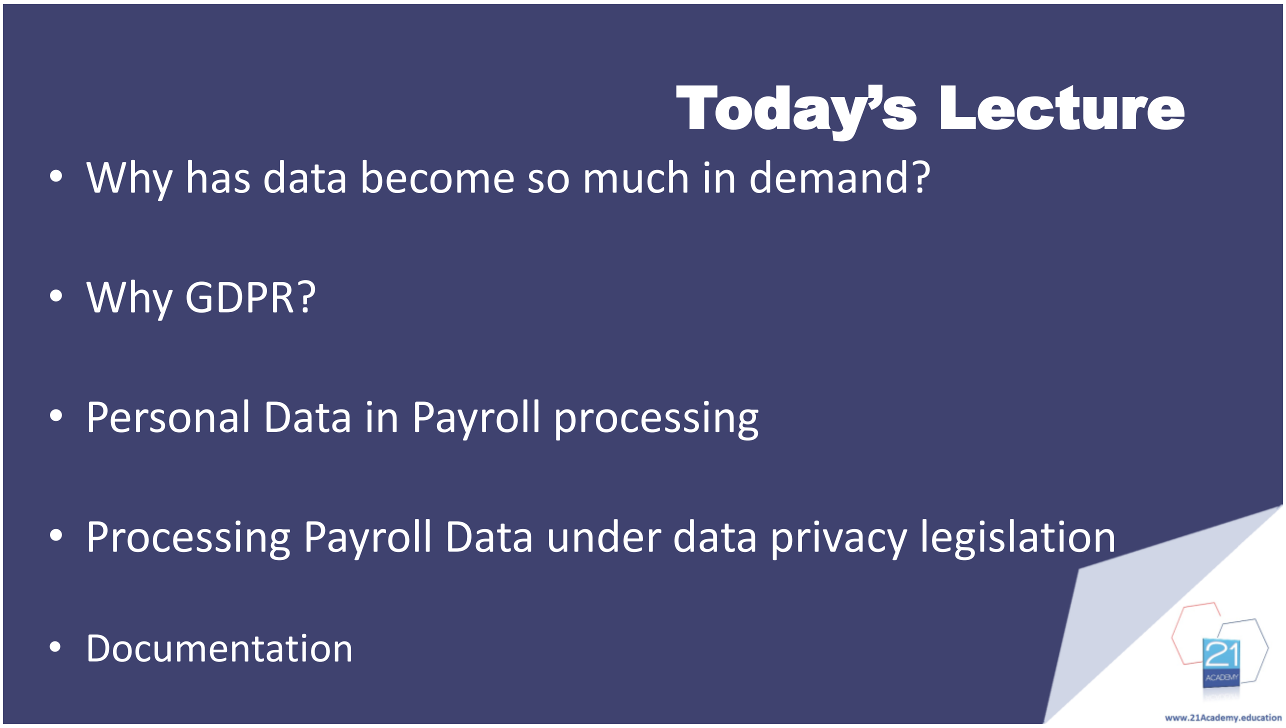
Exercise

1. Answer all the questions in the short questionnaire sent via email.
2. If during the online lecture you need to change the answer tick the new answer in column 2.
3. Correct answers will be given at the end of the online lecture.

This exercise is for your information and own assessment only.

www.21Academy.education

3



Today's Lecture

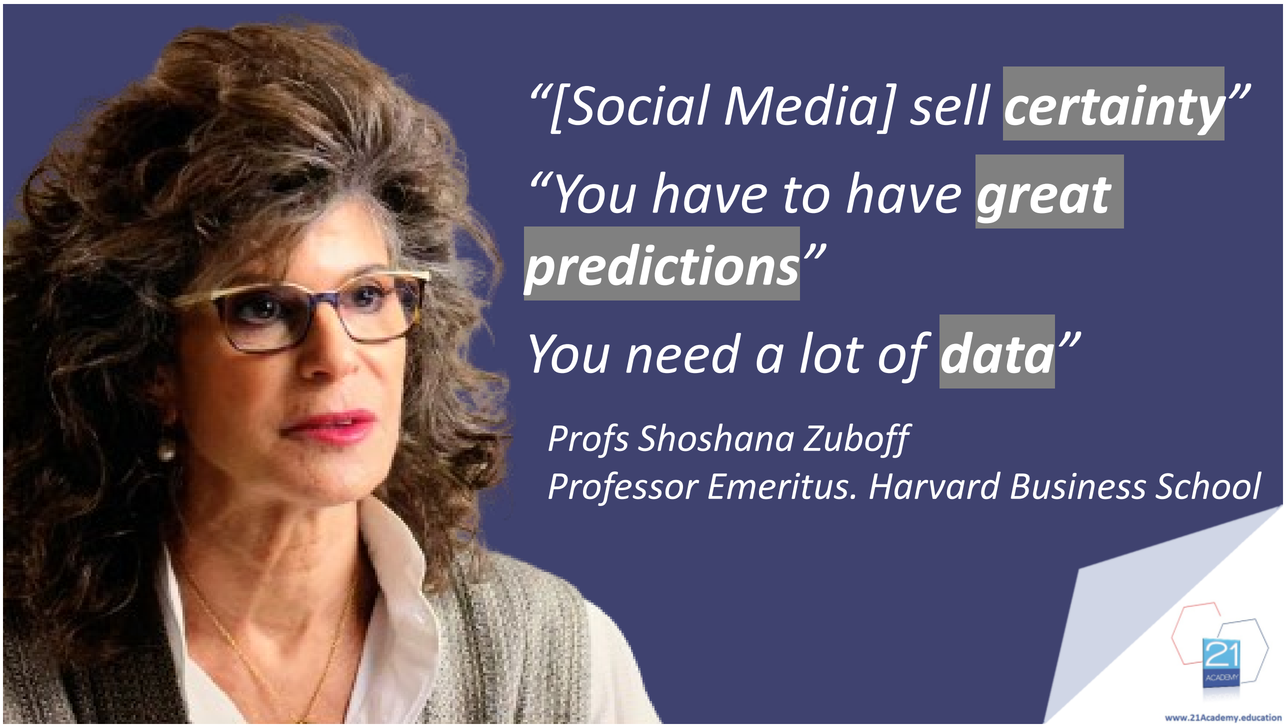
- Why has data become so much in demand?
- Why GDPR?
- Personal Data in Payroll processing
- Processing Payroll Data under data privacy legislation
- Documentation

www.21Academy.education

4

The intention of GDPR is to provide a ***common*** *set of rules across the EU that can meet the* ***changing data protection landscape*** *of today's world and give the* ***adequate protection*** *to individuals - known as "data subjects".*

www.21Academy.education



"[Social Media] sell ***certainty****"*

"You have to have ***great predictions****"*

You need a lot of ***data****"*

Profs Shoshana Zuboff
Professor Emeritus. Harvard Business School

www.21Academy.education

“The world’s most valuable resource is no longer oil, but data”

- The Economist, May 2017

www.21Academy.education

7

Data

What comes to mind when I say House of Cards?...

Actor...

City...

Production House...

Year...

www.21Academy.education

8

Data

VS

9

Data

- Committed to 26 episodes
- @ $3.8million per episode
- Without watching a single episode

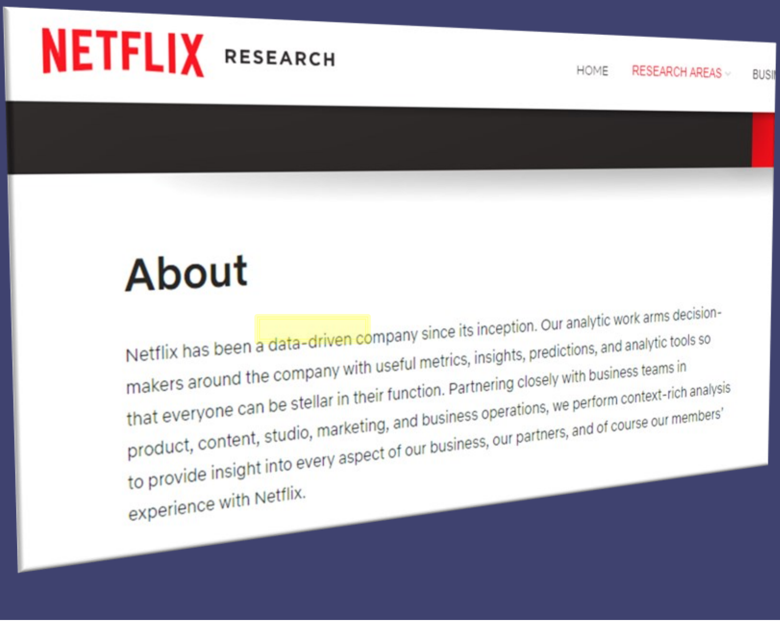
NETFLIX

HOW?

www.21Academy.education

10

Data



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.

11

Personal Data

12

Personal Data

www.21Academy.education

13

Personal Data

1. In 2014 a Facebook quiz invited users to find out their personality type

2. The app collected the data of those taking the quiz, but also recorded the public data of their friends

3. About 305,000 people installed the app, but it gathered information on up to 87 million people, according to Facebook

4. It is claimed at least some of the data was sold to Cambridge Analytica (CA) which used it to psychologically profile voters in the US

www.21Academy.education

14

Personal Data

15

16

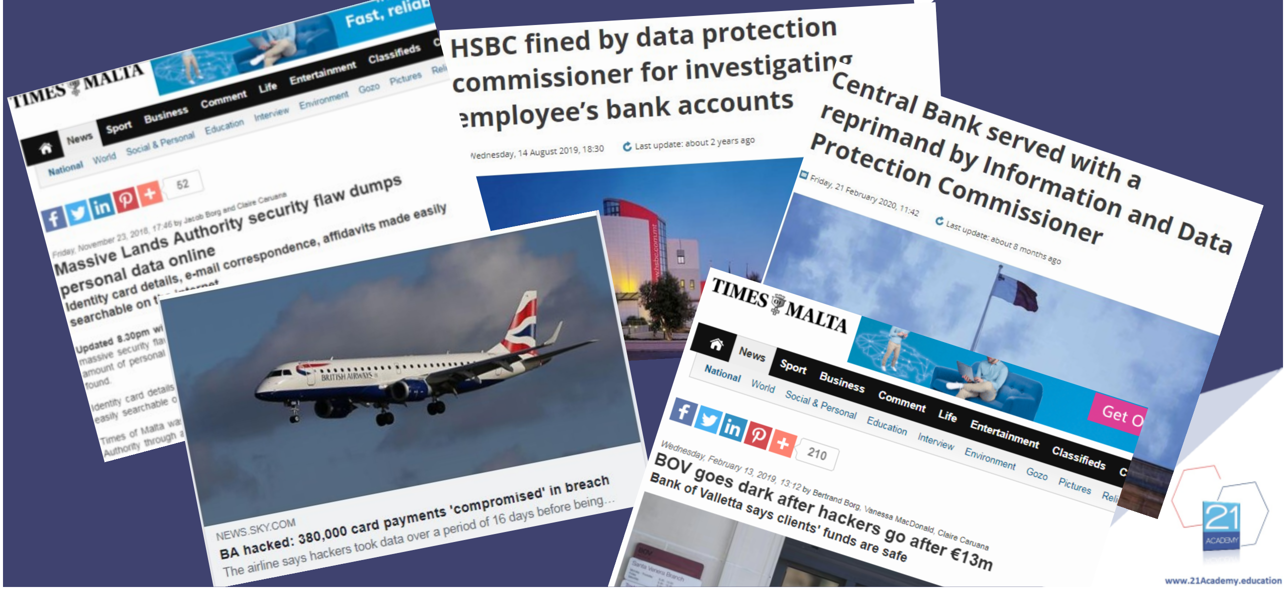
"If you are not paying for the product, then ***you are the product****"*

Tristan Harris
Former Design Ethicist, Google

www.21Academy.education

17

Why GDPR?



TIMES OF MALTA

Friday, November 23, 2018, 17:46 by Jacob Borg and Claire Caruana

Massive Lands Authority security flaw dumps personal data online

Identity card details, e-mail correspondence, affidavits made easily searchable on t

NEWS.SKY.COM

BA hacked: 380,000 card payments 'compromised' in breach

The airline says hackers took data over a period of 16 days before being...

HSBC fined by data protection commissioner for investigating employee's bank accounts

Wednesday, 14 August 2019, 18:30 · Last update: about 2 years ago

Central Bank served with a reprimand by Information and Data Protection Commissioner

Friday, 21 February 2020, 11:42 · Last update: about 8 months ago

TIMES OF MALTA

Wednesday, February 13, 2019, 13:12 by Bertrand Borg, Vanessa MacDonald, Claire Caruana

BOV goes dark after hackers go after €13m

Bank of Valletta says clients' funds are safe

www.21Academy.education

18

Why GDPR?

What is the GDPR?

The intention of GDPR is to provide a common set of rules across the EU that can meet the changing data projection landscape of today's world and give the adequate protection to individuals - known as 'data subjects’.

It repealed Directive 95/46/EC

Macintosh Performa 6200

IBM Personal Communicator

Kodak DCS 460 Camera

Iomega Zip Drive

Motorola Tango Pager

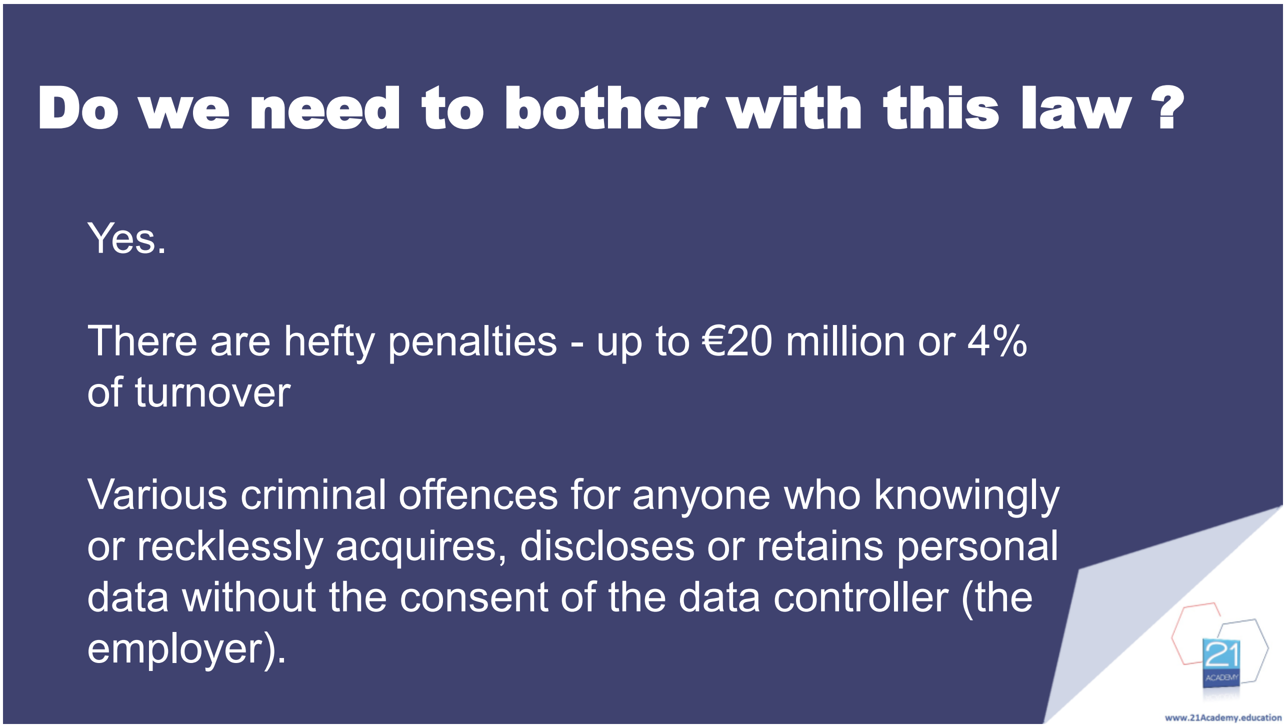
IBM ThinkPad 701C

Sony Handycam DCR-VX1000

DVDs

21

22



Do we need to bother with this law ?

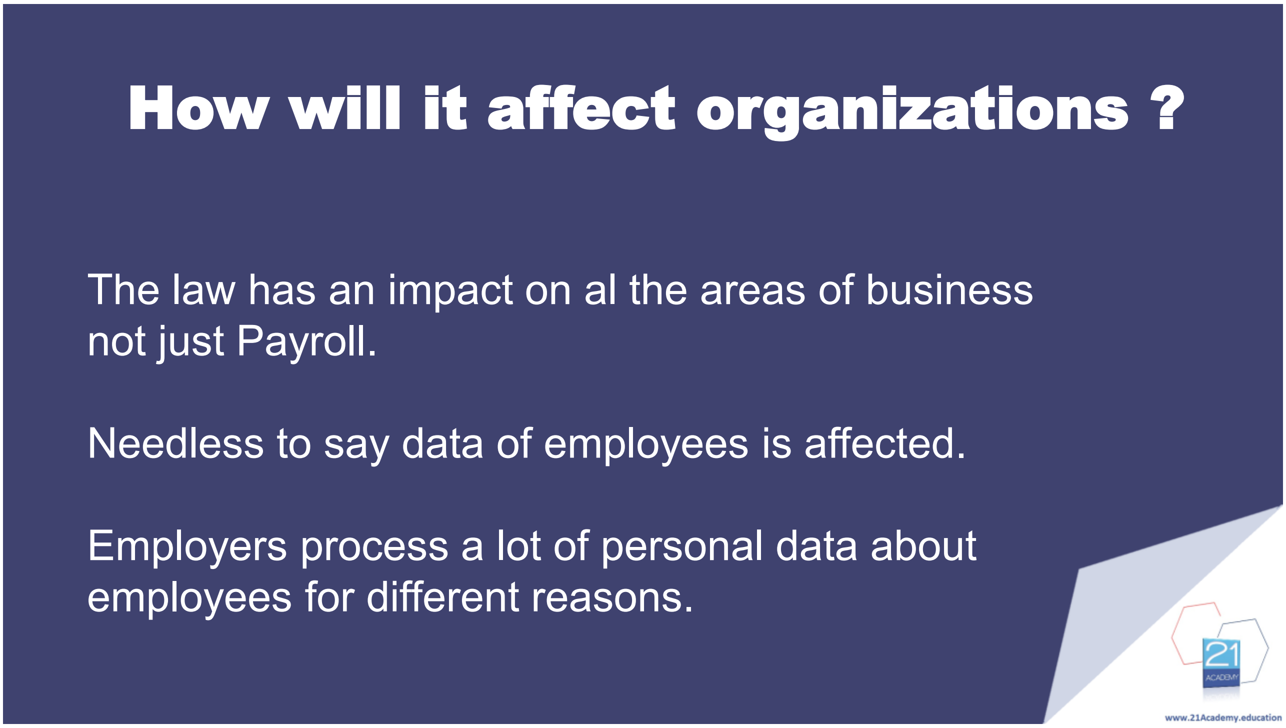
Yes.

There are hefty penalties - up to €20 million or 4% of turnover

Various criminal offences for anyone who knowingly or recklessly acquires, discloses or retains personal data without the consent of the data controller (the employer).

www.21Academy.education

23



How will it affect organizations ?

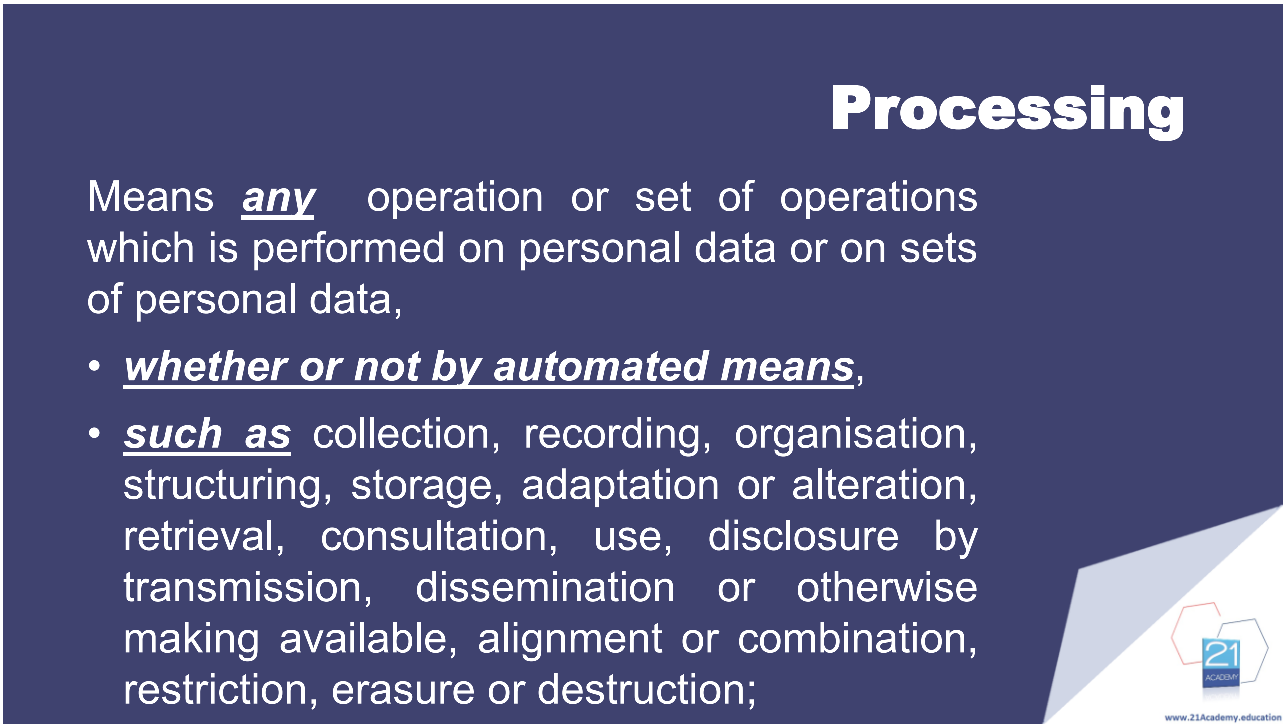
The law has an impact on al the areas of business not just Payroll.

Needless to say data of employees is affected.

Employers process a lot of personal data about employees for different reasons.

www.21Academy.education

24

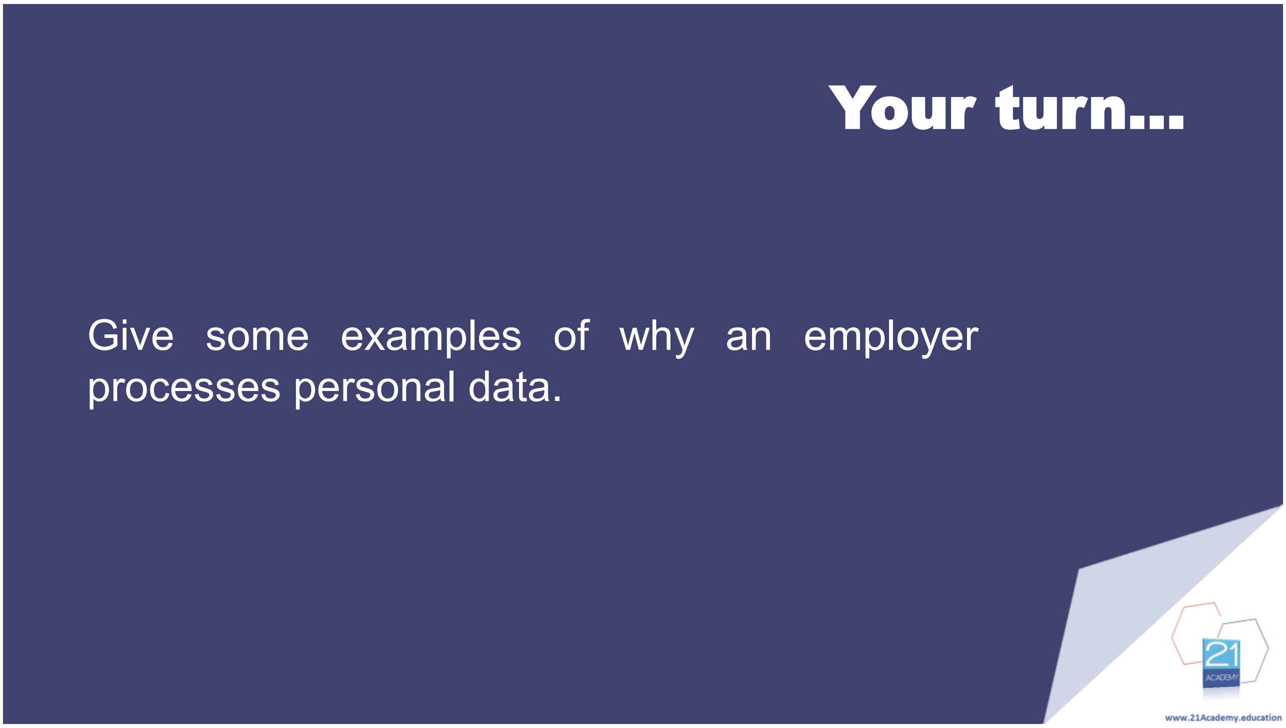


Processing

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;

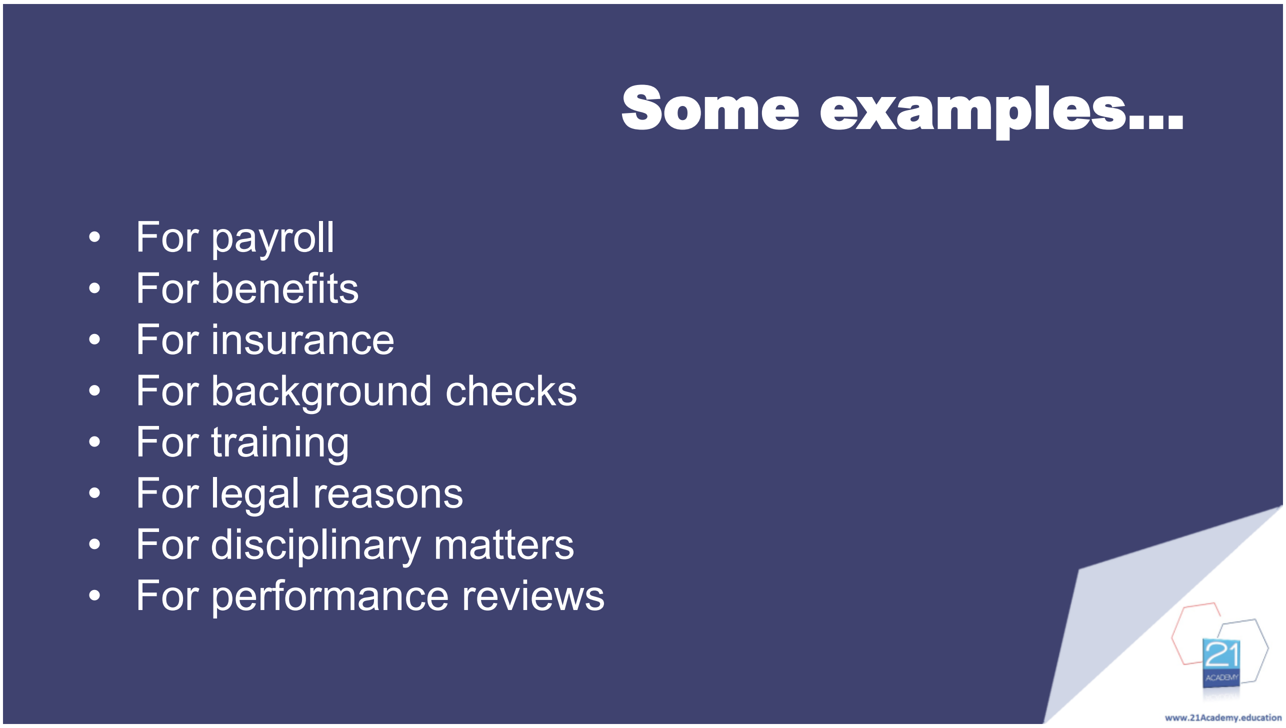
www.21Academy.education



Your turn…

Give some examples of why an employer processes personal data.

www.21Academy.education

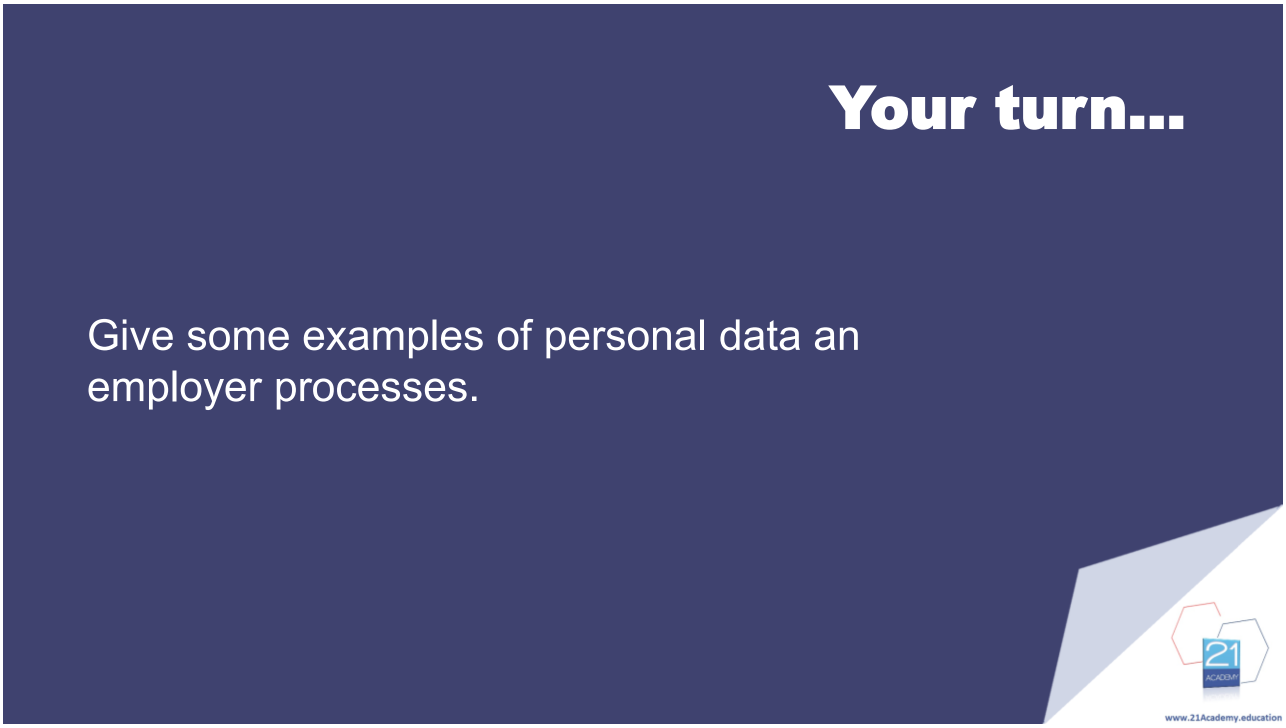


Some examples...

- For payroll
- For benefits
- For insurance
- For background checks
- For training
- For legal reasons
- For disciplinary matters
- For performance reviews

www.21Academy.education

27



Your turn...

Give some examples of personal data an employer processes.

www.21Academy.education

28

Some examples…

- Contact Details
- Financial
- Union Membership
- Health
- CCTV
- Files notes
- Tax Number
- Criminal?

www.21Academy.education

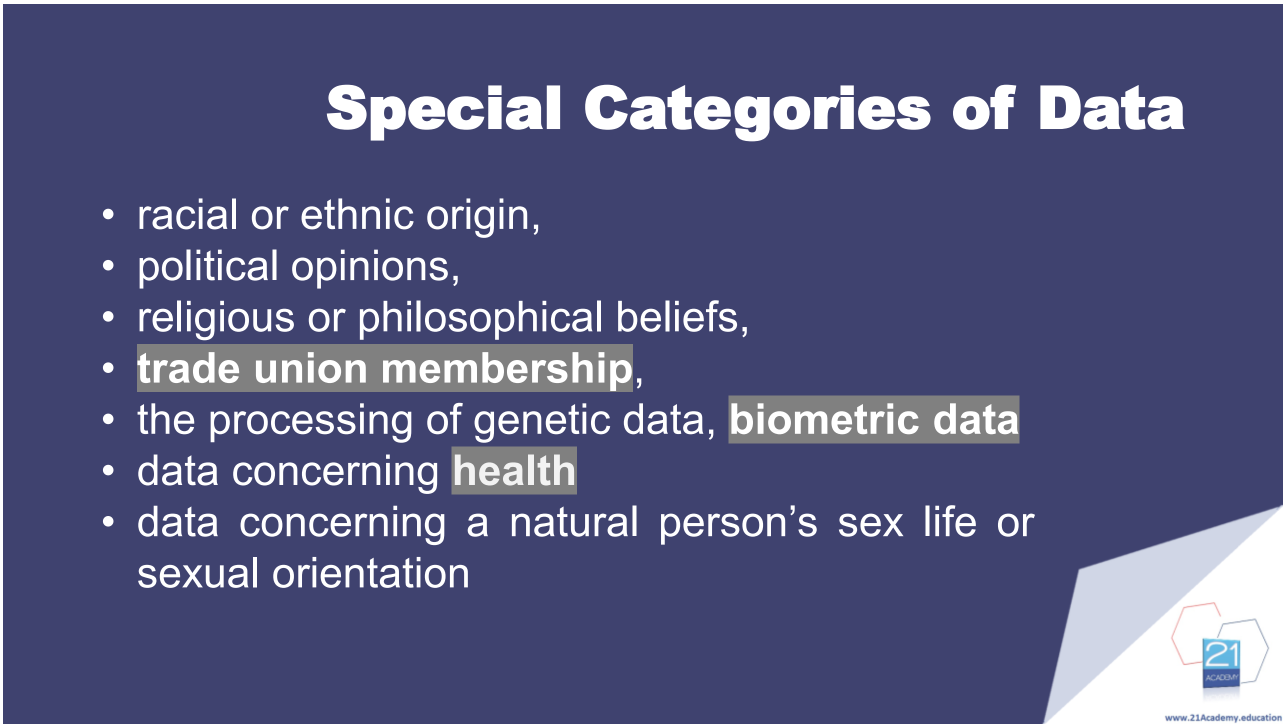
29

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;

www.21Academy.education

30

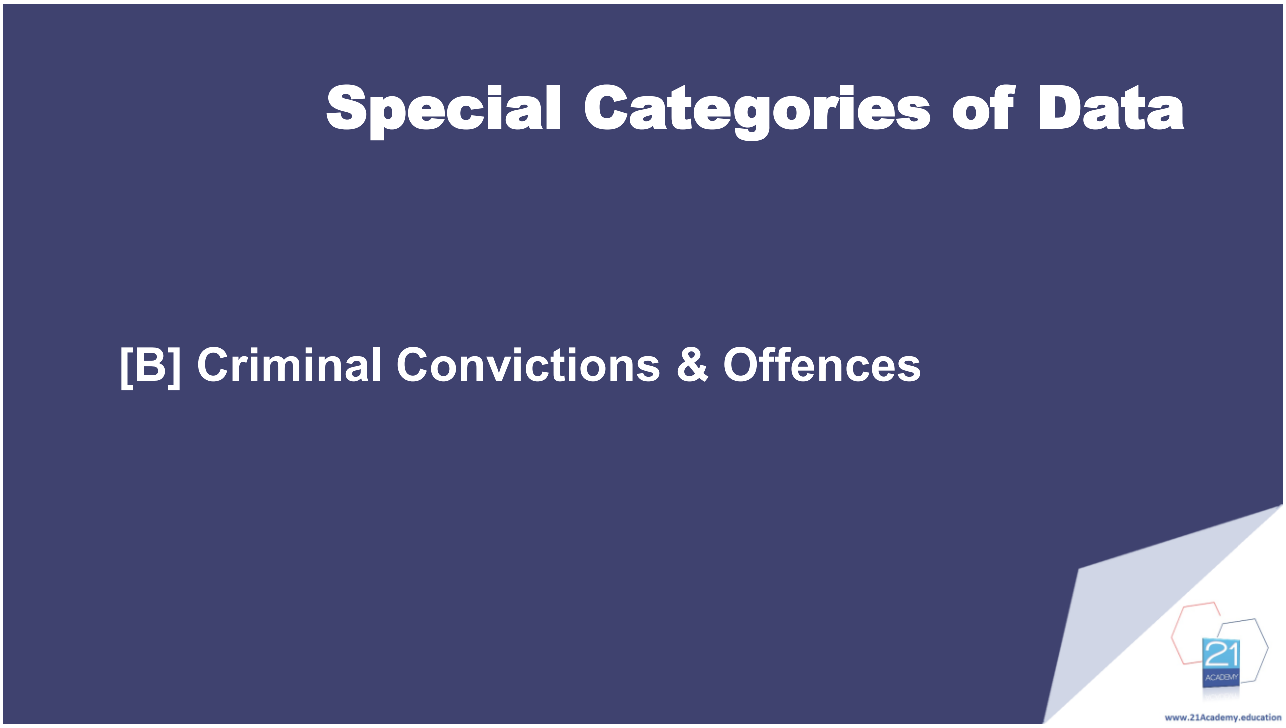


Special Categories of Data

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

www.21Academy.education

31



Special Categories of Data

[B] Criminal Convictions & Offences

www.21Academy.education

32

Data Protection Act (Cap. 440)

The implications in the employment context

Identity Cards

Criminal History

Fines & Penalties

Damages - including Moral Damages

www.21Academy.education

33

Processing of Special Categories

Only allowed to process in specific situations

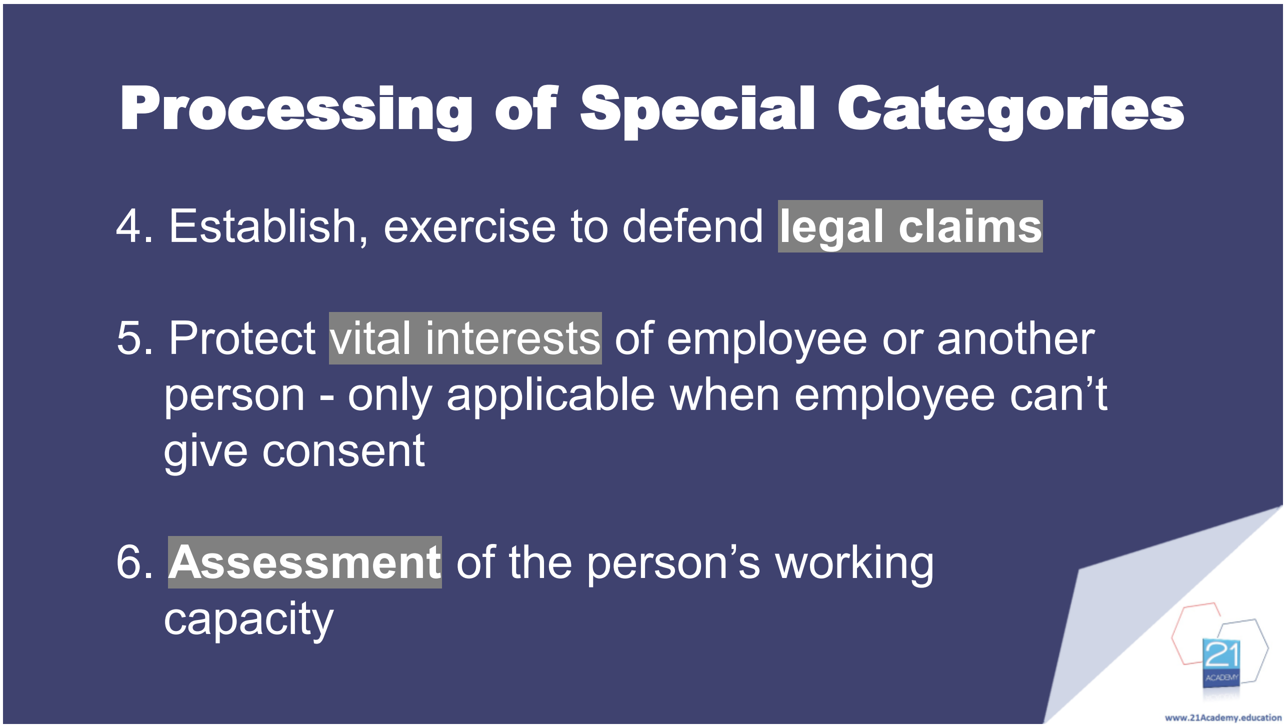
1. **Explicit consent** from employee

2. Data made **public** by employee - social media

3. **Rights and obligations** under employment law - H&S

www.21Academy.education

34



Processing of Special Categories

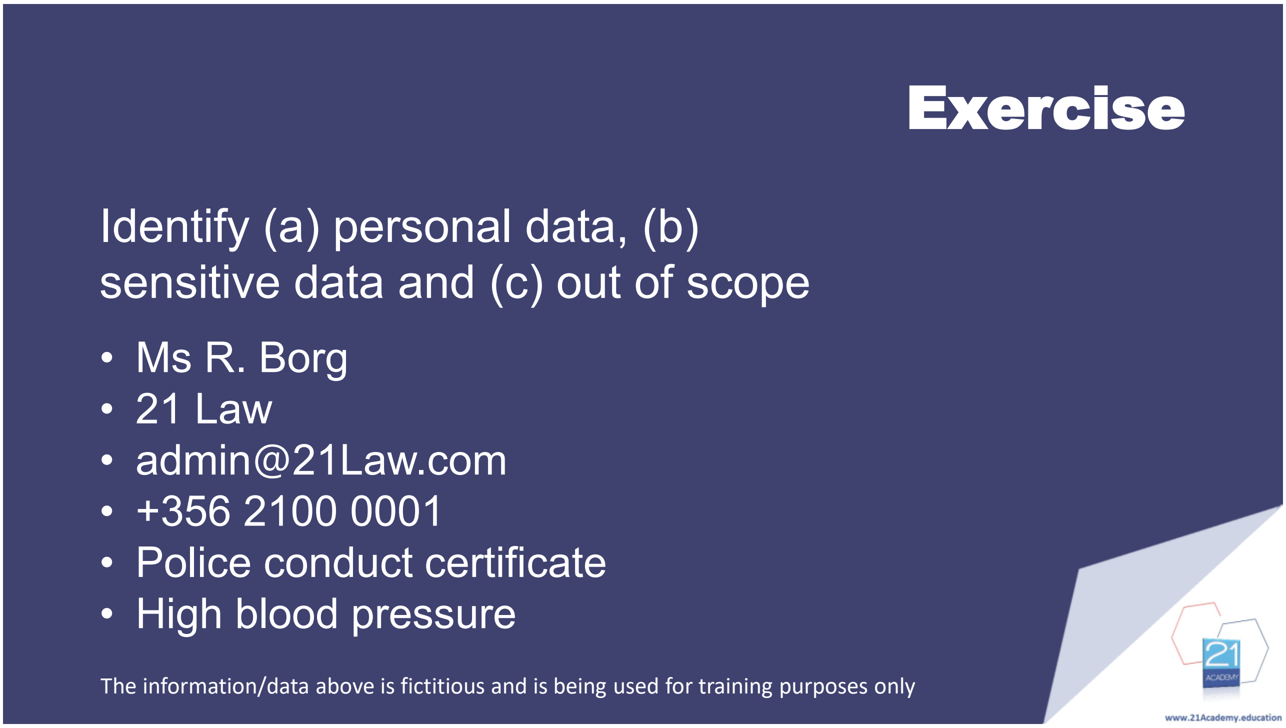
4. Establish, exercise to defend **legal claims**

5. Protect vital interests of employee or another person - only applicable when employee can’t give consent

6. **Assessment** of the person’s working capacity

www.21Academy.education

35



Exercise

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

- Ms R. Borg
- 21 Law
- admin@21Law.com
- +356 2100 0001
- Police conduct certificate
- High blood pressure

The information/data above is fictitious and is being used for training purposes only

www.21Academy.education

36

Controller & Processor

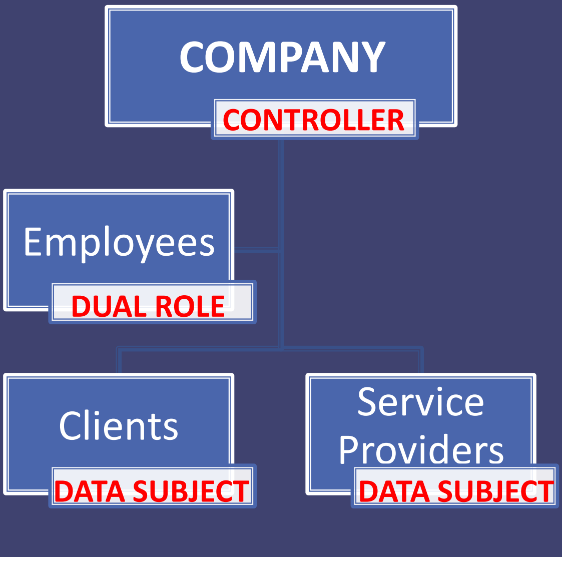
'**Controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

'**Processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (sub-contractor)

www.21Academy.education

37

Controller & Processor



COMPANY

CONTROLLER

Employees

DUAL ROLE

Clients

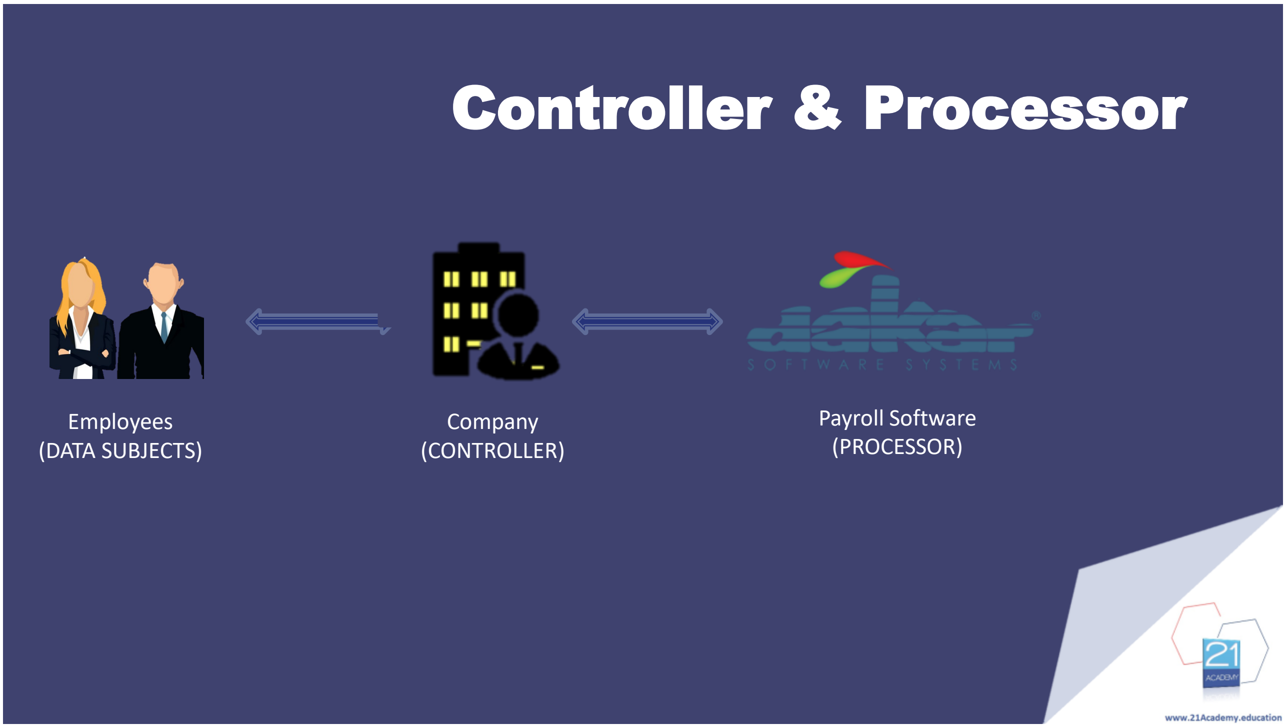
DATA SUBJECT

Service Providers

DATA SUBJECT

www.21Academy.education

38



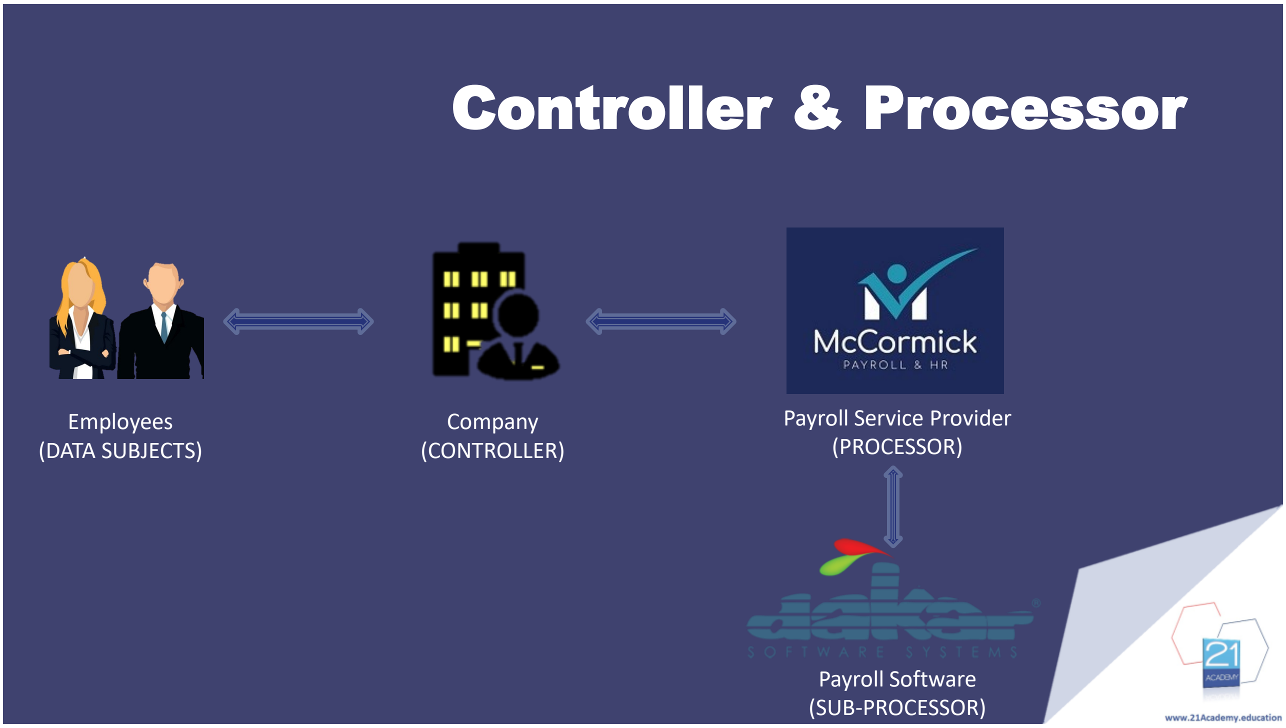
Controller & Processor

Employees
(DATA SUBJECTS)

Company
(CONTROLLER)

Payroll Software
(PROCESSOR)

39



Controller & Processor

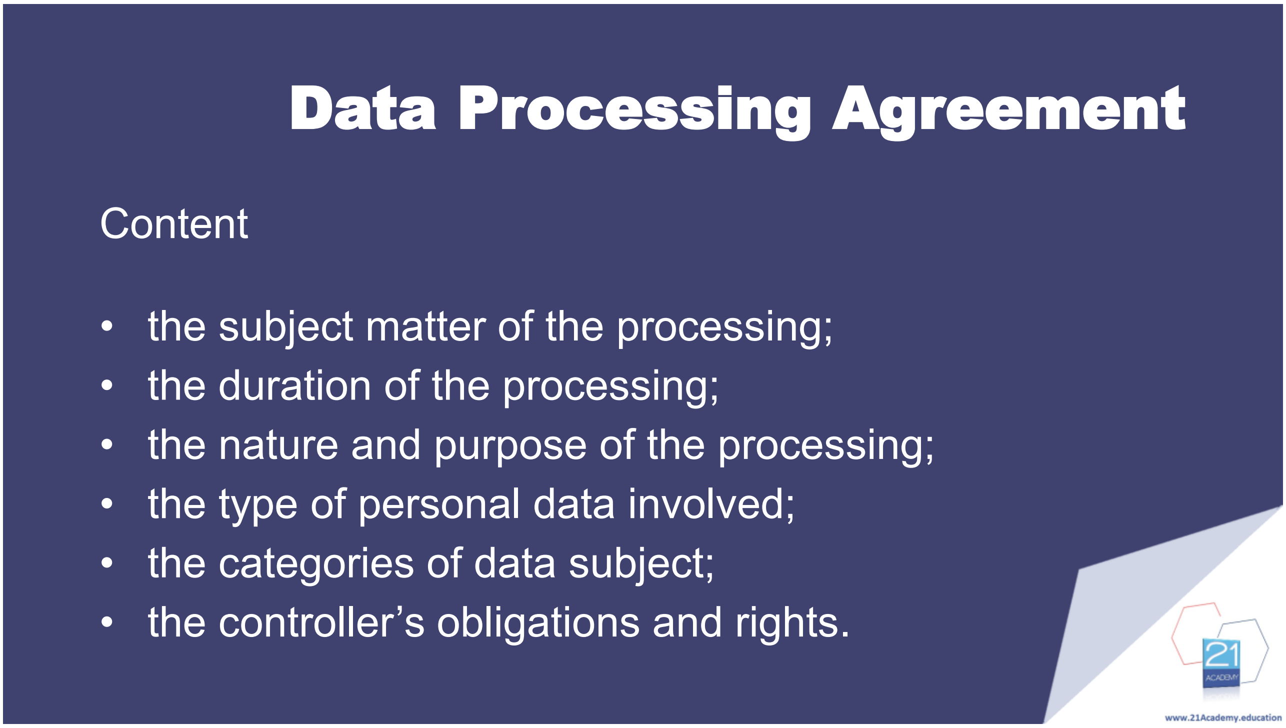
Employees
(DATA SUBJECTS)

Company
(CONTROLLER)

Payroll Service Provider
(PROCESSOR)

Payroll Software
(SUB-PROCESSOR)

40



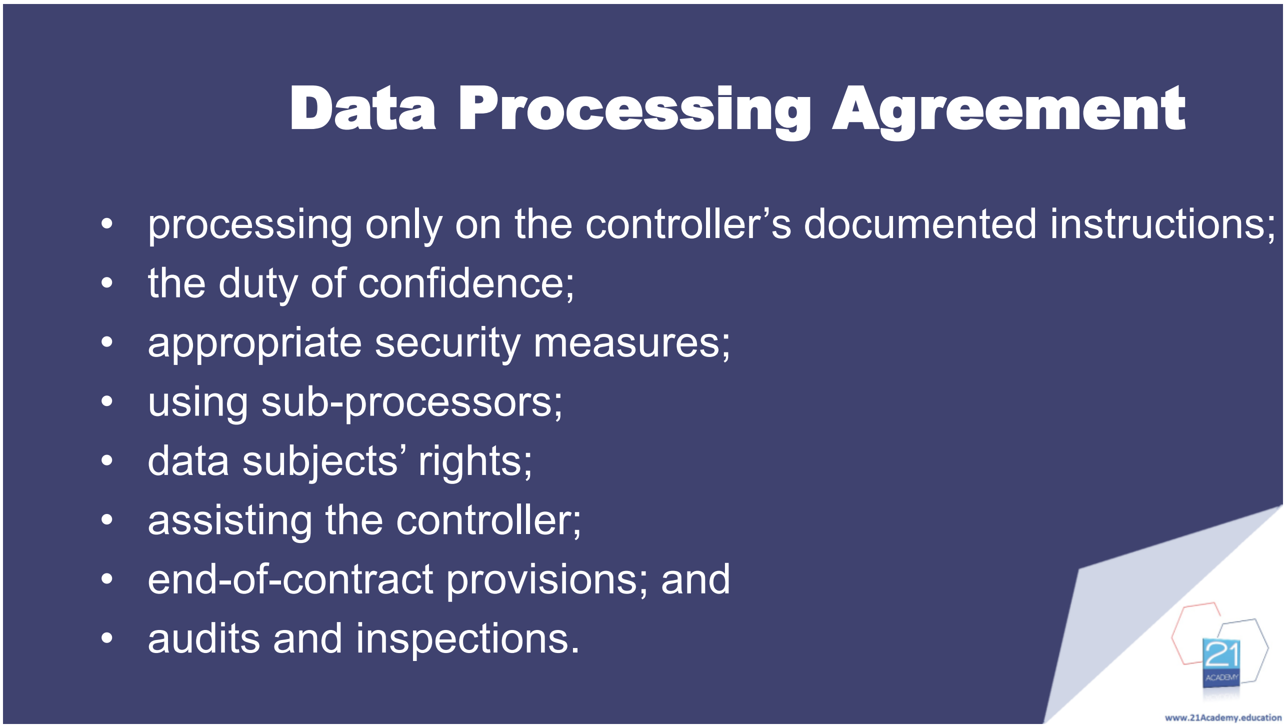
Data Processing Agreement

Content

- the subject matter of the processing;
- the duration of the processing;
- the nature and purpose of the processing;
- the type of personal data involved;
- the categories of data subject;
- the controller's obligations and rights.

www.21Academy.education

41

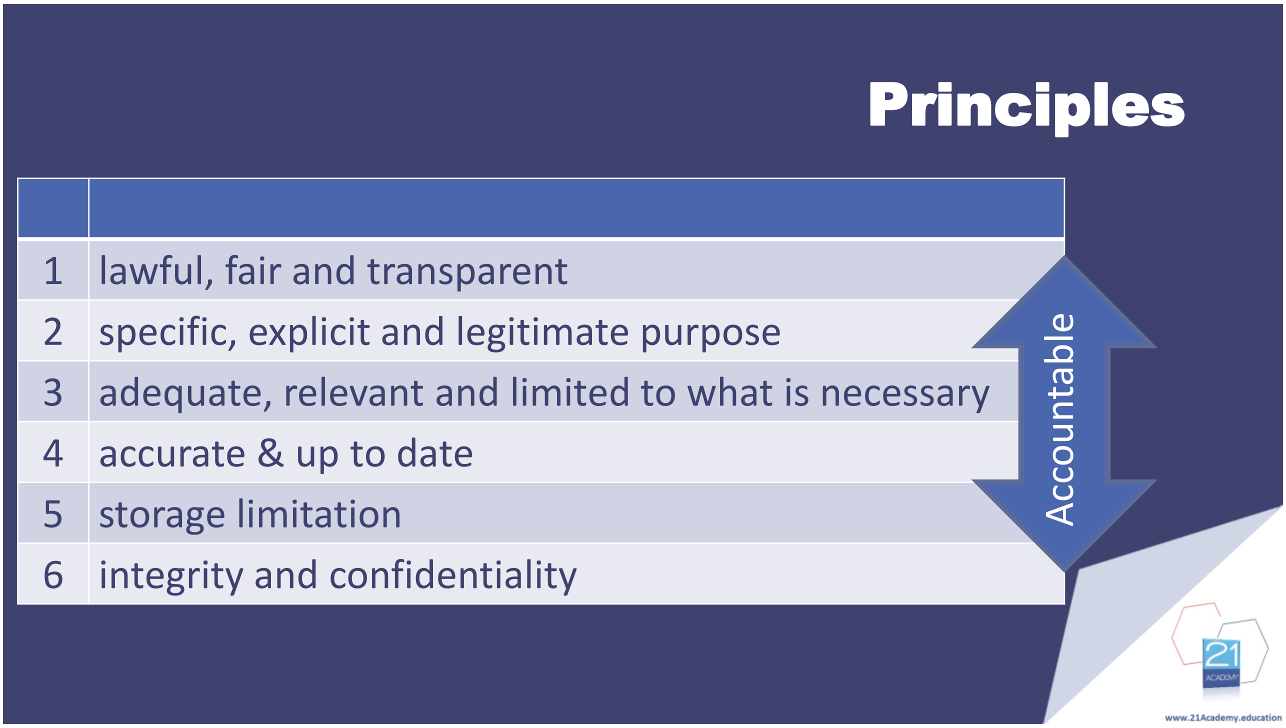


Data Processing Agreement

- processing only on the controller's documented instructions;
- the duty of confidence;
- appropriate security measures;
- using sub-processors;
- data subjects' rights;
- assisting the controller;
- end-of-contract provisions; and
- audits and inspections.

www.21Academy.education

42



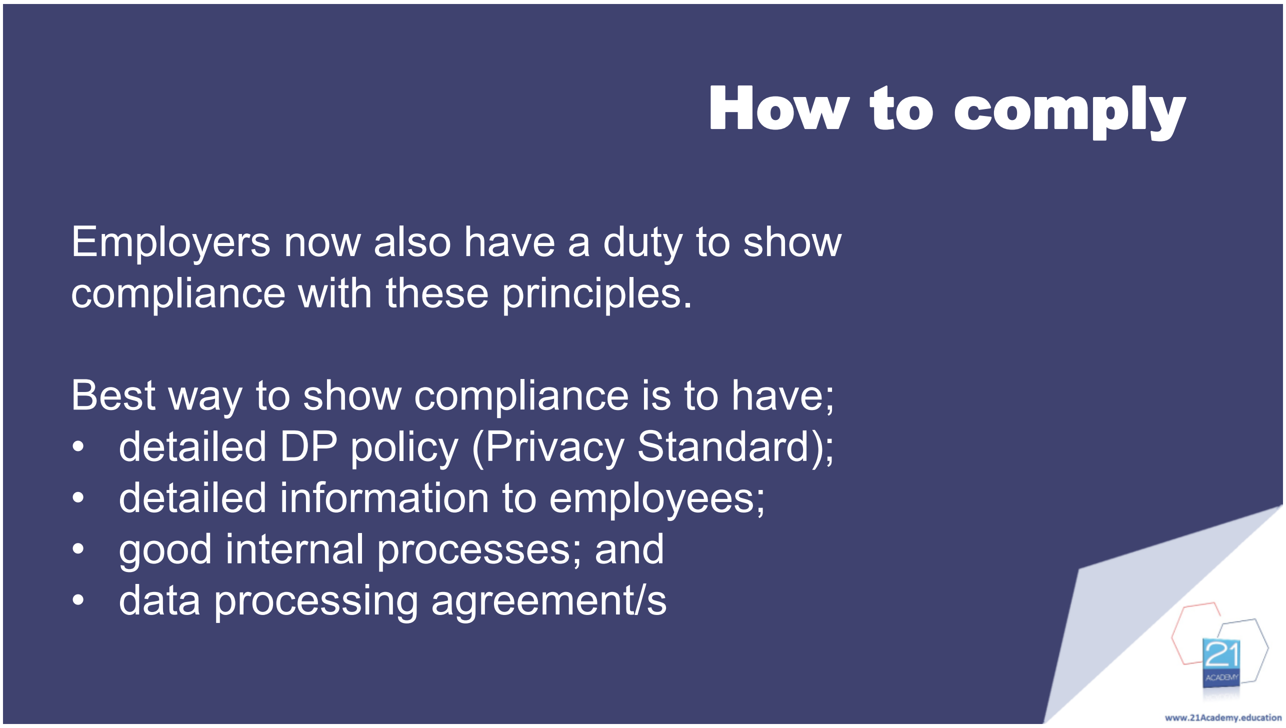
Principles

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

Accountable

www.21Academy.education

43



How to comply

Employers now also have a duty to show compliance with these principles.

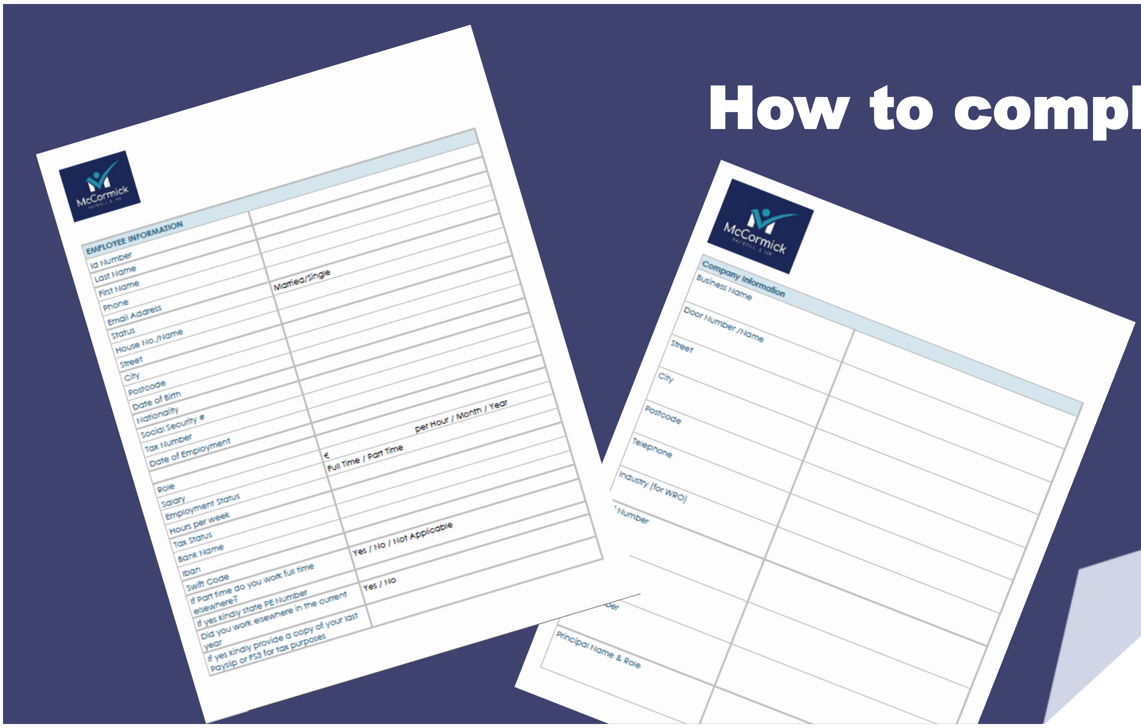
Best way to show compliance is to have;

- detailed DP policy (Privacy Standard);
- detailed information to employees;
- good internal processes; and
- data processing agreement/s

www.21Academy.education

44

How to comply



EMPLOYEE INFORMATION	
Id Number	
Last Name	
First Name	
Phone	
Email Address	
Status	Married/Single
House No./Name	
Street	
City	
Postcode	
Date of Birth	
Nationality	
Social Security #	
Tax Number	
Date of Employment	
Role	
Salary	€ per Hour / Month / Year
Employment Status	Full Time / Part Time
Hours per week	
Tax Status	
Bank Name	
Iban	
Swift Code	
If Part time do you work full time elsewhere?	Yes / No / Not Applicable
If yes kindly state PE Number	
Did you work elsewhere in the current year	Yes / No
If yes kindly provide a copy of your last Payslip or FS3 for tax purposes	

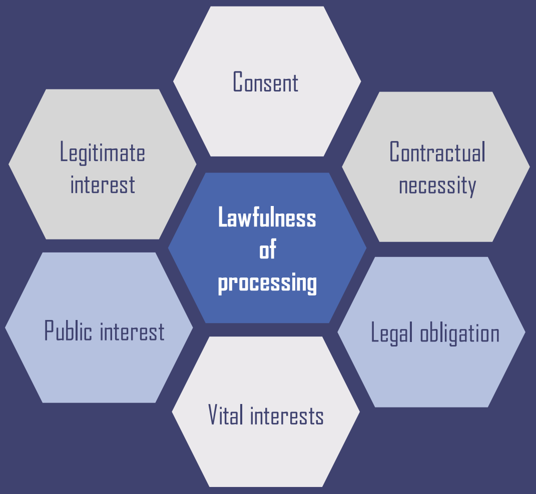
Company Information	
Business Name	
Door Number /Name	
Street	
City	
Postcode	
Telephone	
Industry (for WRO)	
Number	
ber	
Principal Name & Role	

www.21Academy.education

45

Legal Grounds

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



www.21Academy.education

46

The problem with Consent

Imbalance of power between employer and employee.

You cannot just insert a clause in the contract of employment - an employee would have not much option but to accept.

www.21Academy.education

47

The problem with Consent

PWC Business Solutions fined **€150,000**

i. has unlawfully processed the personal data of its employees contrary to the provisions of Article 5(1)(a) indent (a) of the GDPR since it used an inappropriate legal basis.

ii. has processed the personal data of its employees in an unfair and non-transparent manner contrary to the provisions of Article 5(1)(a) indent (b) and (c) of the GDPR giving them the false impression that it was processing their data under the legal basis of consent pursuant to Article 6(1)(a) of the GDPR, while in reality it was processing their data under a different legal basis about which the employees had never been informed.

iii. although it was responsible in its capacity as the controller, it was not able to demonstrate compliance with Article 5(1) of the GDPR, and that it violated the principle of accountability set out in Article 5(2) of the GDPR by transferring the burden of proof of compliance to the data subjects.

www.21Academy.education

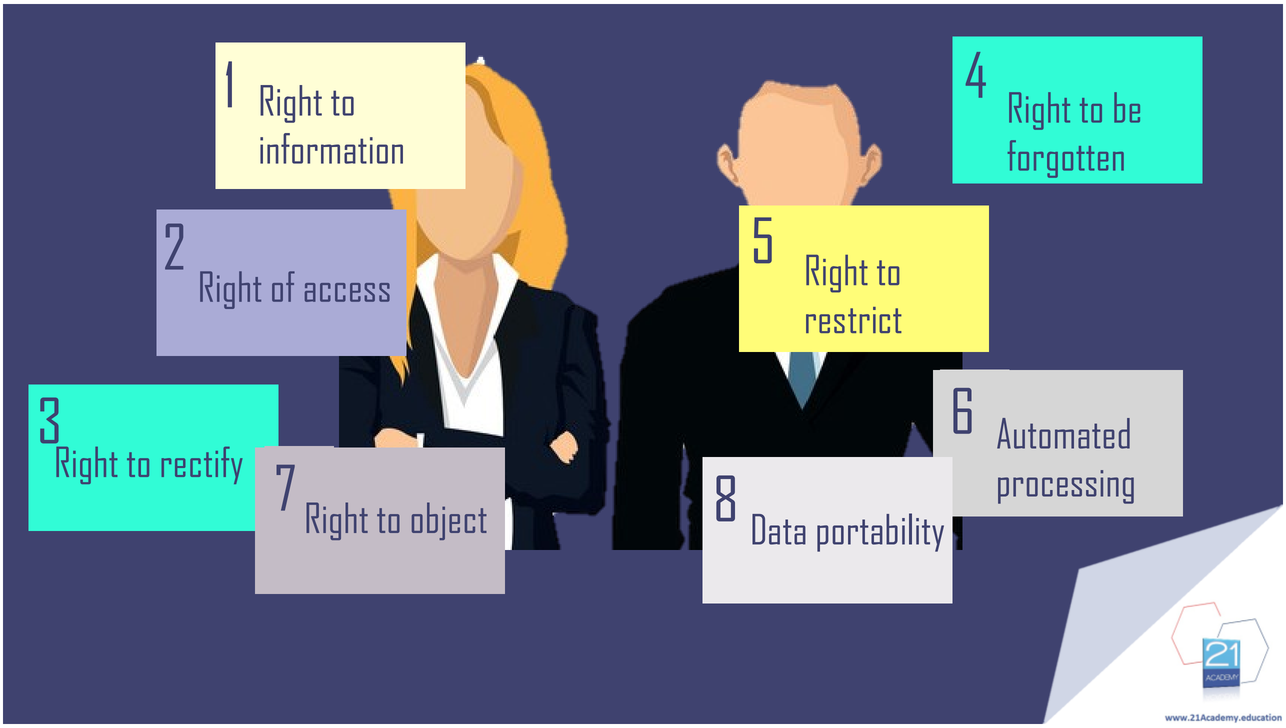
48

Relying on consent

Name circumstances when we have to rely on consent...

www.21Academy.education

49



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

www.21Academy.education

50

Breaches of security

Can you name examples of data breach incidents except for hacking?

Breaches of security

- loss or theft of hard copy notes, USB drives, computers or mobile devices
- sending an email with personal data (eg. pay slip) to the wrong person
- a bulk email using 'to' or 'cc', but where 'bcc' (blind carbon-copy) should have been used
- a disgruntled employee copying a list of contacts for their personal use
- a break-in at the office where personnel files are kept in unlocked storage

Breaches of security

Data subject to be informed without undue delay

IDPC to be notified within 72 hours of breach

Clear internal process should be issued so that everyone knows in which situation a breach needs to be notified and who has responsibility to make those decisions.

www.21Academy.education

GDPR

for HR Professionals

Roselyn Borg Knight

Paul Gonzi

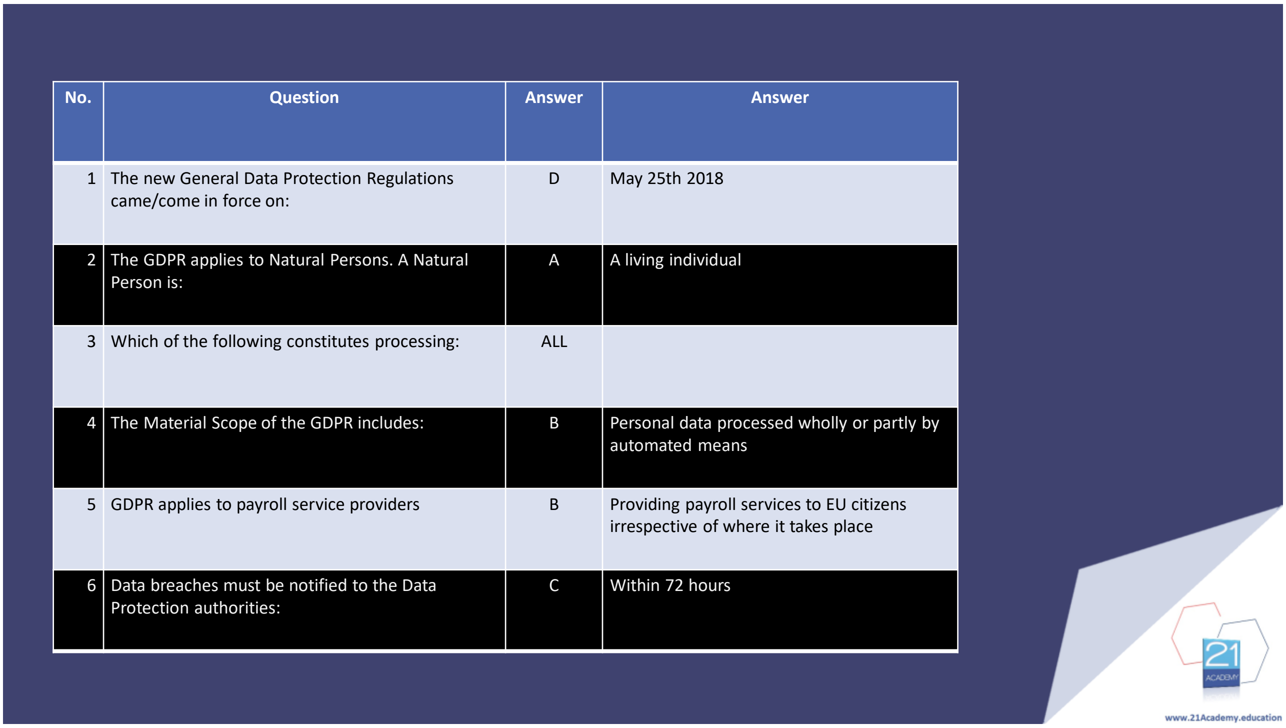
Angelito Sciberras

Sponsored by pkf

Payroll Checklist

Step 1 - Raise awareness
Step 2 - Data audit
Step 3 - Reasons that particular data is obtained
Step 4 - Legal basis you will rely on
Step 5 - Review/update employment contracts and policies
Step 6 - Review/update your internal processes
Step 7 - Review/update your external contracts and processes
Step 8 - Data protection compliance responsibility
Step 9 - Training
Step 10 - Keep compliant

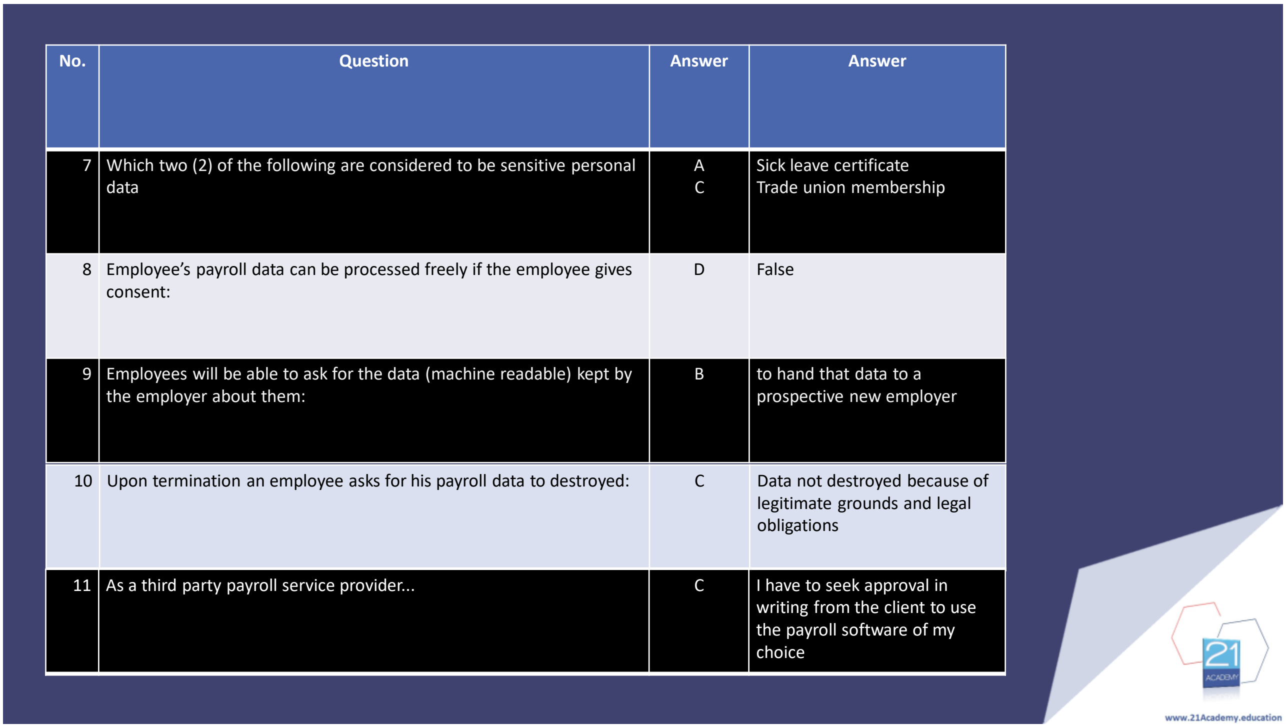
www.21Academy.education



No.	Question	Answer	Answer
1	The new General Data Protection Regulations came/come in force on:	D	May 25th 2018
2	The GDPR applies to Natural Persons. A Natural Person is:	A	A living individual
3	Which of the following constitutes processing:	ALL	
4	The Material Scope of the GDPR includes:	B	Personal data processed wholly or partly by automated means
5	GDPR applies to payroll service providers	B	Providing payroll services to EU citizens irrespective of where it takes place
6	Data breaches must be notified to the Data Protection authorities:	C	Within 72 hours

www.21Academy.education

55



No.	Question	Answer	Answer
7	Which two (2) of the following are considered to be sensitive personal data	A C	Sick leave certificate Trade union membership
8	Employee's payroll data can be processed freely if the employee gives consent:	D	False
9	Employees will be able to ask for the data (machine readable) kept by the employer about them:	B	to hand that data to a prospective new employer
10	Upon termination an employee asks for his payroll data to destroyed:	C	Data not destroyed because of legitimate grounds and legal obligations
11	As a third party payroll service provider...	C	I have to seek approval in writing from the client to use the payroll software of my choice

www.21Academy.education

56

GDPR & Payroll Implications

Angelito Sciberras
June 2021

www.21Academy.education

57

www.21Academy.education

58