

GDPR & Payroll Implications

Angelito Sciberras
11 November 2024



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.



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



*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".*



Pregnancy and Power of Data



Why the hell are you sending these maternity coupons to my daughter?



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

- The Economist, May 2017



Data vs Personal Data



Data vs Personal Data

facts and statistics collected together for reference or analysis

VS

any information relating to an identified or identifiable individual



Data

NETFLIX

amazon
prime video


HBOmax



Data

NETFLIX

60sec

You have been employed by Netflix...

...your friends ask you, what is Netflix? What does it do?

How would you answer?



Data

About

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



Personal Data



Personal Data





NETFLIX



*“If you are not paying for the product, then **you are the product**”*

*Tristan Harris
Former Design Ethicist, Google*



Why GDPR?

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

Massive Lands Authority security flaw dumps personal data online
identity card details, e-mail correspondence, vehicle registration numbers on the internet

IT firm C-Planet fined €65,000 over massive voter data breach

Ombudsman website is probed over security risk

Hellenic Data Protection Authority fines PWC for reported employee data breach

Value of Data

What value does company data have?

- Email addresses
- Mobile numbers

Copies of ID cards?

For what purpose?



Value of Data

The screenshot shows a website for 'MALTESE ID CARD'. The header includes the 'REAL FAKE' logo and navigation links: Home, About Us, All Documents, How To Order, and Contact Us. A WhatsApp icon and the number '91 988 88 8888' are in the top right. The main heading is 'MALTESE ID CARD' with a breadcrumb trail 'Home >> MALTESE ID CARD'. Below this, a product image shows a Maltese ID card with a photo of a woman and the name 'REGINA'. To the right, the price is listed as '350,000'. A WhatsApp icon is visible in the bottom left corner.

<https://www.realfakedocument.com/product/maltese-id-card>



Why GDPR?



What is the GDPR?

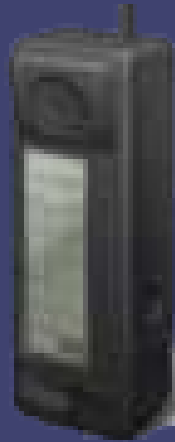
It repealed Directive 95/46/EC



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





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).



How will it affect organisations ?

- impact on all the areas of business not just Payroll
- personal data of employees is affected
- employers process a lot of personal data about employees for different reasons



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;



Your turn...

Give some examples of why an employer processes personal data.

60sec



Some examples...

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



Your turn...

Give some examples of personal data an employer processes.

60sec



Some examples...

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



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**
- data concerning **health**
- data concerning a natural person's sex life or sexual orientation



Special Categories of Data

[B] Criminal Convictions & Offences



Data Protection Act (Cap. 440)

The implications in the employment context

Identity Cards

Criminal History

Fines & Penalties

Damages - including Moral Damages



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



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



Exercise

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

- Mr J. Borg
- Advisory 21 Ltd.
- info@advisory21.com.mt
- +356 2100 0001
- Police conduct certificate
- High blood pressure

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



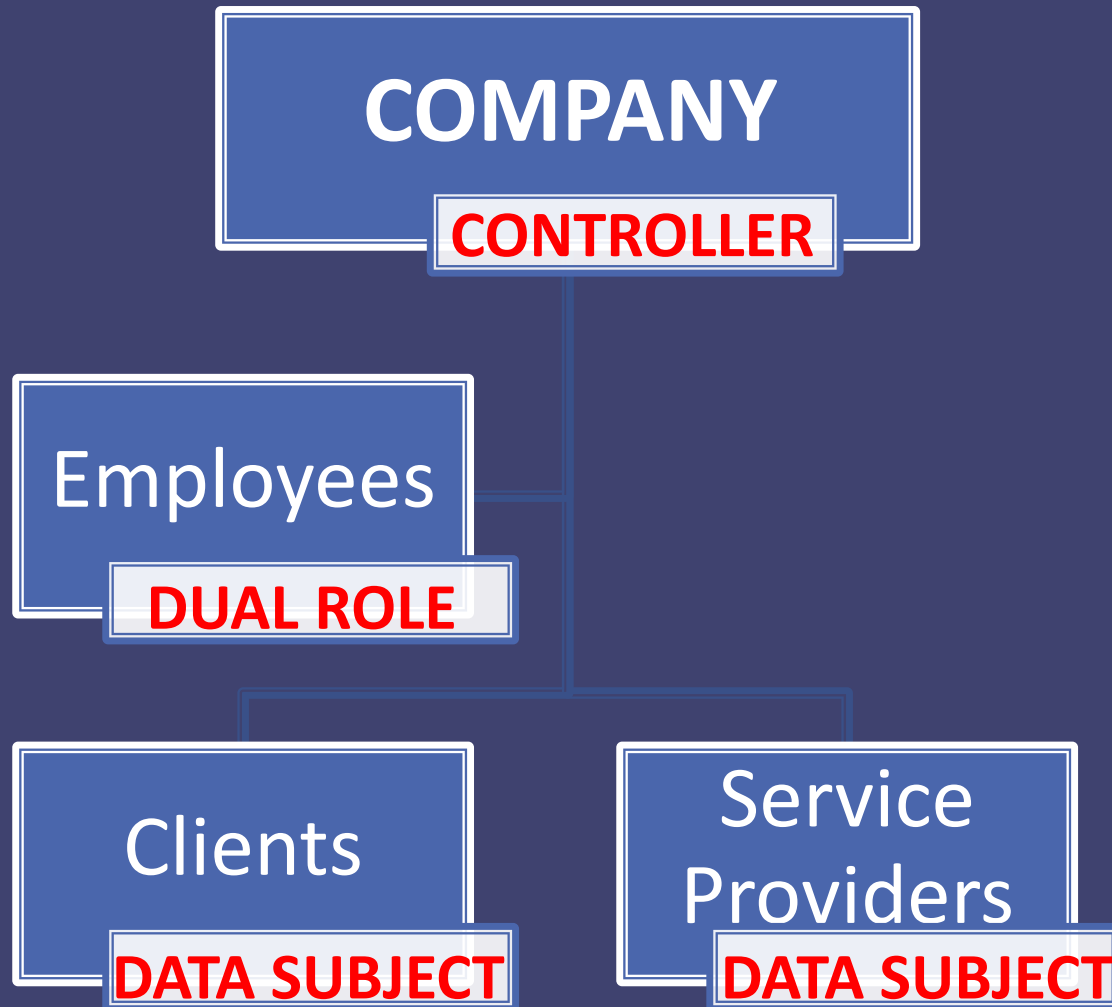
Controller & Processor

‘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)



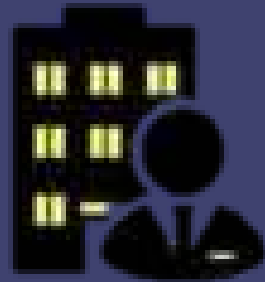
Controller & Processor



Controller & Processor



Employees
(DATA SUBJECTS)



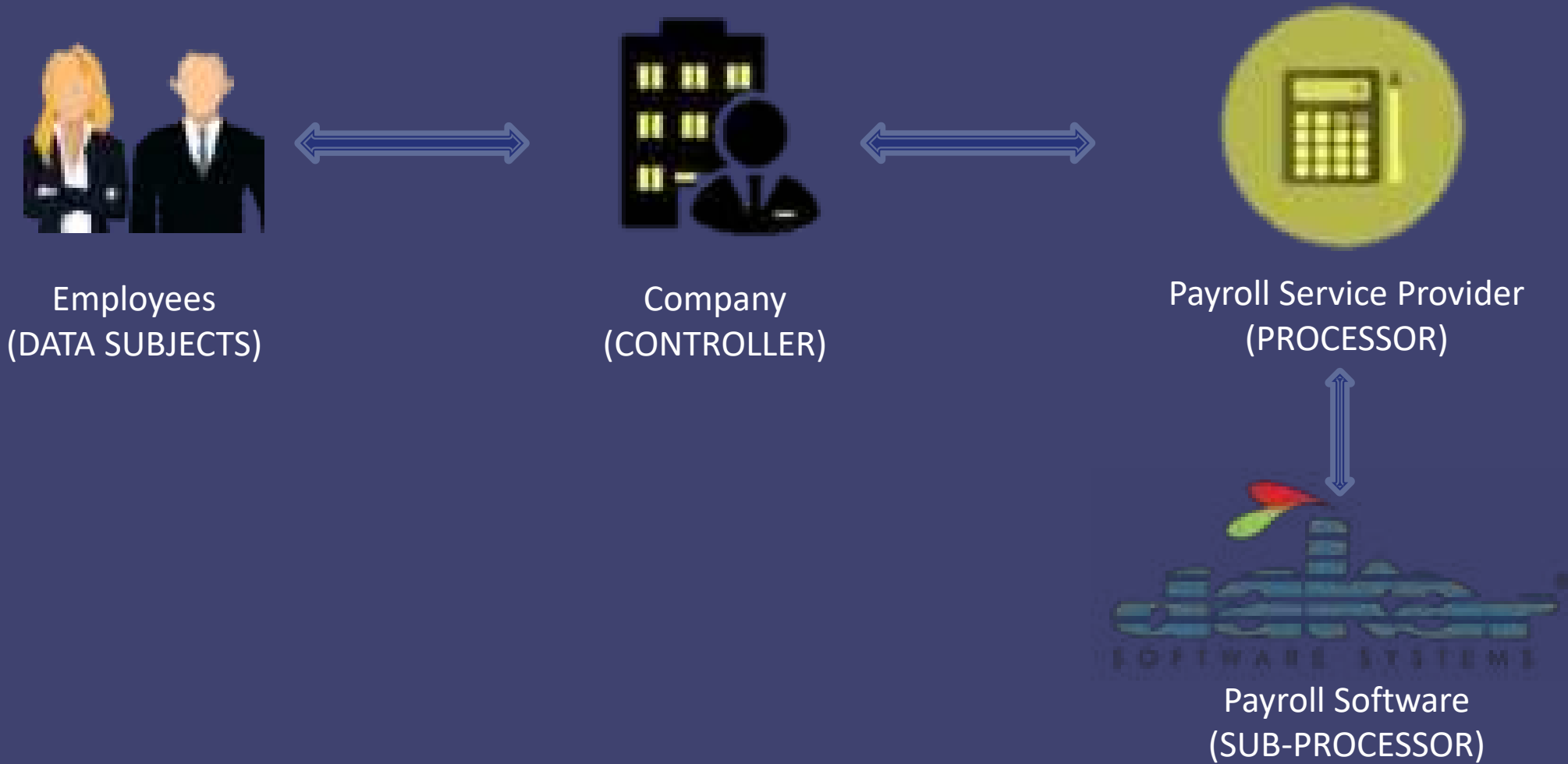
Company
(CONTROLLER)



Payroll Software
(PROCESSOR)



Controller & Processor



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.



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.



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



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



How to comply



Legal Grounds

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



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.



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.



Relying on consent

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



60sec



1 Right to information

2 Right of access

3 Right to rectify

7 Right to object



4 Right to be forgotten

5 Right to restrict

6 Automated processing

8 Data portability



Breaches of security

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

60sec



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.



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



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



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



GDPR & Payroll Implications

Angelito Sciberras
11 November 2024

