Working with and protecting data

Angelito Sciberras

November 2022

www.21Academy.education

The power & value of DATA

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

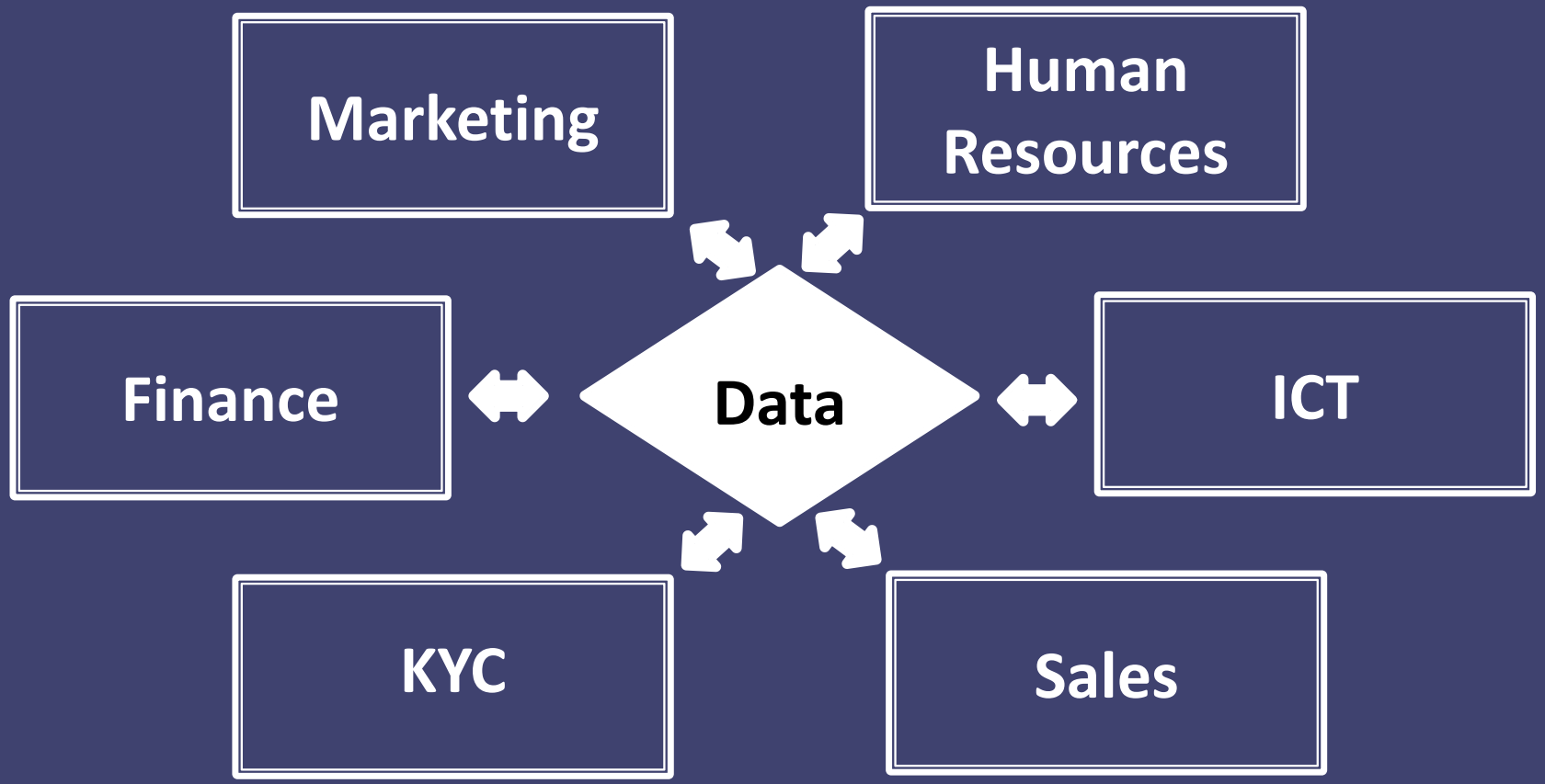
- The Economist, May 2017

Company/Office Data

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

60sec

Company/Office Data



www.21Academy.education

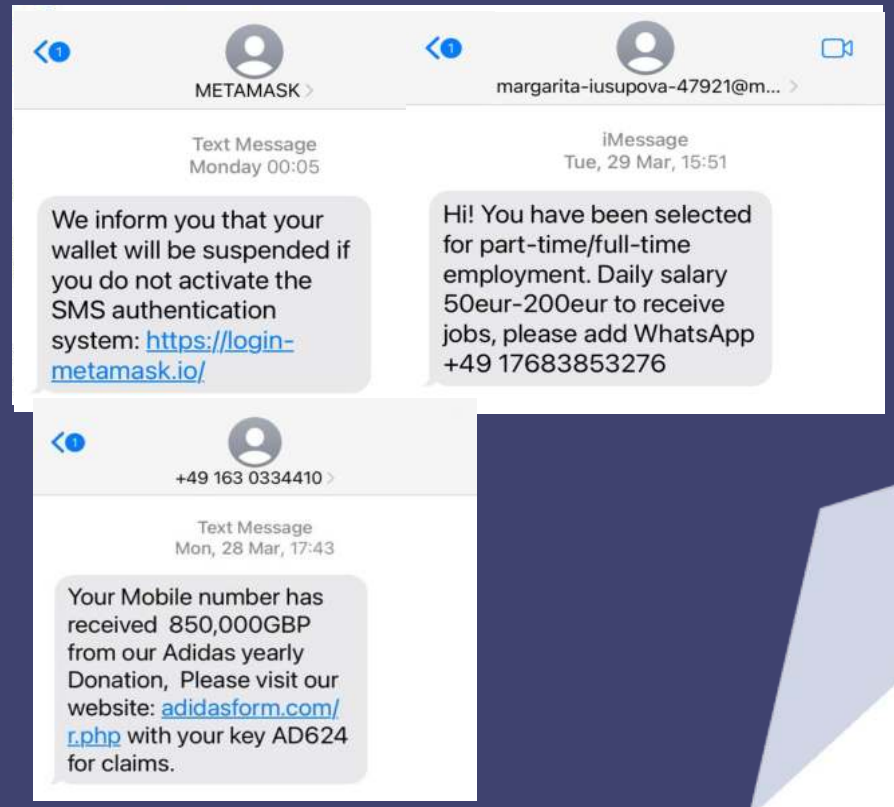
Value of Data

What value does company data have?

- Email addresses
- Mobile numbers

Copies of ID cards?

For what purpose?



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

BUY PASSPORT ONLINE
Real & Fake Documents

All Search Your Document

HOME SHOP DOCUMENTS CONTACT BLOG OUR WORK FAQ REVIEWS

HOME / SHOP / FAKE ID CARDS

Buy Fake ID Card of Malta

$350.00

Buy Malta counterfeit ID Card Online, European We are a real office to get a phony Malta ID card.

- 1 + ADD TO CART

Category: Fake ID Cards

Tags: Fake, ID Card, Malta

www.21Academy.education

Value of Data

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

Data

45sec

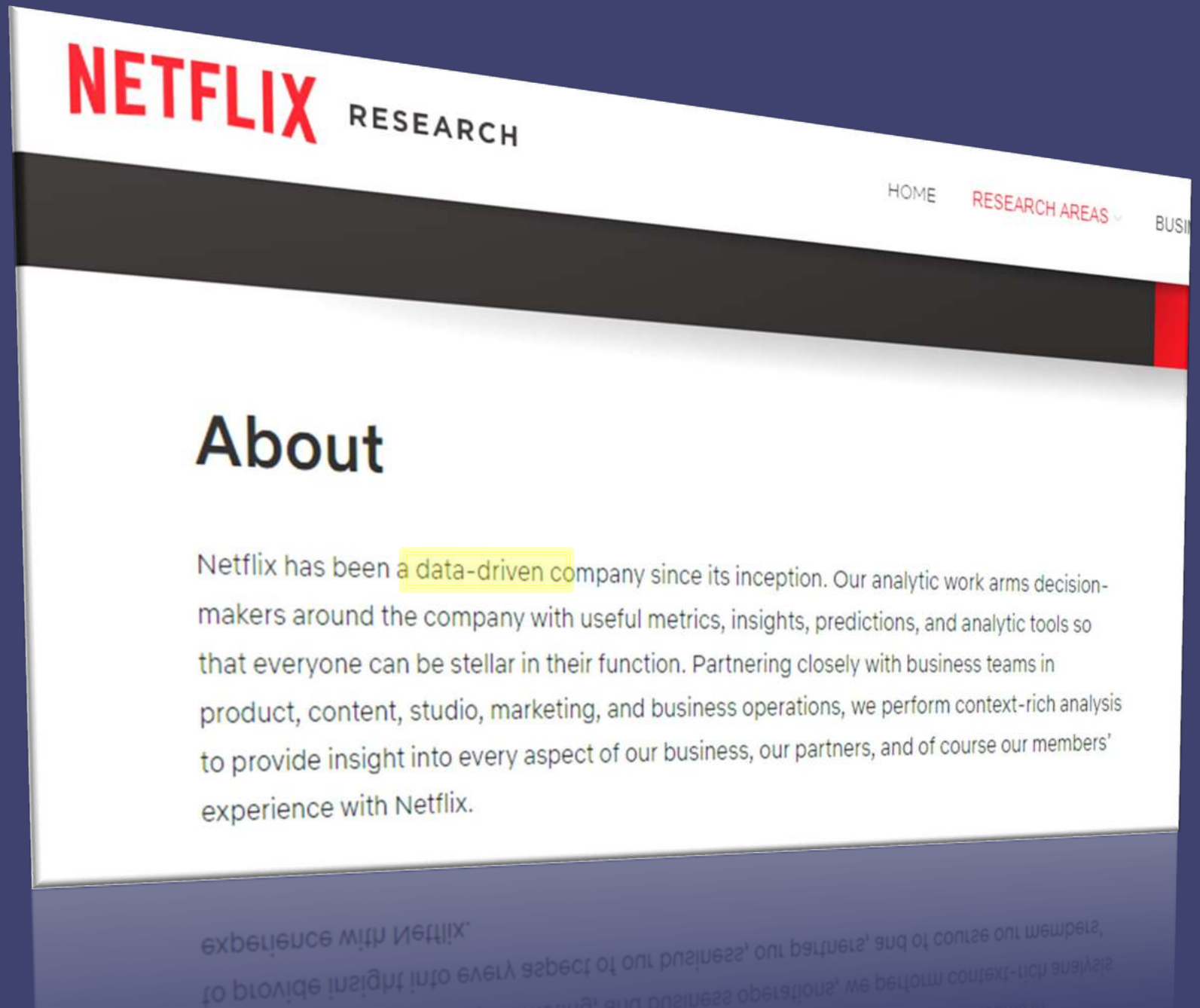
NETFLIX

You have been employed by Netflix...

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

How would you answer?

Data



www.21Academy.education

Personal Data

www.21Academy.education

Personal Data

Personal Data

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

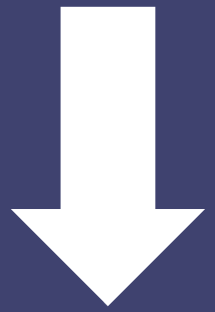
2. The app collected the data of those taking the quiz, but also recorded the public data of their friends

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

Personal Data

Directive 95/46/EC



GDPR

What changed at Office 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

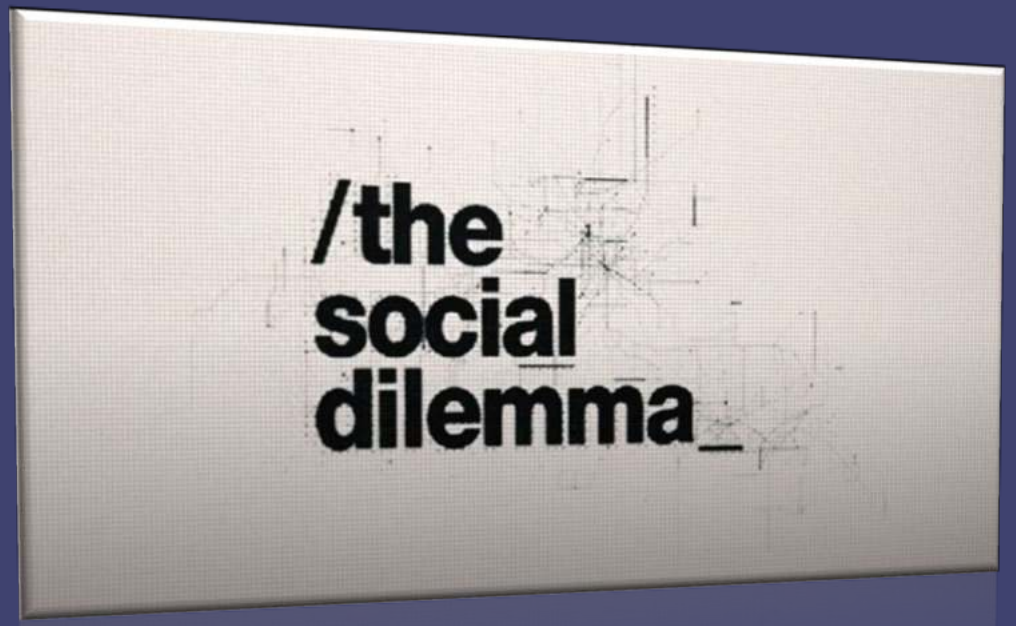
Sony Handycam DCR-VX1000

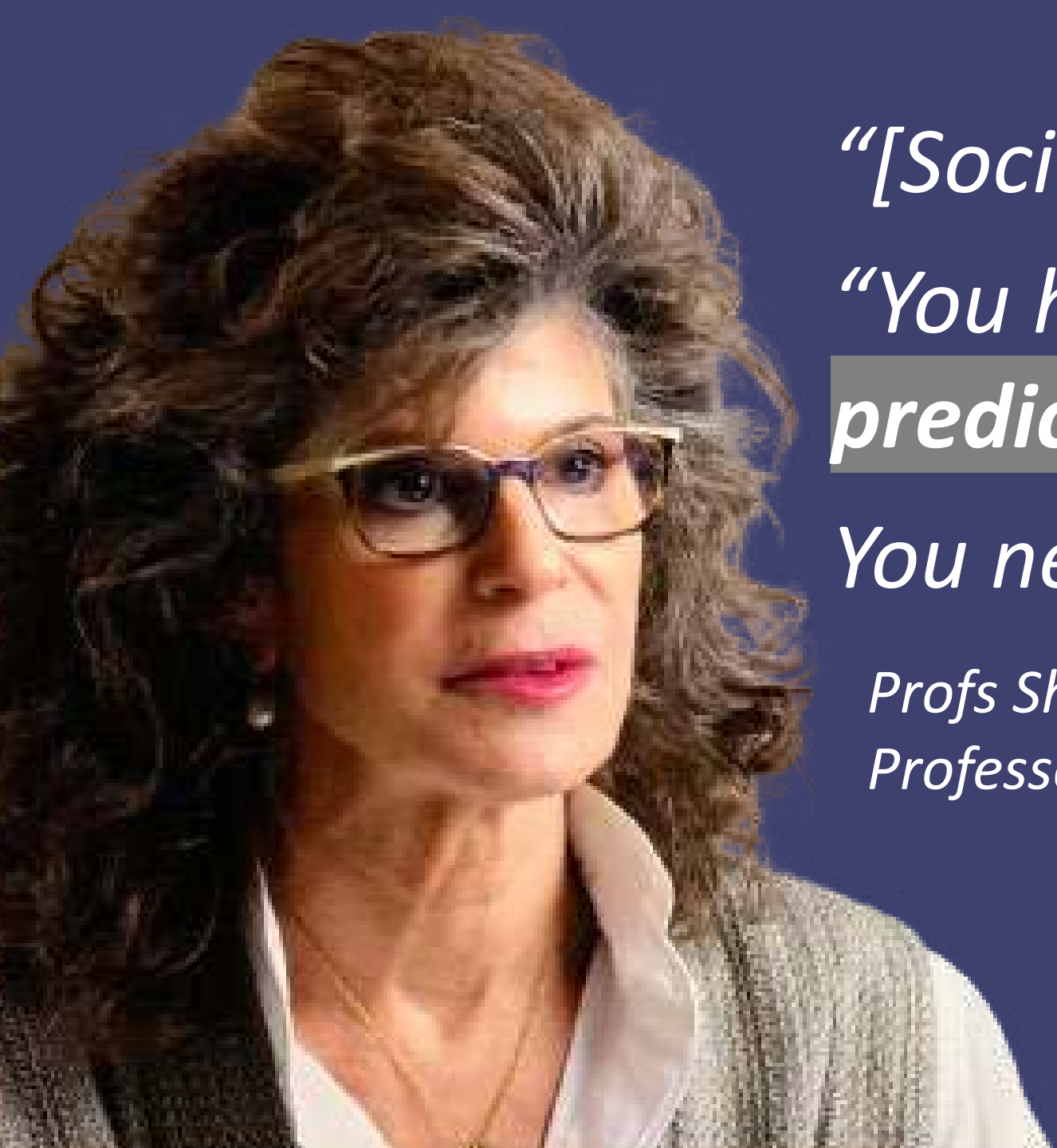
21 ACADEMY
www.21Academy.education

GDPR

www.21Academy.education

Personal Data





*"[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

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

Tristan Harris
Former Design Ethicist, Google

General Data Protection Regulation

"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

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

Why GDPR?

TIMES OF MALTA

News Sport Business Comment Life Entertainment Classifieds

National World Social & Personal Education Interview Environment Gozo Pictures

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 the internet

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

Friday, 21 February 2020, 11:42 Last update: about 12 days ago

H&M fined €35 million for illegally storing employees' personal data

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

Private information on some 337,000 Maltese voters was leaked online

National Elections Data Privacy

January 17, 2022 | Ivan Martin | 64

3 min read

Ombudsman website is probed over security risk

Attackers could view complaints submitted by citizens

National Daphne Caruana Galizia

February 21, 2020 | Jacob Borg | 44

HOME | GREEK NEWS | SOCIETY

Hellenic Data Protection Authority fines PWC for reported employee data breach

TornosNews.gr 30.07.2019 | 15:26

A facebook twitter google+ print

THISTLI CANTIK

21 ACADEMY

www.21Academy.education

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 ?

The law has an impact on all the areas of business.

Needless to say data of employees, clients, service providers, distributors etc., is affected.

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

www.21Academy.education

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;

www.21Academy.education

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

Your turn…

Give some examples of why an office processes personal data of its employees.

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?

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

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

www.21Academy.education

Processing of Special Categories

Only allowed to process in specific situations

1. **Explicit consent** from
2. Data made **public** by data subject - social media
3. **Rights and obligations**

Processing of Special Categories

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

5. Protect vital interests of data subject or another person - only applicable when data subject 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

- Ms A. Borg
- Advisory 21 Ltd.
- info@advisory21.com.mt
- +356 2099 5486
- Police conduct certificate
- High blood pressure

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

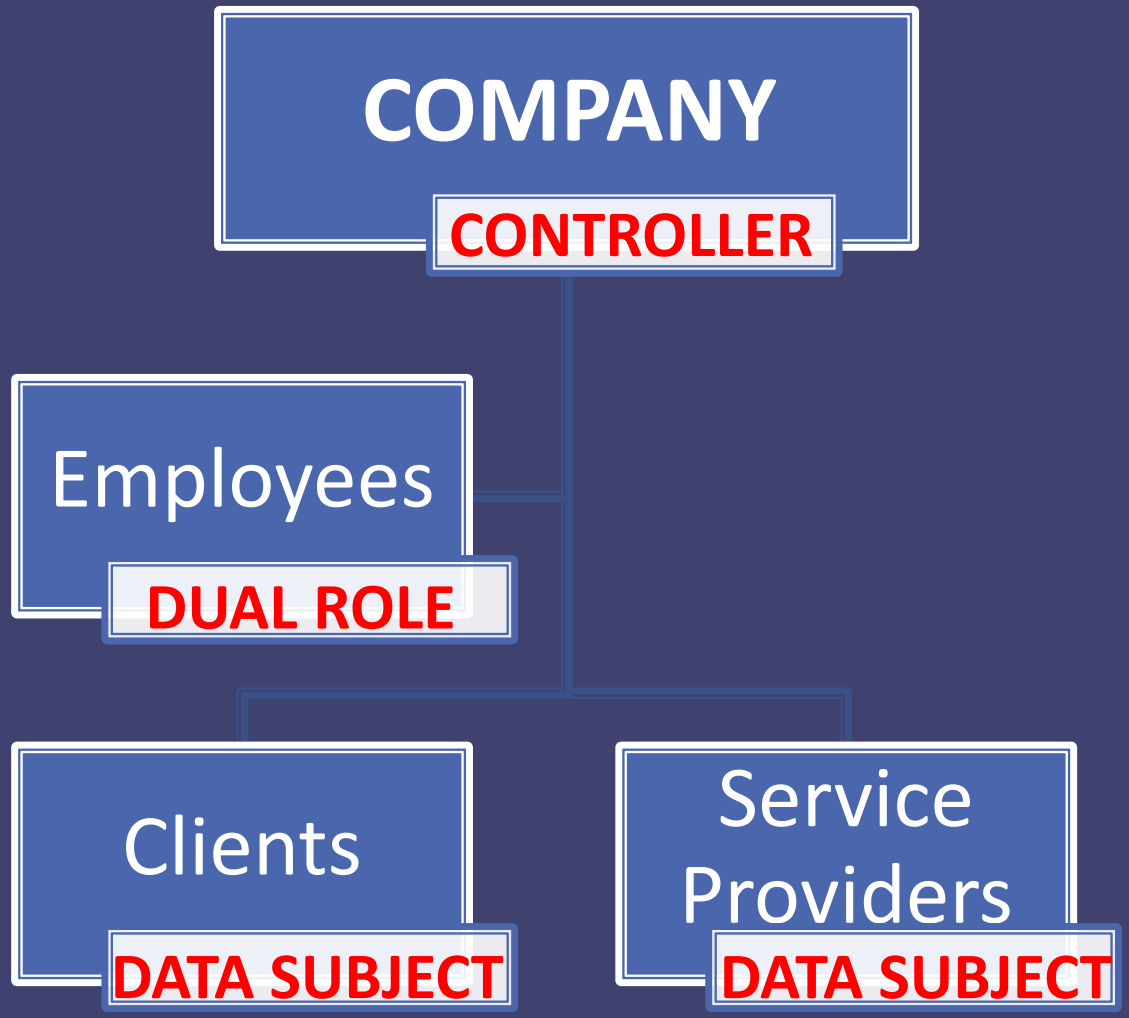
Controller & Processor

‘**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)

www.21Academy.education

Controller & Processor



www.21Academy.education

Controller & Processor

Employees
(DATA SUBJECTS)

Company
(CONTROLLER)

Payroll Software
(PROCESSOR)

Controller & Processor

Clients
(DATA SUBJECTS)

Company
(CONTROLLER)

Security Service Provider
(PROCESSOR)

Storage Provider
(SUB-PROCESSOR)

www.21Academy.education

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.

www.21Academy.education

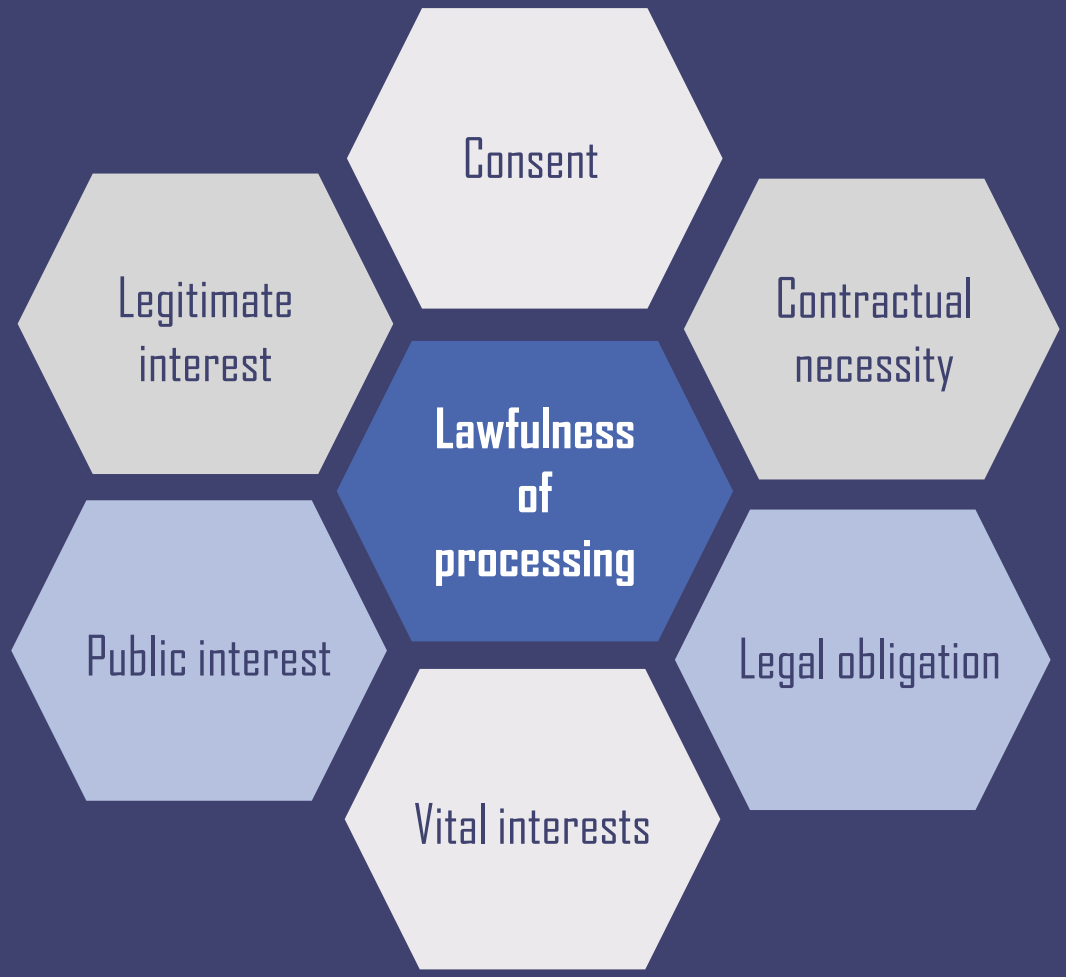
Principles

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

www.21Academy.education

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.

1 Right to information

2 Right of access

3 Right to rectify

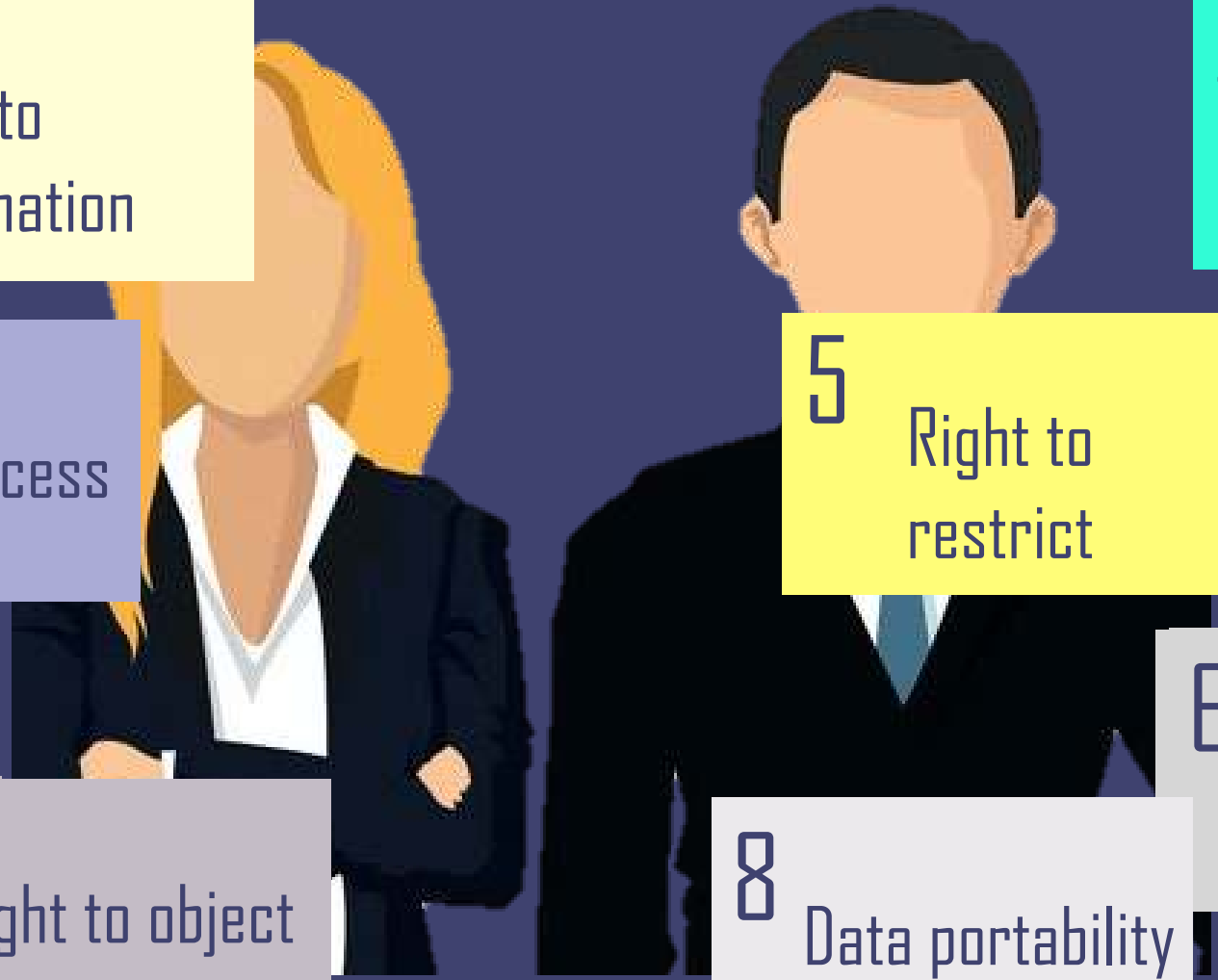
4 Right to be forgotten

5 Right to restrict

6 Automated processing

7 Right to object

8 Data portability



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

www.21Academy.education

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

Complying

How to comply

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

How to comply

Marketing

Human Resources

Finance

Personal Data

ICT

KYC

Sales

How to comply

- Privacy Standard (Data Protection Policy)
- GDPR Privacy notice for employees, and contractors
- Candidate Privacy Notice
- GDPR Privacy notice for Clients
- Website Privacy Notice
- Data Retention Policy and Guidelines
- Data Protection Impact Assessment (DPIA) Template
- Data Processing Agreement Template
- Data Breach Documents
- CCTV Policy
- Subject Access Request (SAR) Documents
- Bring Your Own Device Policy
- Image Consent Forms
- IT Systems Policies
  - IT and Communications System Policy
  - Disposal of IT Equipment Policy
  - Email Usage Policy

Working with and protecting data

Angelito Sciberras

November 2022

www.21Academy.education