5 years of GDPR and HR

what have we learned?

Angelito Sciberras

26 April 2023

5 years of GDPR

to give individuals more control over their personal data

5 years of GDPR

- Global implications vs Local Implications
- Cases worth understanding
- Frequently Asked Questions
- The HR Checklist
- The Headaches

5 years of GDPR

before we start…

5 years of GDPR

What were your impressions of GDPR throughout these five years?

5 years of GDPR

https://adssettings.google.com

5 years of GDPR

Why does Google want to know you?

60 sec

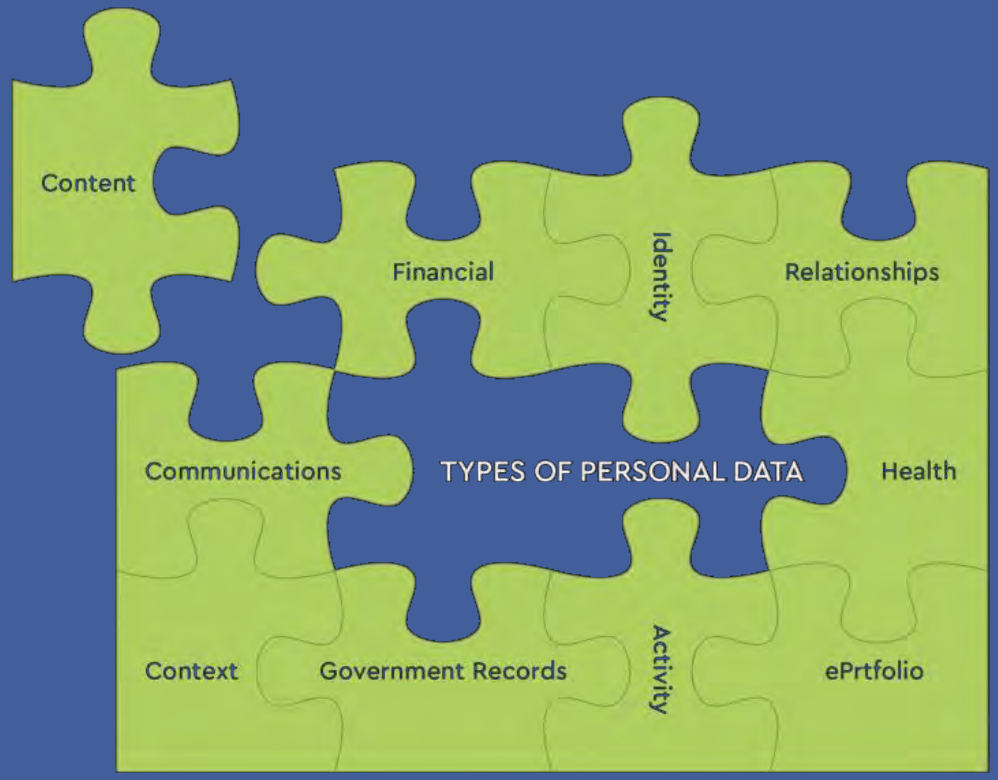
5 years of GDPR

Why do fraudsters want to know you or your employees?

60 sec

5 years of GDPR

Why do fraudsters want to know you or your employees?



5 years of GDPR

5 years of GDPR

TIMES OF MALTA

Latest | National | World | Opinion | Fact-check | X2 | Sport | Motoring | Business | Community

How BOV hackers got away with €13 million

Phishing e-mails did the job...

National

February 25, 2019 | Ivan Martin | 102

3 min read

5 years of GDPR

Impact

5 years of GDPR - Impact

"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

5 years of GDPR - Worldwide

1. Increased data protection
   - new data protection rights
   - Increased accountability

2. Global impact
   - businesses that process the personal data of EU citizens, regardless of where the company is based
   - development of similar laws in other countries - California Consumer Privacy Act (CCPA)
   - restrictions on transfer of data - adequacy decisions or standard contractual clauses

5 years of GDPR - Worldwide

3. Increased awareness and compliance

   - improved compliance with data protection regulations. However, many companies still struggle with implementation and ongoing compliance

4. Data breaches

   - increase in data breach reporting

5. Significant fines

   - €20 million or 4% of a company's global turnover

5 years of GDPR - Malta

1. Increased investment in IT infrastructure
2. Increased awareness (increased complaints)
3. Data breaches
4. Fines

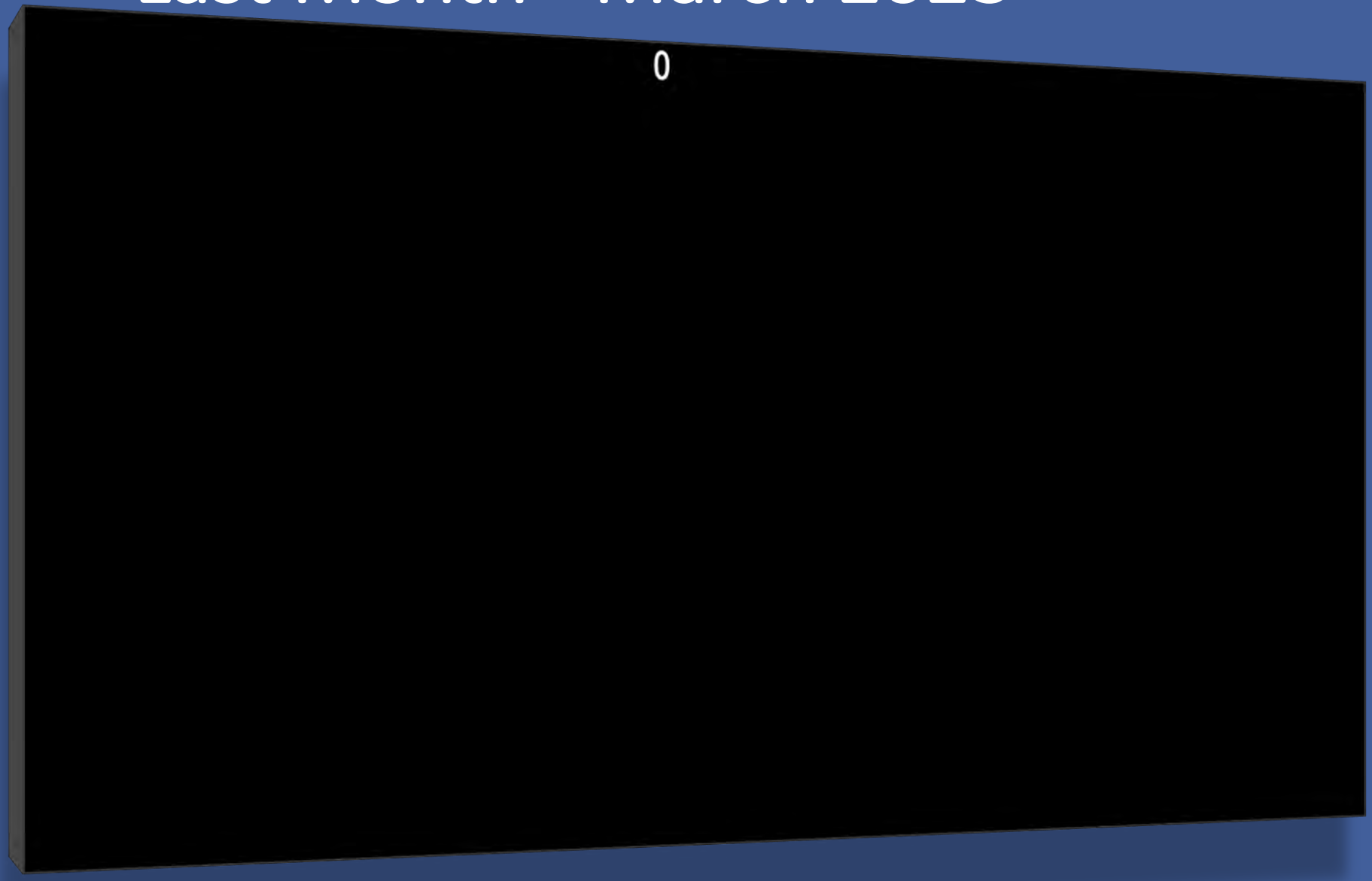
5 years of GDPR

Facts & Statistics

Last year - 2022

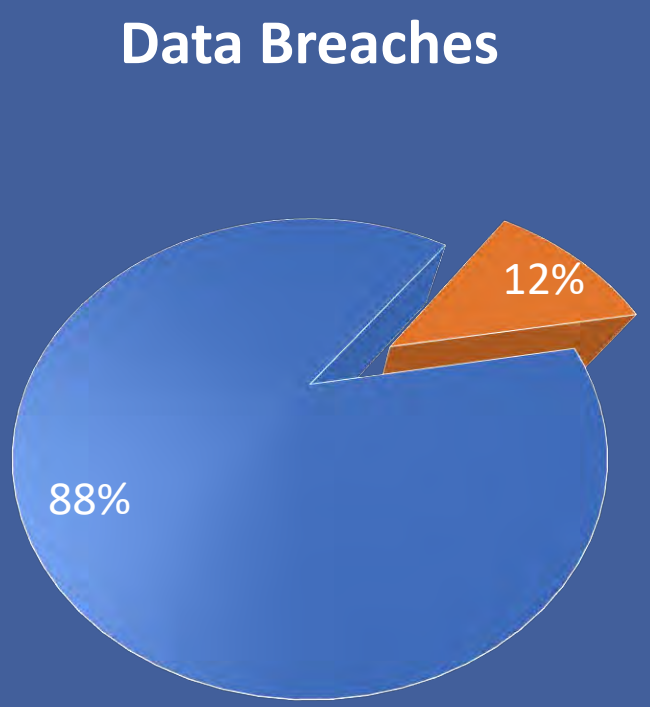
- The number of cyberattacks increased significantly
- Phishing attacks and ransomware being the most common types of attacks
- Stolen or compromised credentials were the leading cause of data breaches
- Healthcare and finance were the most targeted industries
- Remote work and the use of personal devices for work purposes contributed to the increase in cyberattacks.
- Small and medium-sized businesses were targeted more frequently

Last Month - March 2023



At a Glance

Distraction, stress and fatigue influence people's ability to consistently make good cybersecurity decisions

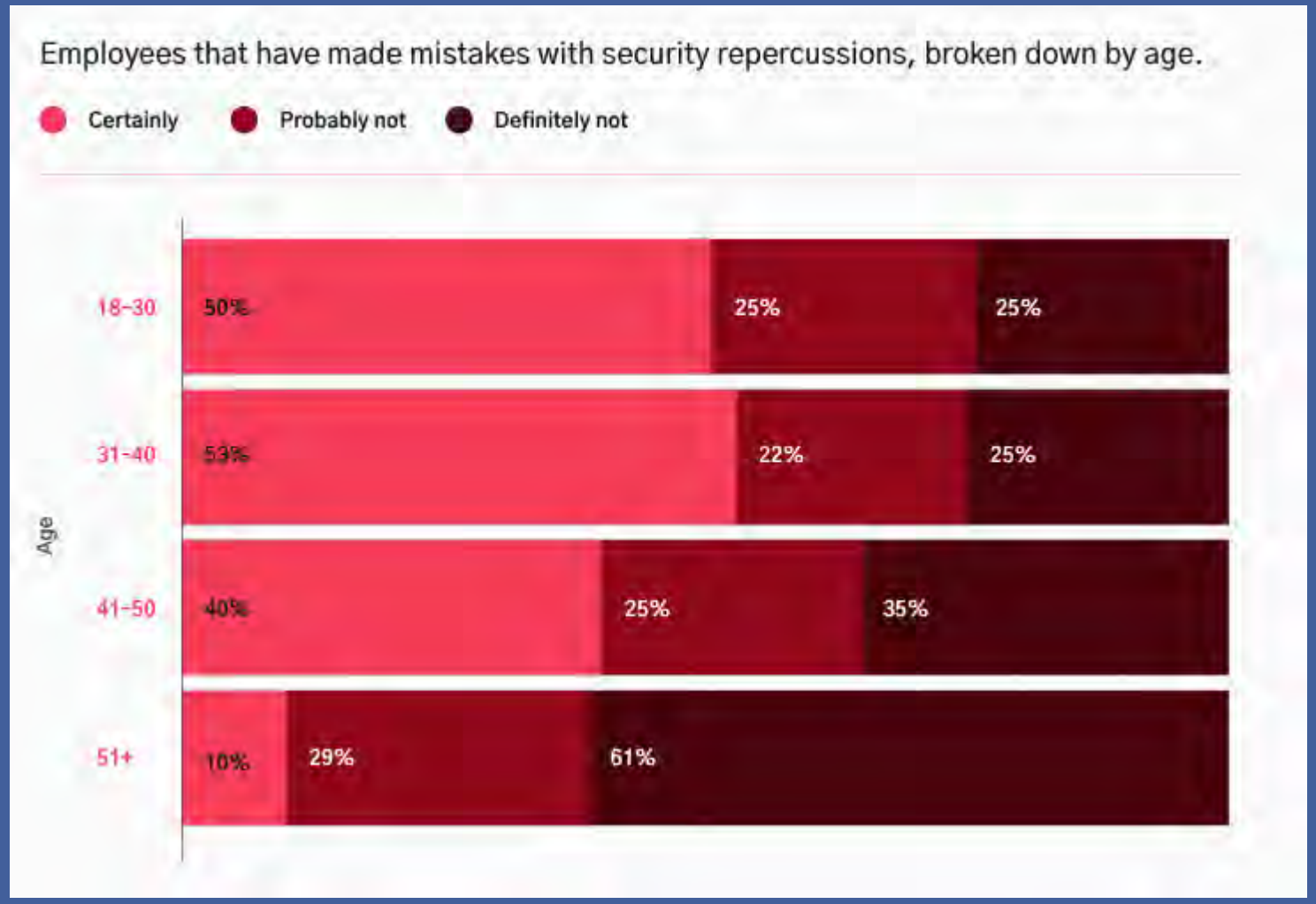


Hancock, J. (2022) *The Psychology of Human Error 2020*, *Tessian*. Stanford University. Available at: https://www.tessian.com/research/the-psychology-of-human-error/ (Accessed: April 23, 2023).

At a Glance

Hancock, J. (2022) *The Psychology of Human Error 2020*, *Tessian*. Stanford University. Available at: https://www.tessian.com/research/the-psychology-of-human-error/ (Accessed: April 23, 2023).

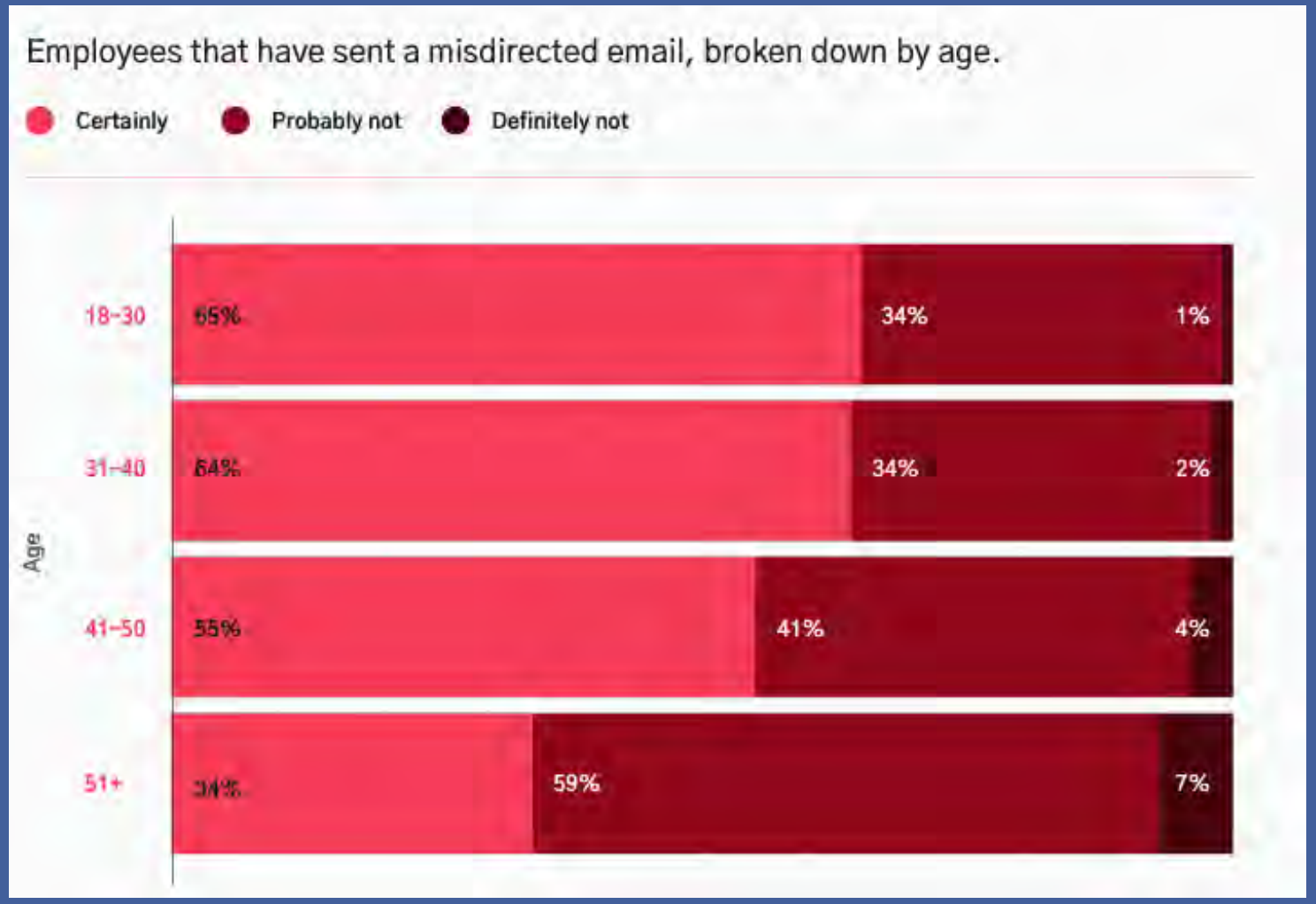
At a Glance - demographics matter?



- Younger workers are actually more aware that they have made a mistake and are more willing to admit their errors
- Older generatons more reluctant to admit they've made a mistake because they feel ashamed due to preconceived notions about older generations and technology and don't want to "lose face"

Hancock, J. (2022) *The Psychology of Human Error 2020, Tessian*. Stanford University. Available at: https://www.tessian.com/research/the-psychology-of-human-error/ (Accessed: April 23, 2023).

At a Glance - demographics matter?

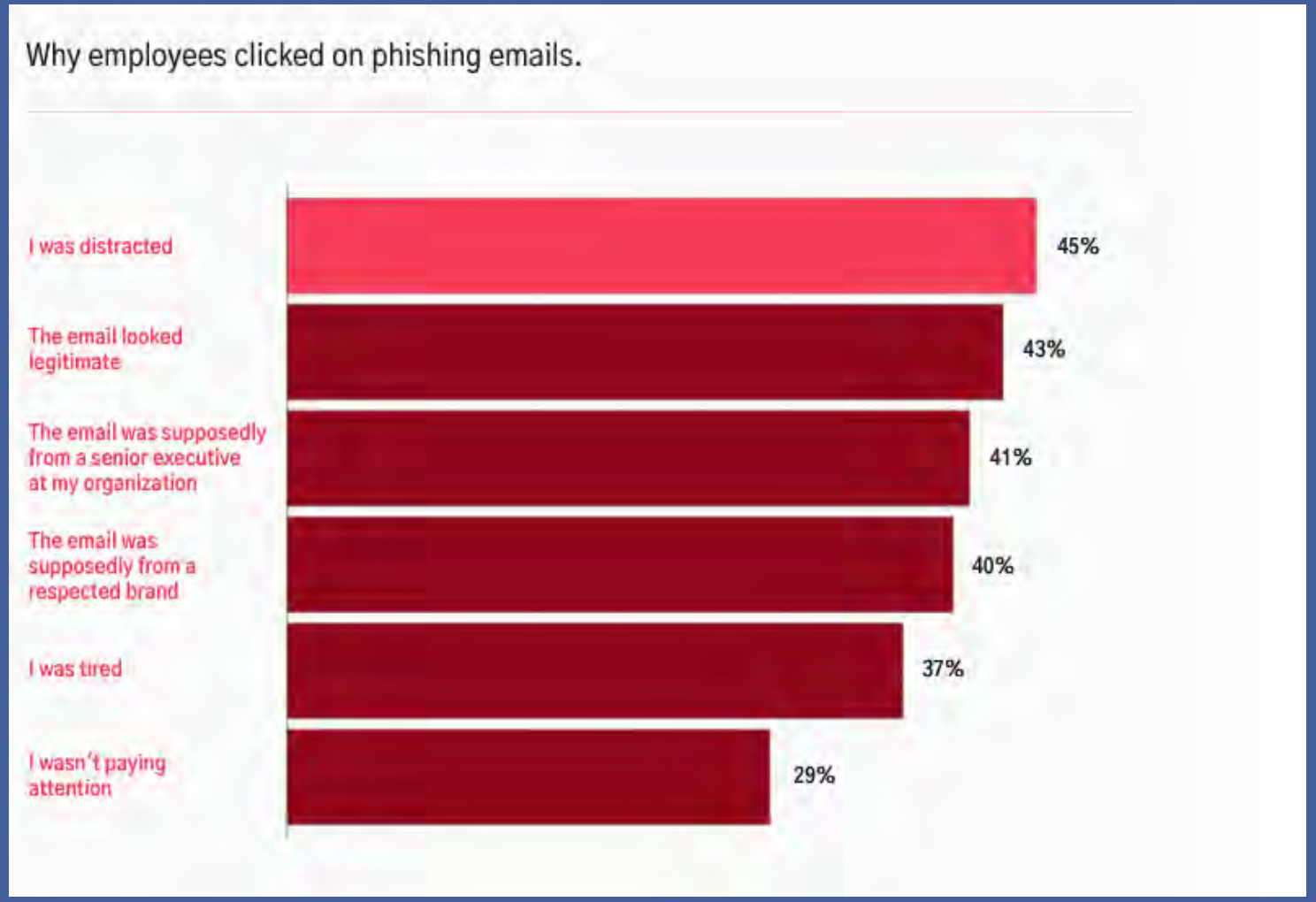


How can you promote reporting?

Limit exposure of reporting and action against who does especially if no company policies were breached

Hancock, J. (2022) *The Psychology of Human Error 2020, Tessian*. Stanford University. Available at: https://www.tessian.com/research/the-psychology-of-human-error/ (Accessed: April 23, 2023).

At a Glance



How can you avoid these incidents besides by having the necessary IT resources?

Hancock, J. (2022) *The Psychology of Human Error 2020*, *Tessian*. Stanford University. Available at: https://www.tessian.com/research/the-psychology-of-human-error/ (Accessed: April 23, 2023).

Act now

- Awareness sessions
- Continous training

5 years of GDPR

Global Cases

5 years of GDPR - what have we learned?

The questions you should continously be asking to yourself

- Do we need that personal data?
- What lawful basis do we have to process it?
- For how long are we going to keep it?
- Is it being transferred to other parties?
- Is it being protected enough?

5 years of GDPR - Highest Fines

What were the highest fines under GDPR so far?

60sec

5 years of GDPR - Highest 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

5 years of GDPR - Highest Fines

€405 million

€390 million

Forced Consent

€265 million

Data breach disclosing the personal data of 533 million users

- Ireland's Data Protection Commission
- processes personal data of teenagers between the ages of 13 and 17
- Instagram accounts automatically displayed the contact information (email addresses and/or phone numbers) of children publicly
- Meta failed to take measures to
  - provide child users with information using clear and plain language,
  - lacked appropriate technical and organizational measures, and
  - failed to conduct a Data Protection Impact Assessment.

5 years of GDPR - Highest Fines

€225 million

- Ireland's Data Protection Commission
- whether WhatsApp supplied enough information to users about how their data was processed and if its privacy policies were clear enough.

- What's more of interest
  - Original proposed fine was €30 to €50 million
  - Objections from 8 countries

5 years of GDPR - Highest Fines - Employment Related

€35.3 million

- Hamburg Data Protection Authority
- The company recorded and stored gigabytes of recorded one-on-one conversations with employees - back to work interviews
- Personal Data included vacation experiences, symptoms of illness, diagnosis, family issues and religious beliefs
- Details provided in those conversations were used in decisions regarding the employees

5 years of GDPR - Highest Fines - Employment Related

€10.4 million

notebooksbilliger.de

- State Commissioner for Data Protection in Lower Saxony
- The company had been using video surveillance to monitor its employees for at least two years with no legal justification
- Some of the areas recorded by the illegal cameras included workspaces, sales floors, warehouses and staff rooms
- Many of the recordings were saved for 60 days,

5 years of GDPR - Highest Fines - Employment Related

€5 million

- UK Information Commissioner Office (ICO)
- Cyber attack in 2020
- Personal data of up to 113,000 employees was encrypted and rendered ‘unavailable’
- An Interserve employee who was working from home forwarded a phishing email to another employee, who opened it and downloaded the contents
- The ICO found that Interserve:
  - failed to follow-up on the original alert of a suspicious activity;
  - used outdated software systems and protocols; and
  - had a lack of adequate staff training and insufficient risk assessments.

5 years of GDPR

Malta

5 years of GDPR - Malta

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

60sec

5 years of GDPR - Highest 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

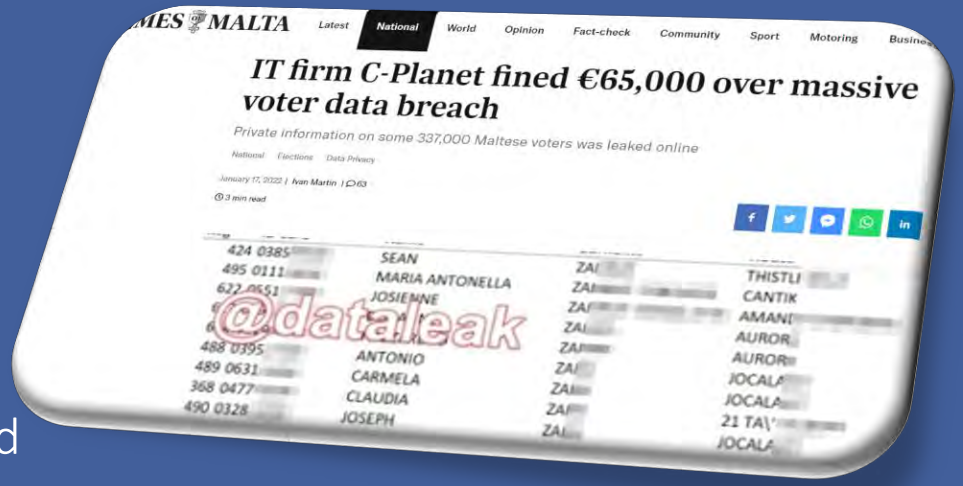
Article 32 - Security of Processing

Emphasises the importance of protecting personal data and requires organisations to take appropriate measures to safeguard it.

Technical & Organisational measures - examples

5 years of GDPR - Highest Fines Malta

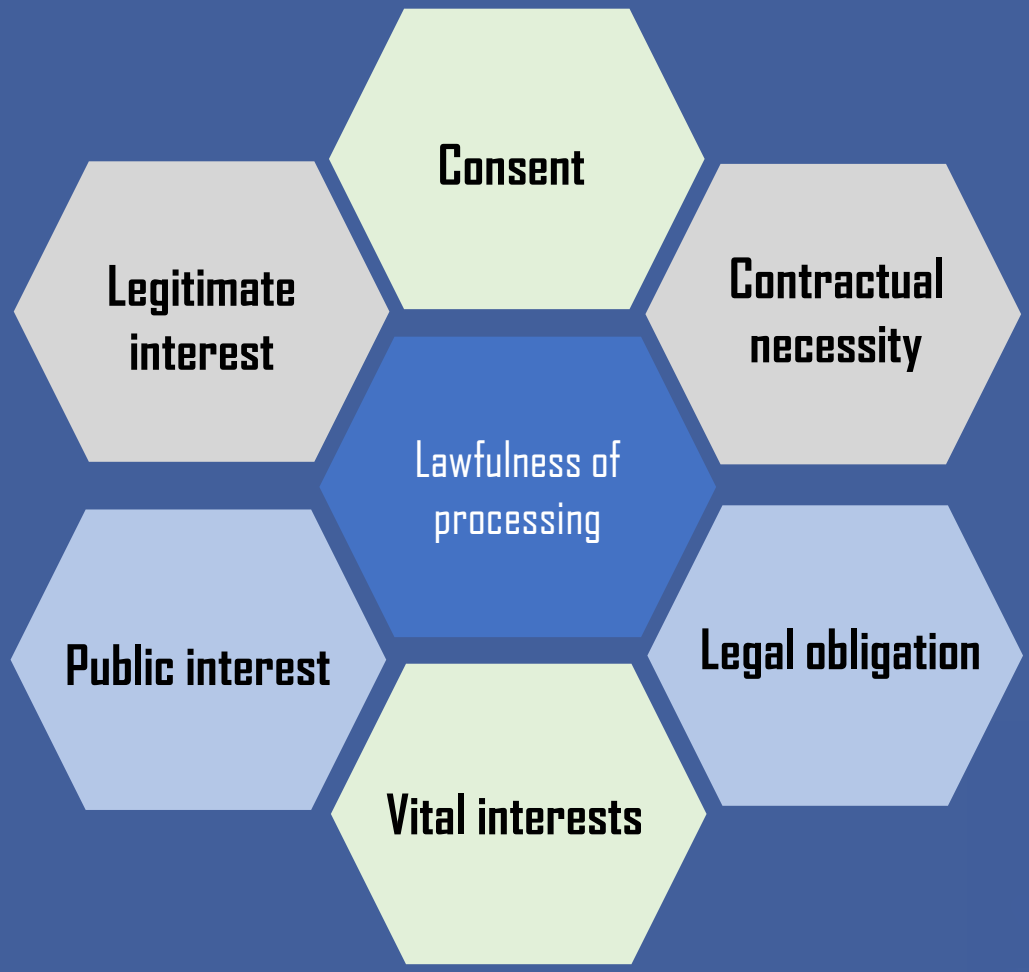
€65,000



- 2022
- Information and Data Protection Commissioner
- Controller infringed principles of security regarding personal and special categories of data of many data subjects
- Infringements of Articles 6(1), 9(1), 9(2), 14, 32(1), 5(1)(f), 33(1) and 34(1) GDPR

Article 6 - Lawfulness of processing

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



Article 9 - Processing of special categories of personal 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

Article 14 - Information to be provided where personal data have not been obtained from the data subject

Over and above the normal information given to data subjects:

- the categories of personal data concerned
- from which source the personal data originate, and if applicable, whether it came from publicly accessible sources

Article 5 - Principles

f. 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 (‘integrity and confidentiality’)

Article 33 - Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Article 34 - Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

5 years of GDPR - Highest Fines Malta

€20,000

- 2020
- Information and Data Protection Commissioner
- Personal data undergoing processing was partially provided following a right of access request. Privacy Policy not satisfying the transparency requirements
- Infringement of Articles 13 and 15 GDPR

Article 13(1) - Information to be provided where personal data are collected from the data subject

a. the identity and the contact details of the controller and, where applicable, of the controller's representative;

b. the contact details of the data protection officer, where applicable;

c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d. where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

e. the recipients or categories of recipients of the personal data, if any;

f. where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Article 13(2) - Information to be provided where personal data are collected from the data subject

a. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

c. where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

d. the right to lodge a complaint with a supervisory authority;

e. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

f. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Article 13(3) - Information to be provided where personal data are collected from the data subject

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

Article 15 (1) - Right of access by the data subject

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

a) the purposes of the processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

f) the right to lodge a complaint with a supervisory authority;

g) where the personal data are not collected from the data subject, any available information as to their source;

h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Complaints received by IDPC

IDPC Decisions

	Monitoring	SAR	Others
2023	1	3	1
2022	4	1	13
2021	9	8	24
2020	9	5	14
	26%	17%	57%

5 years of GDPR - Other Fines Malta

Reprimand

- 2020
- Information and Data Protection Commissioner
- Unauthorized use of personal data leading to employment disciplinary proceedings
- Infringement of Articles 5.1(c) and 6.1 GDPR

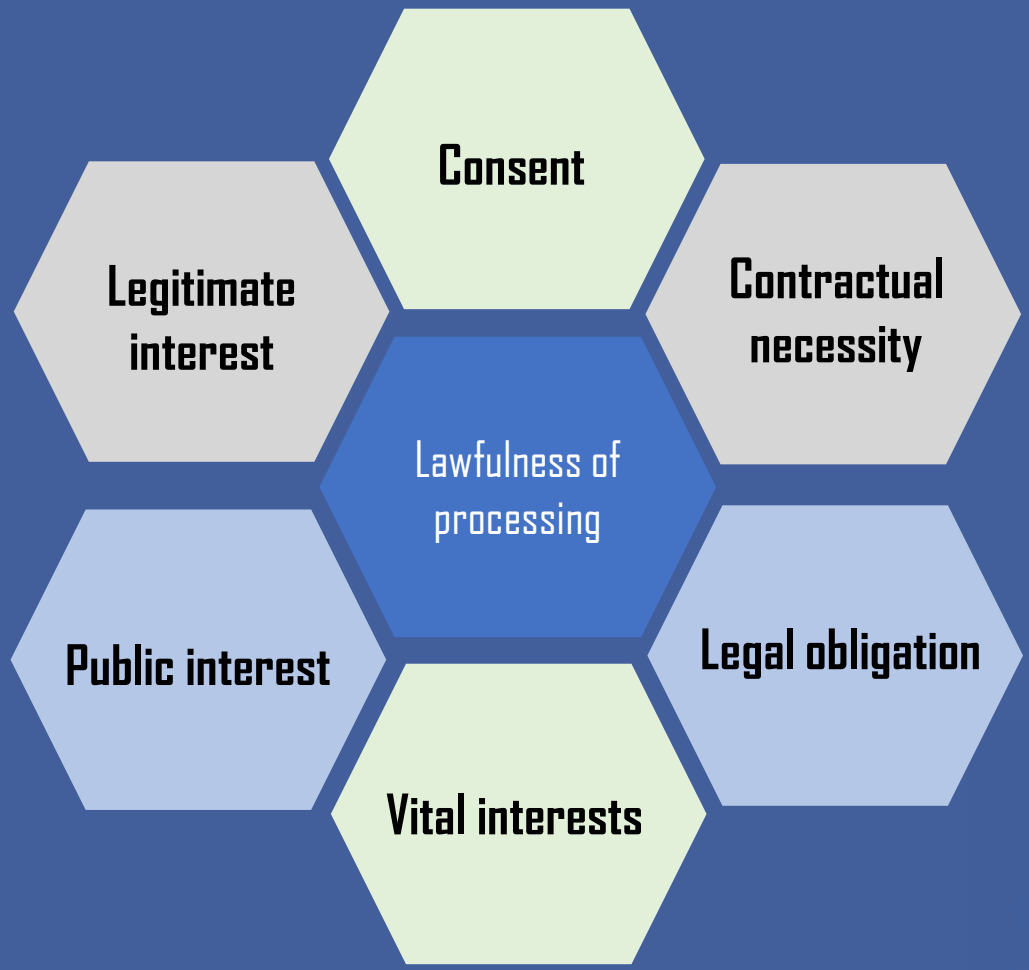
Article 5(1) - Principles

Personal data shall be:

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

Article 6(1) - Lawfulness of processing

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



5 years of GDPR - Other Fines Malta

€2,500

- 2022
- Information and Data Protection Commissioner
- Accidental loss of personal data when a box of documents which contained employment filled-in forms went missing
- Infringement of Article 32(1)(b)

Article 32 - Security of Processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

    (a) the pseudonymisation and encryption of personal data;

    (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

5 years of GDPR - Other Fines Malta

€2,500

- 2022
- Information and Data Protection Commissioner
- Controller has unlawfully disclosed the complainant's personal data
- Infringements of Articles 24(2), 32(1)(b) and 32(4) GDPR

Article 24 - Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.

2. Those measures shall be reviewed and updated where necessary. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

Article 32 - Security of Processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

    (a) the pseudonymisation and encryption of personal data;

    (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

Article 32 - Security of Processing

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

5 years of GDPR

FAQs

5 years of GDPR - FAQS

Can we keep a copy of the employees' identity cards/passports?

5 years of GDPR - FAQS

Can we keep a copy of the employees' identity cards/passports?

Cap. 586 Art. 8

An identity document shall only be processed when such processing is clearly justified having regard to the purpose of the processing and

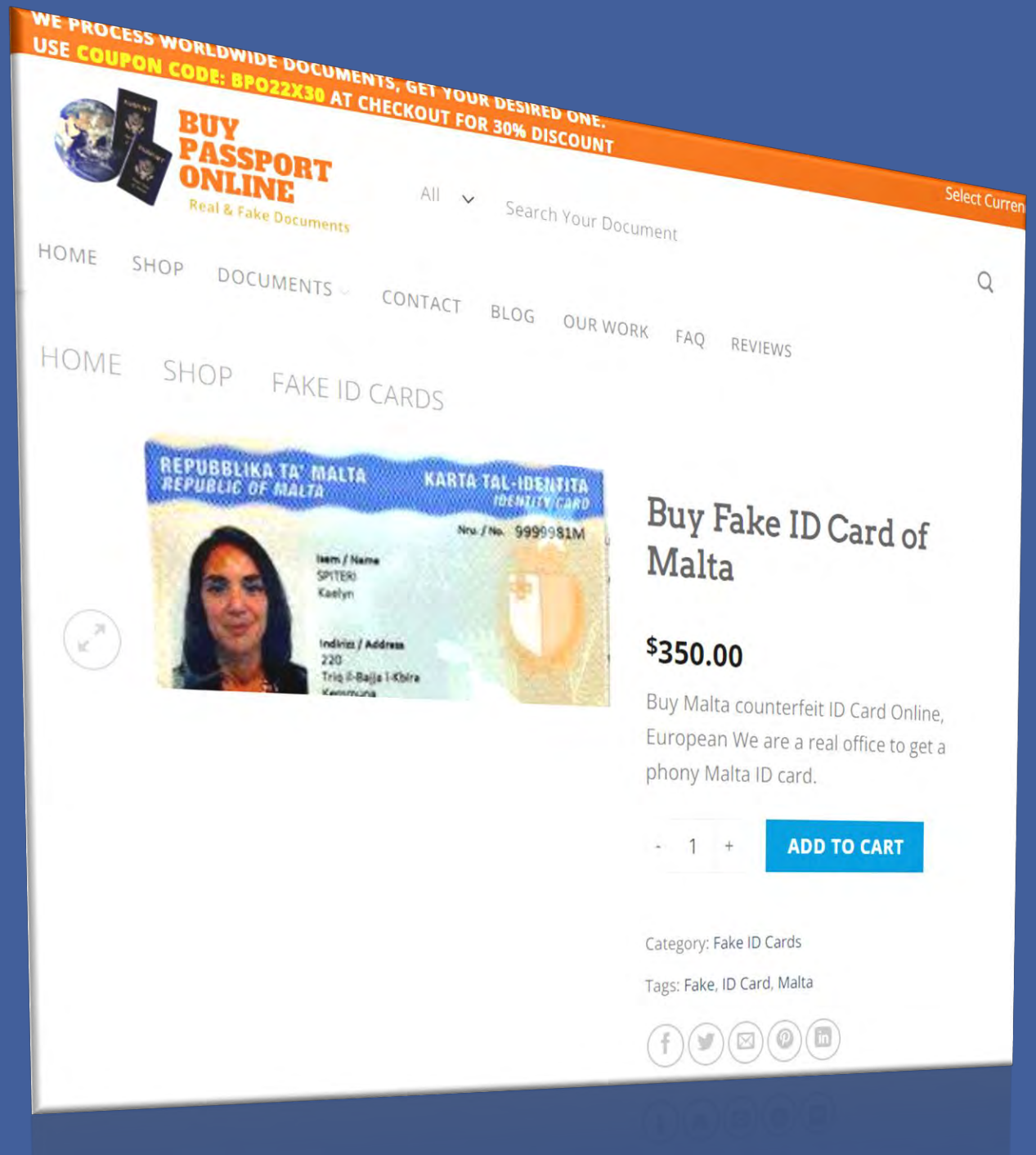
(a) the importance of a secure identification; or

(b) any other valid reason as may be provided by law:

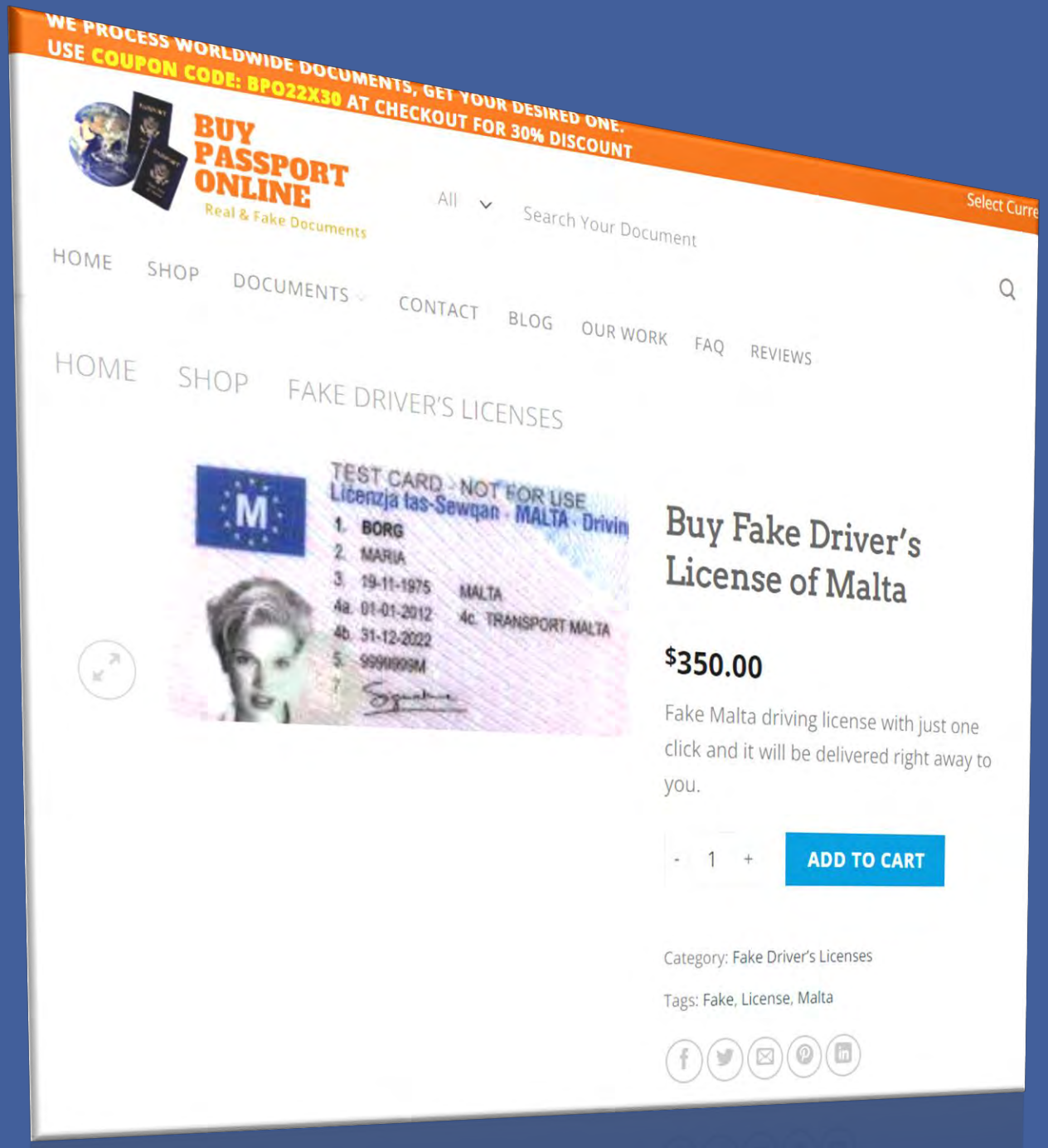
Provided that the national identity number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to the Regulation.

5 years of GDPR - FAQS

What are the risks associated with keeping copies of the employees identity documents?



https://buypassportsonline.com



https://buypassportsonline.com

5 years of GDPR - FAQS

Can we keep a copy of the employees’ police conduct certificate

5 years of GDPR - FAQS

Can we keep a copy of the employees' police conduct certificate

GDPR Art. 10

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) [lawfullness] shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

5 years of GDPR - FAQS

For how long can we keep CVs of unsuccessful job applicants?

5 years of GDPR - FAQS

For how long can we keep CVs of unsuccessful job applicants?

5 years of GDPR - FAQS

For how long can we keep CVs of unsuccessful job applicants?

EIRA Art. 47(1)

Proceedings for an offence under this Act or of any regulations or orders made thereunder may be commenced at anytime within one year from the commission of the offence.

5 years of GDPR - FAQS

For how long can we keep employees’ data post termination?

5 years of GDPR - FAQS

We rely on the followig clause in the employment contract to process the employees' personal data:

"The employee also agrees and consents that any of the details already supplied to the employer, together with any personal and sensitive data in terms of the Data Protection Act which may be supplied subsequent to the commencement of employment is processed for the purpose of assessment, monitoring, analysis and all other matters in relation to employment."

5 years of GDPR - FAQS

Consent must be:

Freely given
Informed
Specific
Unambiguous

If one of the special categories must be explicitly given.

- 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.

5 years of GDPR - FAQS

For how long can we keep employees' personal data post termination?

GDPR Art. 5(1)(e)

Personal data shall be:

kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')

5 years of GDPR - FAQS

For how long can we keep employees' personal data post termination?

Know your data

- Purpose
- Lawfullness of processing

5 years of GDPR - FAQS

We have X of employees. Do we need to have a Data Protection Officer?

5 years of GDPR - FAQS

We have X of employees. Is it mandatory to have a Data Protection Officer?

- where the processing is carried out by a public authority or body;
- where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or
- where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

5 years of GDPR - FAQS

Is it obligatory to have a data inventory of the employees' personal data?

5 years of GDPR - FAQS

Is it obligatory to have a data inventory of the employees' personal data?

GDPR Article 30(1) Records of processing activities

Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

b) the purposes of the processing;

c) a description of the categories of data subjects and of the categories of personal data;

d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

f) where possible, the envisaged time limits for erasure of the different categories of data;

g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

5 years of GDPR - FAQS

Is it obligatory to have a data inventory of the employees' personal data?

GDPR Article 30(5) Records of processing activities

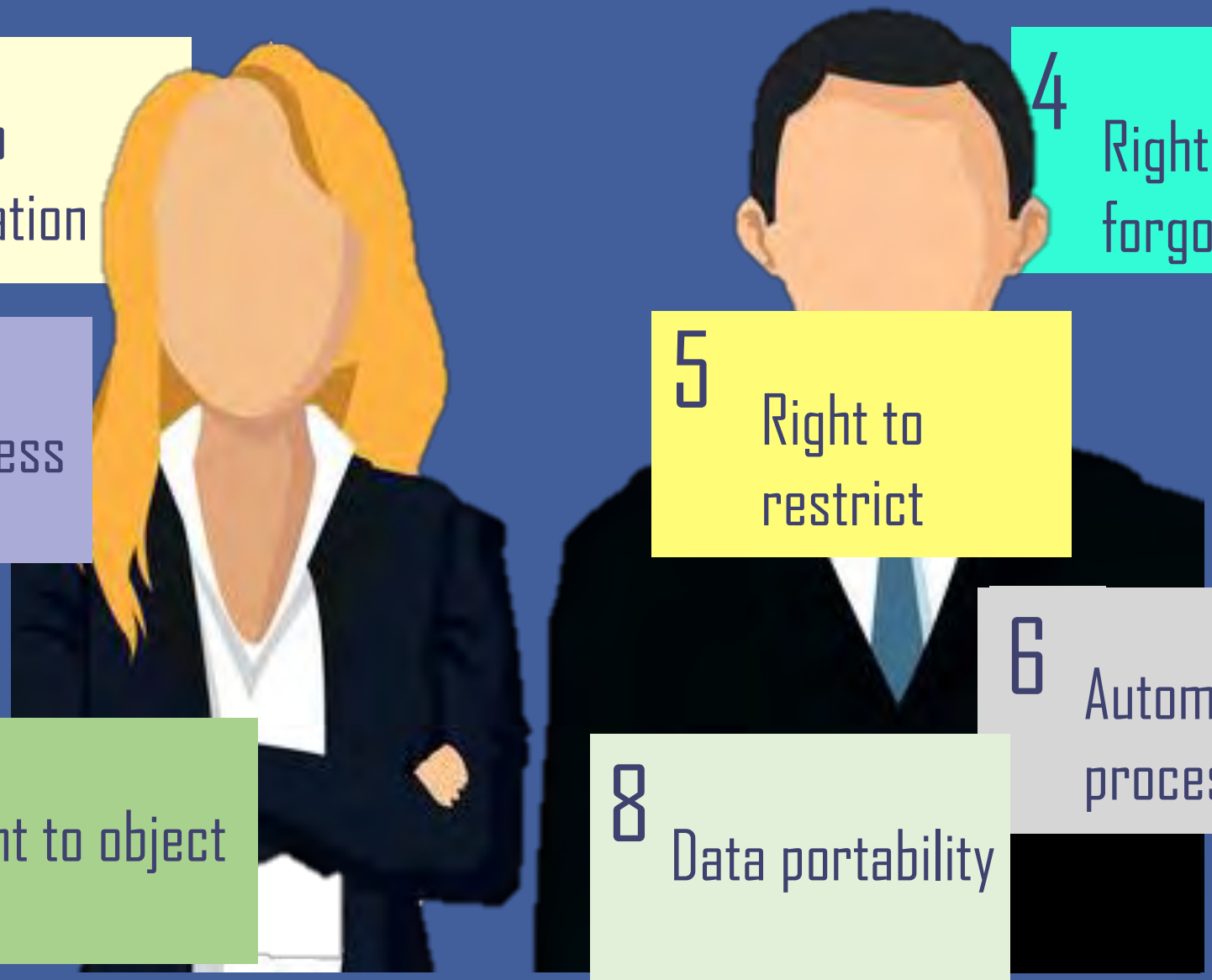
The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

5 years of GDPR - FAQS

Is it obligatory to have a data inventory of the employees' personal data?

You cannot fulfill any of the data subjects' rights unless you have a record of your processing activities

5 years of 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

5 years of GDPR - FAQS

What Policies and Procedures are mandatory from an HR perspective?

5 years of GDPR - FAQS

What Policies and Procedures are mandatory from an HR perspective?

Obligatory Policies/Notices

- Privacy Standard
- Privacy Notice to Data Subjects - candidates, employees
- Monitoring

Recommended Procedures

- Subject Access Request
- Data Breach

5 years of GDPR - FAQS

What Policies and Procedures are mandatory from an HR perspective?

Recommended Policies/Notices

- Retention
- Information Security
- Email use
- BYOD
- Social Media

5 years of GDPR - FAQS

What Policies and Procedures are mandatory from an HR perspective?

DO NOT FORGET

If you have engagged processors you need to have a Data Processing Agreement in place

5 years of GDPR

HR Checklist

5 years of GDPR - HR 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

5 years of GDPR

The Headaches

5 years of GDPR - The Headaches

- Human Resources Department as the Controller
- Copies of ID cards and Police Conduct certificates with employment contracts
- Old employment contracts not reviewed
- Subject Access Requests
- Avoidable data breaches
- CCTV signage not adequate
- Data Protection Impact Assessments
- Identification of data processors
- Lack of phishing awareness

5 years of GDPR and HR

what have we learned?

Angelito Sciberras

26 April 2023