Information Technology & Data related policies, information & procedures

Angelito Sciberras

June 2022

Policies
Notices
Procedures

- **Obligatory**
  - Privacy Standard
  - Privacy Notice to Employees
  - Monitoring
- **Other**
  - BYOD
  - Social Media
  - SAR
  - Secure IT Use
  - Email use

Privacy Standard

- A privacy standard is an ‘inward-looking’ document, recently replacing what was previously known as a “privacy policy”.
- Policies act as a statement of intent, while standards function as rules to achieve that intent. Policies reflect an organisation's goals, objectives and culture and are intended for broad audiences.
- Today, this has become an essential document which regulates an organisation’s handling of personal data (whether obtaining, controlling, processing, transport, or storage) and also informs employees of their duties under data protection legislation.

Privacy Standard

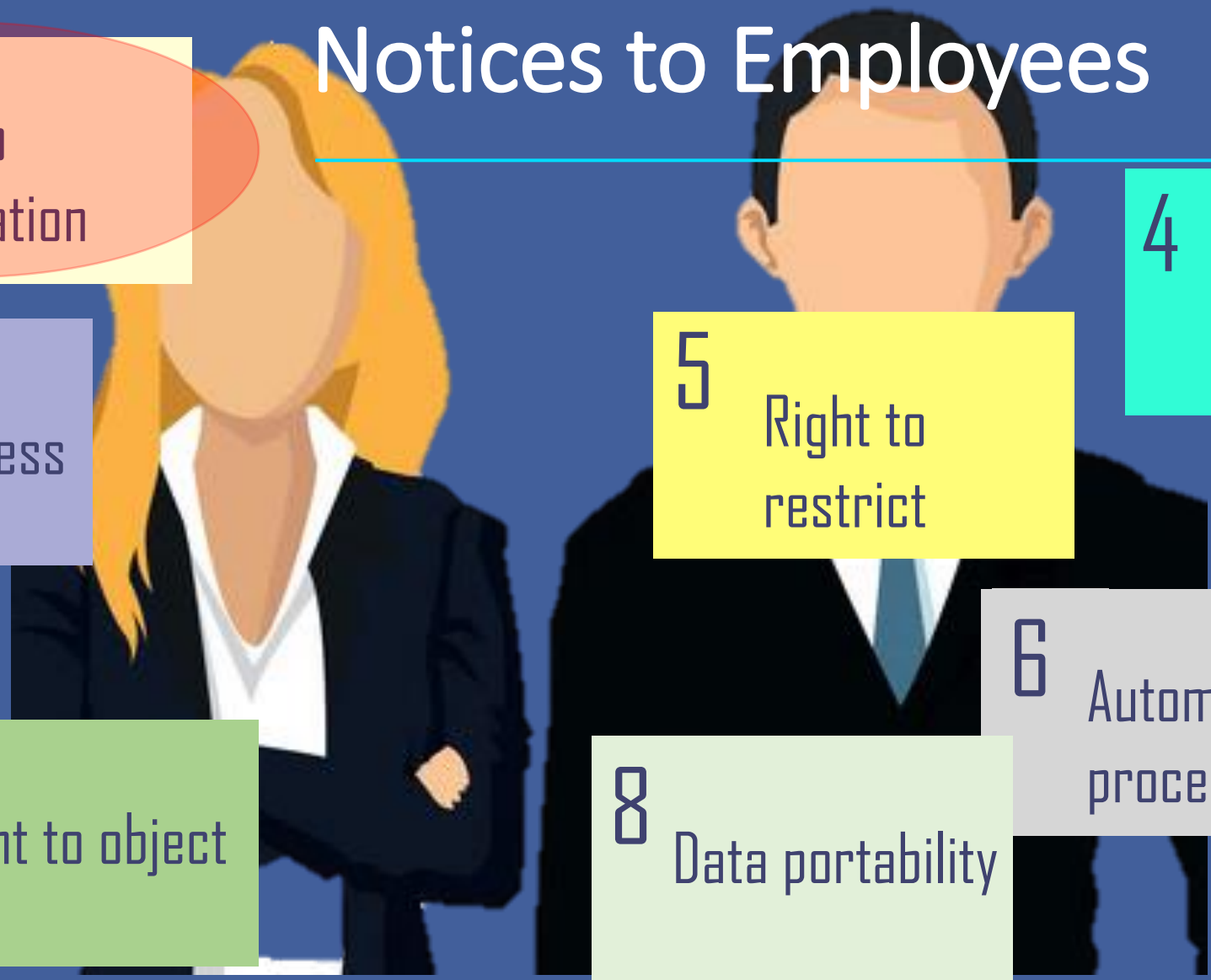
1	lawful, fair and transparent
2	specific, explicit and legitimate purpose
3	adequate, relevant and limited to what is necessary
4	accurate & up to date
5	storage limitation
6	integrity and confidentiality

Accountable

Privacy Standard

Having these duties set out in writing does not exempt the employer from being bound to **educate & train employees on good data practices** in order to comply with the law.

Notices to Employees



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

Notices to Employees

- Personal Data Processing for employment purposes
- Monitoring

Privacy Notice to Employees

- **identity** and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the **data protection officer**, where applicable;

Privacy Notice to Employees

- the **purposes** of the processing for which the personal data are intended

What can the purpose of processing be in employment?

Privacy Notice to Employees

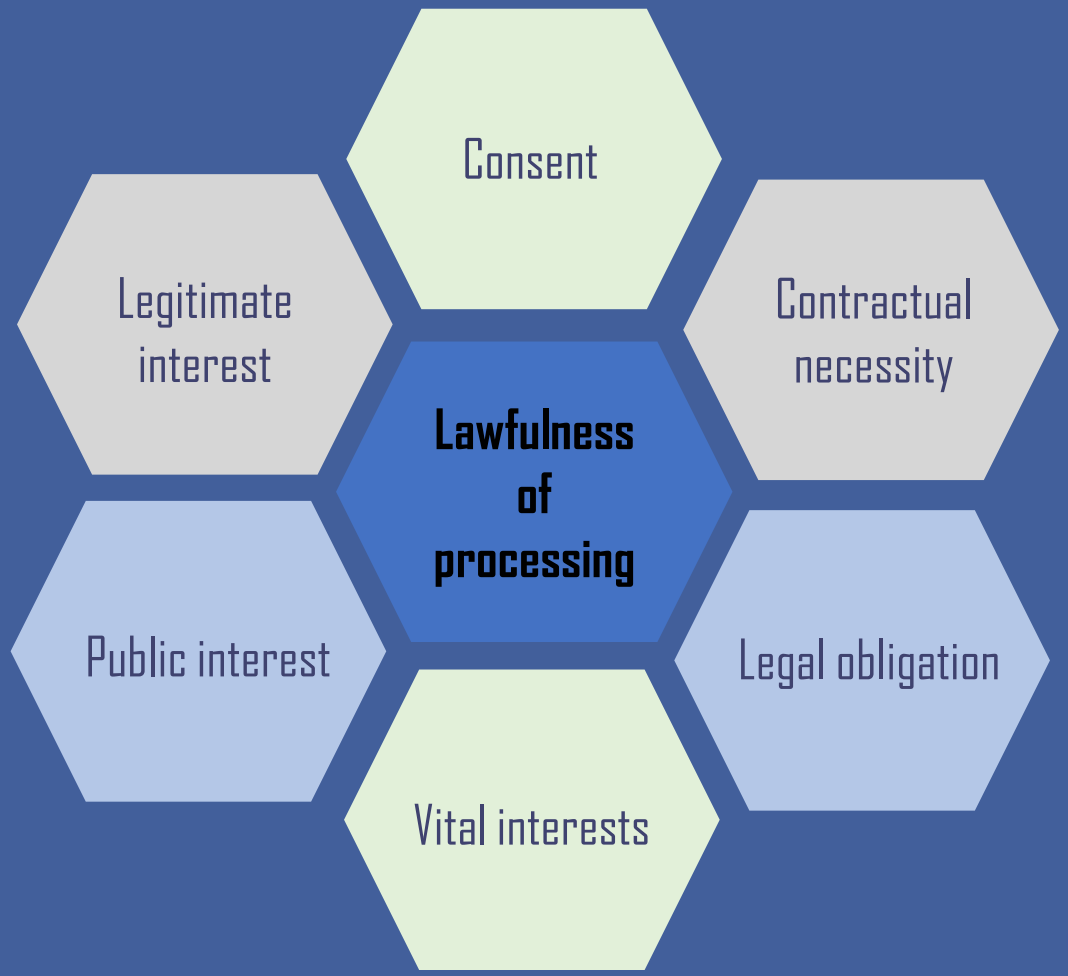
- Assess suitability for a particular role or task.
- Support in implementing any health-related adjustments.
- Monitor, evaluate and support.
- Administer remuneration, payroll, and other standard employment functions.
- Administer HR-related processes, including those relating to performance/absence management, disciplinary issues and complaints/grievances.
- Operate security (including CCTV).
- Deliver IT facilities.
- Communicate effectively.
- Support training, health, safety, and welfare.
- Contact others in the event of an emergency.

Privacy Notice to Employees

- the **lawful basis** for the processing;

Can you mention any of the 6 possible lawful basis?

Privacy Notice to Employees



Privacy Notice to Employees

- the **recipients** or categories of recipients of the personal data, if any;
- where applicable, the fact that the controller intends to **transfer** personal data to a third country or international organisation

Privacy Notice to Employees

- where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;

Privacy Notice to Employees

- Need to know your data
- Data Register
  - Purpose of processing
  - Categories of personal data
  - Categories of recipients (DPA?)
  - Third countries (safeguards)
  - Retention period
  - Lawful Basis
  - Source
  - Storage

Question Time

Types of Monitoring

Mention different types of monitoring which are carried out at the place of work or on employees

www.menti.com

Code: 7857 1675

Types of Monitoring

- **Email content and traffic**
  - search the content of emails sent;
  - checking for key “danger” words; or
  - destination addresses
- **Internet use**
  - monitor and block employees’ use of different sites
  - see which websites have been visited by the use of “cookies” or “web prints”
- **Telephone use**
  - volume and cost
  - record samples of telephone conversations

Types of Monitoring

- **CCTV**
  - Security
  - Disciplinary
- **Biometric**
  - Access control
  - Verification of attendance
- **Vehicles**
  - Unlawful use
  - Tracking of whereabouts

Types of Monitoring

- **Automation**
  - **Analytics**
- **Mystery Shopping**
  - **Assess service**
  - **Reporting/filming**

Monitoring

Employees must be informed:

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

Question Time

BYOD

- may use an approved personal mobile device for business purposes
- to protect our systems and company data, and to prevent company data from being deliberately or inadvertently lost, disclosed or altered

BYOD

Clearly outline the security measures required from employees' personal devices being used for work:

- Physical security (such as not leaving devices lying around unlocked)
- Anti-virus/malware software
- Protection via pin-number/passwords/pattern locks/facial/fingerprint etc.
- Maintain operating systems (to keep updated with the latest security patches)

BYOD

Employees must also be made aware of what they should do in the case of a **lost or stolen device**, or when **unauthorised use** of the device has been made.

Employer’s action when device is reported lost or stolen

Should also cover what happens with the device upon **termination of employment**.

Question Time

Social Media

- The **use of the internet and social media continues to grow each day**, and may affect business whether or not employees are allowed to use personal devices at the place of work.
- A social media policy aims to **regulate employees' behaviour and presence on social media** in terms of the protection of their employers' reputation.
- The policy must strike a balance between the **protection of business** and not curtailing employees' freedom.

Social Media

- **Prohibited behaviour on social media**, with respect to the maintaining of the employer's reputation and prohibition from misrepresenting or disparaging the employer's business
- Guidelines on **acceptable and responsible use of social media**, whether on or off the place of work
- Disciplinary action which may be taken (depending on the severity of the violation - one cannot compare the use of WhatsApp for a mere few minutes to the uploading of videos on Facebook of employees fooling around at the place of work).

WhatsApp Use Policy

- Impose the activation of all the apps security features, including 2 factor authentication;
- Require activation of the messages auto-destruct function
- Set out the type of data and categories of data subjects which can and cannot be shared OR completely exclude the sharing of data through the app

WhatsApp Use Policy

- Indicate whether sharing is limited for internal purposes only and exclude sharing with external third parties
- Exclude backups of the chats
- Highlight the unacceptable use of the app
- Include a reporting procedure in case of misuse
- Explains how WhatsApp messages/groups are to be handled in relation to employees who are no longer working for the company

Question Time

SAR

A right granted and regulated by the GDPR

A data subject has the right to obtain all personal data pertaining to them which is held and/or processed by an organisation

The requested organisation must comply with such a request within a period of 1 month (which may be extended up to a maximum of a further 2 months if the situation so warrants)


Employees

SAR


117%
increase
for the Metropolitan Police
POLICE

SAR

- Form
- Procedure
- Policy

SAR

- Receipt formats
- Directed to
- Receipt acknowledgement
- Data subject identity
- Request made on behalf of data subjects
- Identifying the data
- Reasons for denying requests
- Responding to different types of SAR

Question Time

Secure IT Use Policy

Equipment Security and Passwords

Systems and Data Security

Email

Using the Internet

Personal Use of Systems

Monitoring

Prohibitive use of systems

Disposal of IT equipment

Email Use Policy

- Prevents Phishing
- Abide with privacy legislation
- Personal Data

“It helps protect your organisation against security breaches including unauthorised data access and distribution.”

Email Use Policy

Phishing Stats

- One in every 99 emails is a phishing email.
- It's estimated that **3.4 billion** fraudulent emails are sent daily.
- **81% of organisations** around the world have experienced an increase in email phishing attacks since March 2020.
- around **25% of all data breaches** involve phishing and 85% of data breaches involve a human element (Verizon 2021).
- 2021 was the costliest year for data breaches in 17 years.

Email Use Policy

- Standards users must follow when using the Work Email
- Ensuring availability by protecting it from unauthorised or accidental modification
- Preserving confidentiality and protect against unauthorised disclosure
- Making the Users aware of what is acceptable and unacceptable use of the Work Email.

Email Use Policy

- Password (changes and strength)
- Using account on mobile devices
- Personal Use of the Work Email
- Monitoring
- Protecting data sent via email
- Retention/Archiving/Deletion of Emails
- Post termination

Question Time

Information Technology & Data related policies, information & procedures

Angelito Sciberras

June 2022