Workforce Monitoring and Subject Access Requests

Angelito Sciberras

29 March 2022

Why?

Website Monitoring and Subject Access Requests

WIFY?

Why?

IDPC Decisions

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

Why?

Other cases

- unauthorised disclosure of data
- breach of security principle
- breach of data minimisation
- breach of right to be forgotten
- unauthorised uploading on social media
- failure to implement appropriate technical and organisational measures
- unauthorised use of personal data leading to employment disciplinary proceedings
- lack of privacy policy/notice
- unauthorised access to personal data
- failed right of data portability
- processing without consent
- emails sent with all recipients in copy
- accidental loss of data
- lack of transparency
- no valid legal basis
- cyber attack
- unsolicited marketing

Why?

IDPC Decisions

Monitoring	20 in favour of ds vs 3 in favour of controller
Access Requests	13 in favour of ds vs 4 in favour of controller
Personal data undergoing processing was partially provided following a right of access request. Privacy Policy not satisfying the transparency requirements	**€20,000**
Controller failed to provide information following a right of access request and failed to inform the data subject about a restriction	**€5,000**

Today

- Monitoring
  - Lawfulness
  - Types of Monitoring
  - Privacy Implications
- Subject Access Requests
  - Policies & Procedures
  - Information to be given

Monitoring

Questions

- Can we monitor?
- What can be monitored?
- To what extent?
- For how long can the monitoring take place?
- Monitoring data retention periods?

“Being an emcee onstage is mostly about crowd control, about monitoring energy levels”

Daveed Diggs

Monitoring

Reason

Lawfulness

Impact

Information

Implementation

Reasons for monitoring employees?

60sec

Monitoring

Provides visibility into employee work habits used to improve;

- operational efficiency
- meet compliance requirements
- improve security in businesses

Operational efficiency

Time Theft

*Gallup estimates that actively disengaged employees cost the U.S. between **€415 billion to €520 billion** each year in lost productivity*

- Unauthorised “extended” breaks
- Workers punching/signing in on coworkers behalf
- Exaggerated time spent working on tasks
- Cyberloafing
- Extending working hours for overtime purposes

Operational efficiency

UK Parliament staff made 24,000 attempts to view online pornography in four months

- The Telegraph (2018)

Combatting Time Theft

- Monitoring of internet usage
- Limit browsing of non-work websites
- Identify suspicious bandwidth hogs
- Optimise work processes through productivity & engagement trends analysis
- Performance Improvement Plan (PIP)

Increased Productivity

Politics
City of London

U.K. MP Resigns After Admitting Watching Porn in Parliament

- Conservative MP Parish tells of 'moment of madness,' BBC says
- 'I was wrong, I was stupid,' Parish tells broadcaster

By Emily Ashton and Colin Keatinge
April 30, 2022 at 5:05 PM GMT+2

Meet compliance requirements

Cybersecurity Risks

99% of professionals admitted to sharing and storing login credentials to sending work documents to personal email accounts

- Data Vulnerability Report, Intermedia

- Sharing of login credentials
- Unauthorised file transfers
- Downloading of malware
- Email autoforwarding
- Copying of company data

Meet compliance requiremer

34% of employees store work documents using sync-and-share services such as cloud storage websites, allowing them to access the documents from personal accounts even after leaving an organisation

- Data Vulnerability Report, Intermedia

Combatting Cybersecurity Risks

- Monitoring of internet usage
- Monitoring of App usage for potentially dangerous applications
- IP and sensitive data monitoring during offboarding process
- Optimise work processes through productivity & engagement trends analysis
- Monitoring user activity for anomalous bandwidth spikes

Enforce Company Policies

Improve security in businesses

Video surveillance

- Unauthorised access
- Negligence of health & safety procedures
- Harassment, bullying or assaults
- Vandalism, pilferage & theft
- Time theft

Improve security in businesses

Video surveillance

- Limit access to authorised personnel
- Enforce health and safety procedures
- Signage and visible CCTV cameras

Safer work environment

Situations which can be avoided or detected

Lawfulness of monitoring

*"Employers have **legitimate interests in monitoring** in order to improve efficiency and protect company assets. However, workplace monitoring becomes **intrusive and unjustifiable** if it is not limited or transparent."*

- Working Party 29

Constitution

Article 32 of the Constitution of Malta

Every person in Malta is entitled to the fundamental rights and freedoms of the individual, that is to say, the right, whatever his race, place of origin, political opinions, colour, creed, sex, sexual orientation or gender identity, but subject to respect for the rights and freedoms of others and for the public interest, to each and all of the following, namely […] **respect for his private and family life**.

European Convention on Human Rights

Article 8. **Right to respect for private and family life**

8.1 Everyone has the **right to respect for his private and family life**, his home and his correspondence.

8.2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Right to Privacy

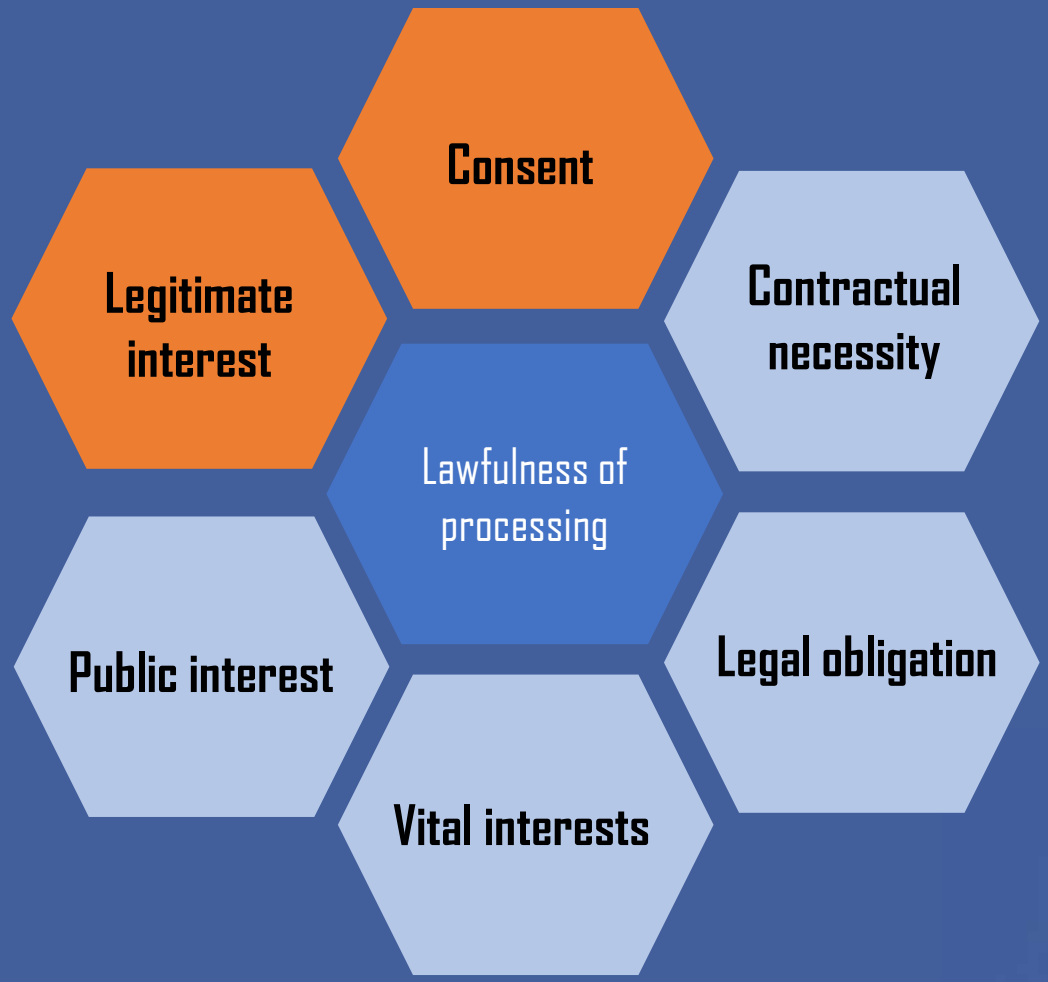
Not an absolute Right

European Convention of Human Rights - Art. 8

the right to respect for one's private and family life, his home and his correspondence, is **subject to certain restrictions** that are "**in accordance with law**" and "**necessary in a democratic society**".

Lawfulness of Processing Data

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



Bărbulescu v Romania (ECHR)

found that the **monitoring of an employee's email account resulted in the violation of his right** to respect for private life and correspondence within the meaning of Article 8 of the ECHR

The Court additionally observed that the domestic courts did not pay attention to the **scope** of the monitoring, the **degree of the intrusion** nor to whether the monitoring was justified by **legitimate reasons**. In fact, the specific aim of such strict monitoring was not even identified, while **neither the seriousness of the consequences for the applicant nor alternative less intrusive measures were examined**.

Bărbulescu v Romania (ECHR)

flow and the **content** of the applicant's communications had been recorded and stored by the employer.

the applicant did not appear to have been informed "of **the extent and nature** of his employer's monitoring activities, or of the possibility that the employer might have access to the actual contents of his communications".

the Court concluded that Article 8 was applicable as "**employer's instructions cannot reduce private social life in the workplace to zero**".

Libert v France (ECHR)

all files created by employees on a work computer were to be considered as being of professional nature, **unless identified as private**

López Ribalda and Others v. Spain (ECHR)

- the prior notification to employees of the possibility and the implementation of such measures and the disclosure of information regarding their exact nature;
- the extent of the monitoring, meaning the degree of limitations in time and space as well as the number of people with access to the footage;
- the legitimate reason to justify the monitoring;
- the possibility of implementing less intrusive methods;
- the severity of consequences of the monitoring; and
- the provision of legal safeguards for the employees (i.e. in order for them to challenge the measures before an independent body).

Increased monitoring

are we going to far?

Increased Monitoring

- New monitoring technologies are cheaper to implement but have **increased processing capacity**.
- New forms of monitoring, such as location data from a smartphone, can be **less visible** to employees than traditional forms.
- The growth of homeworking, remote working and "bring your own device policies" has reduced the distinction between the workplace and home. This raises the risk that individuals could be **monitored in a private context**.

Increased Monitoring

Two monitoring tools

Hardware + software

Software only

Which is the most intrusive and might breach the employees' right to privacy?

Think about this…

Think about this...

Increased Monitoring

Two monitoring tools

Hardware + software - Humanyze

Software only - Kickidler

Which is the most intrusive and might breach the employees' right to privacy?

Types of monitoring

Your Turn

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

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

- Device Tracking
  - Geo Location
  - Duration
- Automation
  - Analytics
- Mystery Shopping
  - Assess service
  - Reporting/filming

Monitoring

Processing of Personal Data

Processing of Personal Data

Regulated by Data Protection Legislation - GDPR and Data Protection Act (Cap. 586)

Application of GDPR

- Principles
- Conditions for processing
- Data Subject Rights

Data Protection Legislation

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**

Data Protection Legislation

Conditions for processing

1. **Consent**
2. Contractual necessity
3. Legal obligation
4. Vital interests
5. Public interest
6. **Legitimate interest**

Data Protection Legislation

Consent

- highly **unlikely to be a legal basis** for employee monitoring unless employees can refuse without adverse consequences.
- in exceptional circumstances - must be **specific, informed** and requiring an **active expression** of will.
- **inaction**, such as not changing default settings, **cannot qualify as consent**.

Data Protection Legislation

Legitimate Interest

- provided that the purpose of the processing is legitimate.
- chosen method or specific technology is necessary, proportionate and implemented in the least intrusive method
- does not override the fundamental rights and freedoms of employees

Impact

Data Protection Legislation

Legitimate Interest... The employer should;

- conduct a **proportionality test**, which can form part of a **data protection impact assessment (DPIA)**, prior to the introduction of any monitoring tool.
- introduce specific **mitigating measures** to ensure a balance between the interests of the employer and the employee's rights and freedoms.
- include **limitations** on monitoring to ensure the employee's privacy is not violated.

Data Protection Legislation

Legitimate Interest... **Proportionality Test;**

Questions to be answered

- What monitoring is carried out?
- Why is the monitoring carried out?
- Can the identified purpose be achieved without monitoring?
- Is there a less intrusive method of monitoring?
- What is the impact of monitoring on employees?
- Is the monitoring justified?

Data Protection Legislation

Legitimate Interest... DPIA;

- before undertaking any processing that presents a specific privacy risk by virtue of its nature, scope or purposes.
- GDPR sets out a list of situations where a DPIA is required which includes profiling.
- CCTV

Data Protection Legislation

Legitimate Interest...

DPIA;

is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan.

Data Protection Legislation

Legitimate Interest... **Limitations may include;**

- **Geographical** (limiting monitoring to specific places).
- **Data-oriented** (excluding personal electronic files and communications from monitoring).
- **Time-related** (sampling instead of continuous monitoring).

Information

Data Protection Legislation

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

Data Protection Legislation

Right to Information... Employees must be informed:

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

Data Protection Legislation

Right to Information... Employees must be informed:

- Acceptable use policy
- Privacy policies/information
- Signage

Secure IT Use Policy

Work email use Policy

Data Protection Legislation

Right to Information... Employees must be informed:

- Acceptable use policy
- Privacy policies/information
- Signage

Employee Privacy Notice

CCTV Policy

Data Protection Legislation

Right to Information... Employees must be informed:

- Acceptable use policy
- Privacy policies/information
- Signage

Data Protection Legislation

Right to Information...

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

Signage:

CCTV
IN OPERATION

IMAGES ARE BEING MONITORED AND MAY BE RECORDED FOR THE PURPOSE OF CRIME PREVENTION AND PUBLIC SAFETY

This scheme is operated by:

123 Limited

For further information contact
The Data Controller

TEL: **+356 123456**

What is missing in this notice from an HR perspective?

Data Protection Legislation

Right to Information... Notice:

- When information about their (email/internet) use will be obtained.
- Why it is being obtained.
- How this information will be used.
- Who it will be disclosed to.

Data Protection Legislation

Right to Information... Notice:

- Ensuring the contents of the policy are dealt with in the induction process for new workers.
- Setting up IT systems so that workers must read the policy in full from time to time before they can access email or the internet.
- Setting up reminder systems by using emails or having a short-form message that pops up when workers access email or the internet.

Data Protection Legislation

Right to Information... Notice:

- Consider requiring workers to electronically confirm they have read the policy before they can continue work on their computer.
- Training, including general data protection awareness training and training for managers on appropriate monitoring techniques.
- The use of workplace surveys to check levels of awareness among the workforce.

Data Protection Legislation

Right of Access...

Data Protection Legislation

Automated processing... **Employees have the right NOT to:**

- be subject to a decision based solely on the automated processing of data

Unless the decision is necessary to enter into or perform a contract or the data subject has **consented** explicitly.

New Technologies

Guidelines on using new technology

Social media profiles

- do not assume that it is allowed to inspect a candidate's social media profile during the recruitment process
  - legal basis is required
  - is profile for business or private purpose?
  - the individual must be notified of the processing in advance

- once an individual becomes an employee, screening of social media profiles should not take place on a generalised basis.

Guidelines on using new technology

Monitoring ICT usage

- monitoring all online activity is likely to be disproportionate and less invasive methods of protection should be investigated
- employees must be notified of the type of monitoring that is carried out

Guidelines on using new technology

Monitoring outside the workplace

- employers should balance the risks posed by home and remote working in a proportionate manner
- use of an employee's own device will be personal in nature and any monitoring that could potentially access all data on a device must be carefully managed (BYOD)
- a DPIA should be carried out prior to the use of tracking technology on any device (inform employee)
- do not track wearable devices (health data)

Guidelines on using new technology

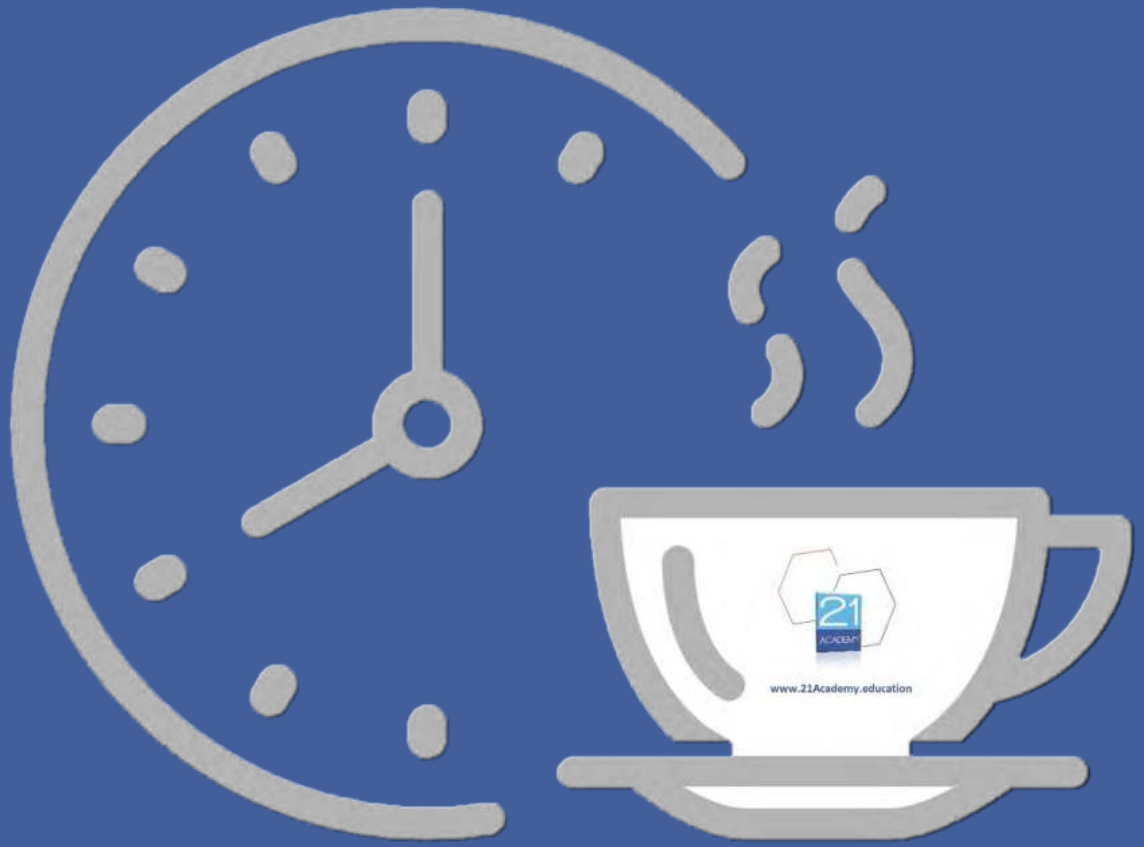
Vehicle monitoring

- a facility should be offered for the employee to turn tracking off during personal use
- employees must be clearly informed of the tracking device (in vehicle)
- no location monitoring of vehicles outside working hours

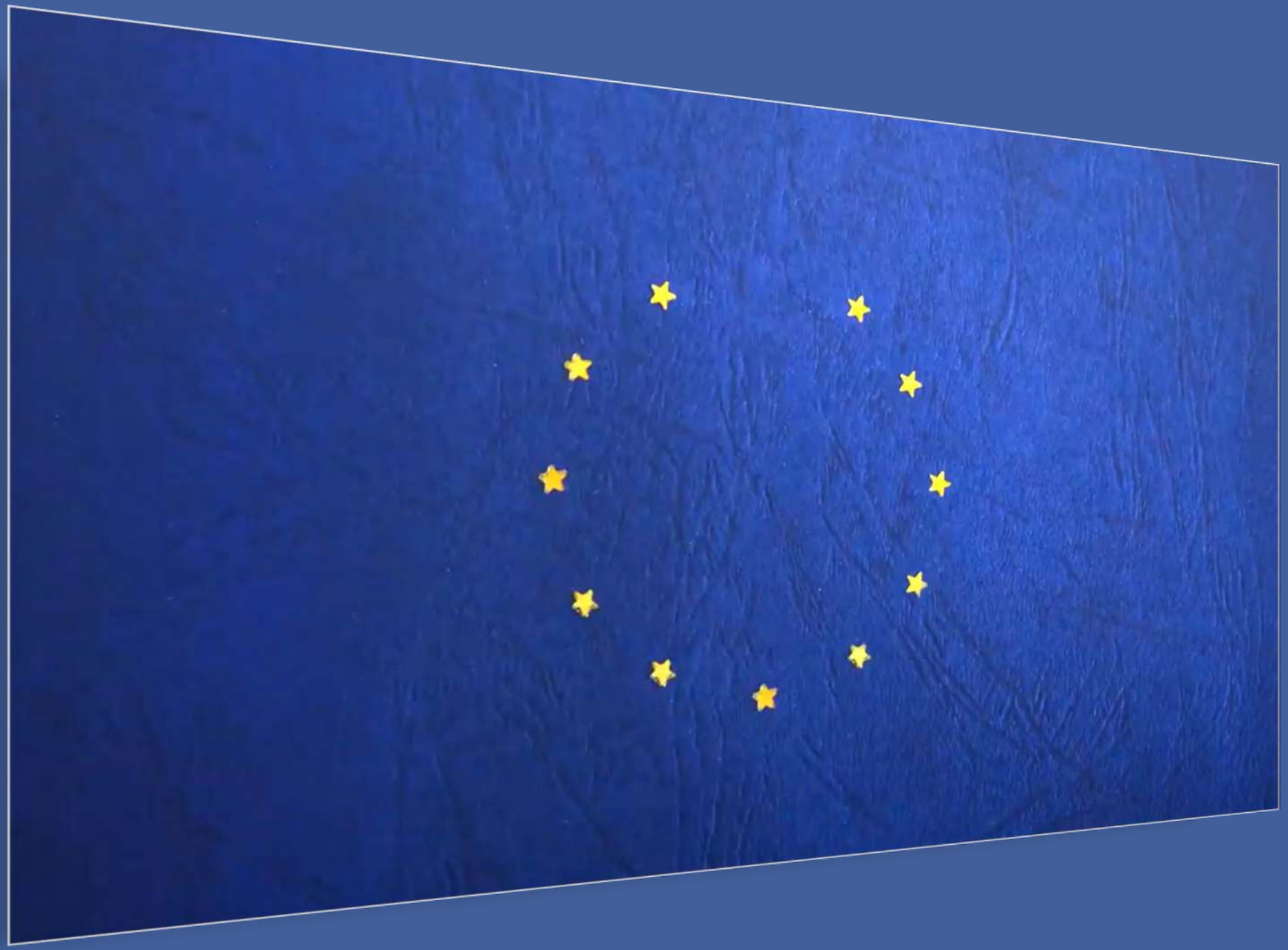
Guidelines on using new technology

Access controls

- employees must be clearly informed
- cannot be justified if these data are also used for another purpose, such as employee performance evaluation


www.21Academy.education

Subject Access Requests



The Right to SAR

A fundamental right under the Charter of Fundamental Rights of the European Union (2012/C 326/02)

Article 8(2) of the Charter states that "*everyone has the right of access to data*" which is collected about them.

The Right to SAR

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

Summary of rights

An employee has the right to obtain from an employer information as to whether or not personal data is being processed about him or her.

What's being advised to employees?

Alex Monaco

Senior Employment Solicitor

Summary of rights

If personal data is being processed, the employee is entitled to be given a copy of his or her personal data together with the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom data has been or will be disclosed;
- the period during which personal data will be retained;

Summary of rights

- information on the source of the data;
- information regarding complaints and disputes;
- transfer of data outside the EEA (if any);

Summary of rights

The information must be provided free of charge (Article 12.5).

The employer must provide the information without undue delay and, in any event, within one month of receipt of the request.

Approach

Employer should approach compliance in a positive and helpful way:

- The employer must facilitate the exercise of the subject access right (Article 12.2).
- The request must be handled fairly and transparently (Article 5.1(a)).
- Information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language (Article 12.1).

Receiving a SAR

A SAR may be made:

- in writing
- email
- other electronic means and,
- orally

Employer should provide means for requests to be made electronically

Set out a preferred method of contact

Responding to a request

Initial assessment

- Is data concerning the employee processed?
- Respond or not?
- Scope behind the request?
- Approach to find the data and response.

Responding to a request

Checking identity of person making request

- make sure that a person is lawfully authorised to act on behalf a data subject
- no exceptions for family members

Responding to a request

Timing

- basic rule is that requests must be handled without undue delay and, in any case, within one month of the receipt of the request
- (may) extend by 2 months were necessary (complexity and number of requests)
- inform data subject within a month

Responding to a request

Understanding what the employee wants

- ask the employee in more detail what information he or she is after
- aim of the request should not be to narrow the scope

Responding to a request

Manifestly unfounded or excessive requests

- Charge a reasonable fee.
- Refuse to act on the request.

Need to demonstrate that the request is indeed manifestly unfounded or excessive

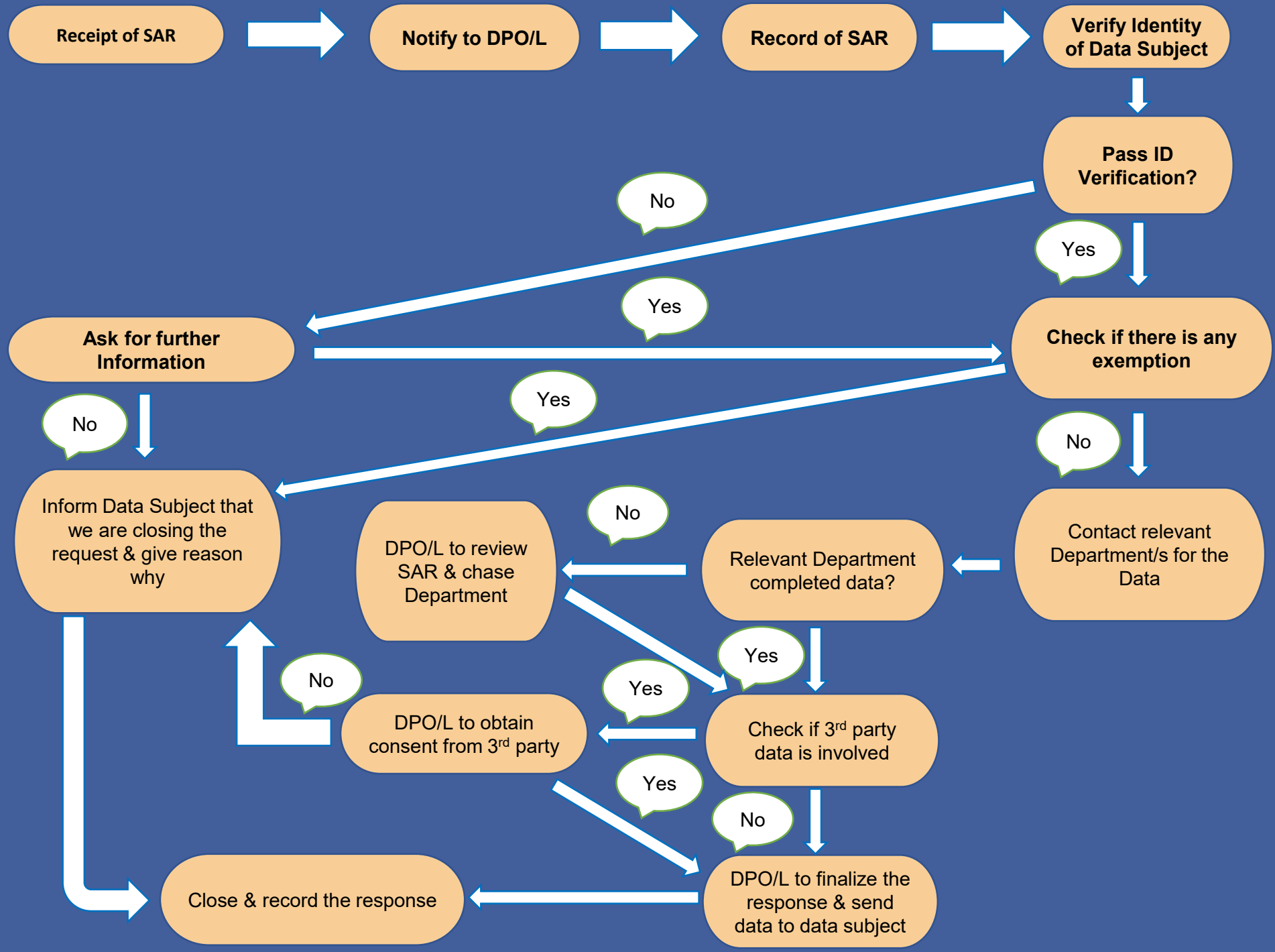
Responding to a request

Form of response

- Writing
- Electronic means
- Orally (following a request by employee)

Ideal Scenario

Policy on handling a SAR
Response procedure
Form (one for each subject right)
Tracking form
Letters
Logbook



Workforce Monitoring and Subject Access Requests

Angelito Sciberras

29 March 2022