

MAMO TCV

ADVOCATES

Data Processing in Employment

Dr. Warren Ciantar

Senior Associate, MamoTCV Advocates

26.10.2023

What is the aim of Data Protection Legislation in Employment?

- Creating a balance → legitimate interests of the employer and reasonable privacy expectations of employees.
- More advanced technology – greater risks of invasion of privacy of the individual.



Modern Risks to Employee Privacy



- Data processing technologies have become cheaper;
- New forms of processing and tracking have become less visible to employees;
- Blurring of lines between home and work – working remotely.



Stages of Employment...

Data Protection issues can arise in all 3 stages:

- Recruitment/Interviewing stage;
- During Employment;
- Post-employment.

What is Protected?

‘Personal Data’ – No need to be identified by name – the data subject can be identifiable:

“...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”.



PERSONAL DATA (AND DATA SUBJECTS)

“Personal Data” means 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 (IP address, Cookies, device IDs etc.);
- One or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

NB 1 the GDPR does not apply to the processing of **anonymous data**.

NB 2 the GDPR does not apply to the processing of **personal data of deceased persons**.

Definitions of Key Terms

Pseudonymisation

Definitions of Key Terms

- **'Pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Pseudonymisation

Definitions of Key Terms

- 'Pseudonymisation' *EX*:

List A

- *Employee A*
- *Employee B*
- *Employee C*
- *Employee D*
- *Employee E*

List B

- *Brad Pitt*
- *Leonardo da Vinci*
- *Cristiano Ronaldo*
- *Warren Ciantar*
- *Freddie Portelli*

Special Categories of Personal Data (Art. 9)

(Formerly 'sensitive personal data')

Means Personal Data that reveal:

- Race or ethnic origin, or
- Political opinions; or
- Religious or philosophical beliefs; or
- Trade union membership; or
- Data concerning health or
- Data concerning a natural person's sex life or sexual orientation.

As well as Processing of:

- Genetic data (genes, gene products etc.)
- Biometric data (fingerprints, retina and iris patterns etc.)

Stricter rules apply to the processing of **sensitive** personal data

Definitions of Key Terms

Criminal Conviction Data



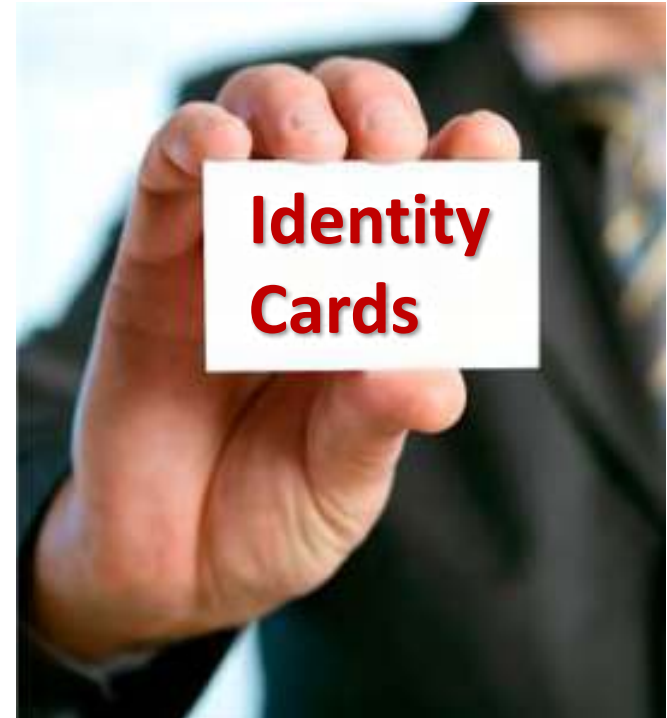
- Under the GDPR and the Maltese DPA, **data relating to offences or criminal convictions** may only be processed **under the control of a public authority** and **under strict requirements**, except as may be authorised by regulations and subject to suitable safeguards in accordance with Article 10 of the GDPR.
- The GDPR also specifically states that a complete register of criminal convictions can only be kept by a public authority.
- There are presently no Maltese derogations to this general rule.

What About ID Cards?

Under the DPA, ID Cards may only be processed (i.e. including storing of such information):

If the processing is clearly justified by:

- A) The purpose of the processing;
- B) The importance of a secure identification;
- C) Another valid reason prescribed in regulations.



IDPC: *"Copies of ID cards can only be stored in exceptional cases where a law specifically requires or authorises such processing" (e.g. AML laws).*



Principles of Processing Data (Art. 5)

- Data processed for specified and legitimate purposes;
- Limit purpose of processing;
- Apply proportionality and subsidiarity;
- Be transparent with employees about use and purpose;
- Enable data subject to access data and rectify;
- Keep data accurate and not longer than necessary;
- Protect against unauthorised access.



Legal Basis for Processing (Art.6):

When processing personal data, one of the 6 legal bases must be applicable:

1. Data subject has given his consent;
2. Necessary for performance of a contract;
3. Necessary for compliance with legal obligation;
4. Necessary to protect the vital interests of data subject or another person;
5. Necessary for performance of a task carried out in the public interest;
6. Necessary for the purposes of the legitimate interests pursued by the controller or by a third party – except when this is overridden by interests/rights of data subject.

Can Consent be a Valid Basis?

- In other non-employment scenarios – yes;
- Consent – “any **freely given**, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”



Can Consent be a Valid Basis?

- In employment – can it be *freely given*?
- Employee is 'dependent' on the employer
→ imbalance of power in the employment relationship.
- There can be no genuine choice on part of the employee – therefore consent cannot be legal basis.
- Consent by data subject can be withdrawn at any time – unfeasible for employer to rely on this.

Can Consent be a Valid Basis?

- Certain limited instances where there is no other legal basis to process → ex. Filming at the place of work / use of photos for social events.
- In such a case – consent may be an adequate basis to process as employee has a choice as to whether to accept to or not without suffering any consequences.



Consent as an invalid basis...

Decision from Greece's Data Protection Authority – 26/2019 relating to PWC;

Cannot use consent to process personal data of employees;

Fine of €150,000 imposed on PWC.

Legitimate Bases to Process:

- Necessary for the performance of a contract;
- Necessary to comply with a legal obligation;
- Necessary for the purposes of the legitimate interests pursued by the employer – importance of proportionality with legitimate interests of data subject.



Legitimate Interest Ground

Purpose must be legitimate (ex. Security reasons);

Chosen method or technology for processing must be necessary for the legitimate interest of the employer;

Processing must be proportionate to the business needs;

Processing should be carried out in the least intrusive manner possible.



Information to be Provided:

Not only must the employer identify a legitimate basis for data processing but the following information must also be provided:

- i. Identity & contact details of controller;
- ii. Contact details of data protection officer (if applicable);
- iii. Purpose and legal basis for processing;
- iv. Legitimate interests pursued (if this is legal basis);
- v. Recipients or categories of recipients;
- vi. Intention to transfer data to third country or international organisation (if applicable).



More Information to be Provided:

- i. Existence of the right to request access to data/ rectification or erasure of data/ restrict processing or object to processing;
- ii. Data retention period or criteria used to determine the period;
- iii. Right to lodge a complaint with supervisory authority;
- iv. Whether providing personal data is a contractual or legal requirement or necessary to enter into a contract & consequences of failure to provide data;
- v. Existence of automated decision making.

Transparency:

- New technologies – allow collection and processing in more secretive ways = greater need for transparency.
- Important to inform employees about existence of any monitoring, the purpose for which data is to be processed etc;
- How? Employment contract itself or through specific policies;



Recruitment Stage:

- Using social media to view profiles of candidates for employment – is it permissible?
- Can the employer keep the data collected during an interviewing process? If yes – for how long?
- Keep rules on police conduct certificates in mind



Outboarding Stage:

- Employer should inform the employee beforehand of what will take place with their data and what the employee should do.
- E.g. Company will keep a copy of the entire work inbox and they should make sure to remove any personal emails they have in it before leaving





Monitoring During Employment

- Development of potentially more intrusive means of monitoring – not only monitoring of email or website use;
- Monitoring all online activity of employees – disproportionate interference with data subjects' rights.
- Importance of written policies re monitoring – allows employees to adapt their behaviour.
- Consider – proportionality + acceptable use policies.

Monitoring at the Workplace

- Necessity to protect network and preventing unauthorised access or data leakage – employer might implement measures to monitor online activity of employees;
- Good practice:
 - provide alternative unmonitored access for employees ex. Free WiFi for private usage;
 - No interception of certain kind of traffic ex online banking and health websites;
 - Clear policy about acceptable and unacceptable use of the network and facilities;
 - If possible block certain websites as opposed to monitoring use.





Monitoring ICT use Outside the Workplace:

- Remote working – may result in breaches to employer's security/ loss of information etc – what means are permissible to monitor activity?
- Bring Your Own Device (BYOD) – can lead to employers processing non-business related information;
- Mobile Device Management (MDM) – enables employers to locate devices remotely and even delete data on demand.
- Tracking of vehicles used by employees for work purposes – duty to inform and switch off tracking after working hours.

Monitoring Cont:

Ownership of an electronic device does not necessarily mean that the employees do not enjoy the right to secrecy of their communications, related location data and correspondence.

Prohibiting all communications for personal reasons is not practical & might require a high level of monitoring which is disproportionate.


On-Premises Monitoring – General CCTV Rules:

- 7-day retention period for footage (extendable to 20 days in limited cases with IDPC approval)
- Camera must not be pointed at areas you do not own/control
- Sound recording should be avoided wherever possible
- Cameras should not be pointed directly at employees' terminals/workstation
- You can (and in most cases must) provide footage to the police if they ask for it (provided you still have it – if you don't, it's not an infringement at your end)
- Ensure that any security contractors also abide by data protection law (have a DPA in place if they process personal data on your behalf)
- Individuals under surveillance may exercise their right of access
- **No covert recording** – You must always notify data subjects via a notice as per EDPB template



CCTV Notice – EDPB Template

(Note the legal
basis being used)

 <p>Video surveillance!</p>	<p>Identify of the controller and where applicable, of the controller's representative:</p>
	<p>Contact details of the Data Protection Officer (where applicable):</p>
	<p>Purposes of the processing for which the personal data are intended as well as the legal basis for the processing: Our legitimate interests to ensure adequate security on our premises, for crime-prevention purposes [and for monitoring of work-related activity].</p>
<p>Further information is available:</p> <ul style="list-style-type: none">• Via the notice provided to you• At our reception/customer information/HR manager• On our website (URL/QR Code: ___)	<p>Data subject rights: As a data subject you have several rights against the controller, in particular the right to request from the controller access to or erasure of your personal data.</p> <p>For details on this video surveillance including your rights, see the full information provided by the controller through the options presented on the left.</p>

Limitations to be imposed on monitoring:

- Limitations ensure that employees' privacy is not violated:
- Limitations can be:
 1. Geographical ex. Monitoring only certain specific places;
 2. Data-Oriented ex. No monitoring of personal files and communications;
 3. Time-Related ex. Sampling instead of continuous monitoring.

Subject Access Requests

- Right of data subjects (incl. employees) to obtain a copy of information the controller holds about them;
- Employer should have a procedure in place as to how to handle such requests and how to respond.
- Also – right to obtain a rectification of inaccurate personal data.



Right to be Forgotten

- Retain data only for as long as necessary;
- What is 'necessary'?
- During employment – for the duration;
- After employment? – Any legal obligations to keep data? What data to keep? And for how long?
- What about details of candidates? CVs?





Proportionality and Data Minimisation:

- Processing must be a proportionate response to the risks faced by the employer and be the least intrusive method possible → ex. Detecting internet misuse without analysing content.
- Prevention vs detection misuse;
- Data minimisation and short retention period of data collected;

Recent Fines

- **Greece: EUR15,000** – The controller had installed a **video surveillance system** without properly informing employees and the use of the video surveillance system was considered unlawful.
- **Finland: EUR25,000** – The controller had introduced a mobile application that allowed teleworkers to clock in and out. The use of the application on a mobile device also required authorization for **location data** collection. The collection of location data at the time of clocking in was a feature of the app, without which it was not possible to clock in working hours using the app. According to the information received from the controller, the controller did not actively use or exploit the location data in any situation, but only processed the location data at the time of clocking in for technical reasons. However, the mere fact that time clocking is not possible in the application without processing the location data does not make it necessary to process them. The DPA therefore considered this to be a violation of the lawfulness of the data collection and of the principle of data minimization, since the processing of location data was not necessary for the purpose of the processing – i.e., the mere recording of working hours.
- **Denmark: EUR53,800** – The controller (a company) had emailed two of the company's customers informing them that a former employee had committed **crimes** in the course of employment and had admitted to committing them, as well as describing in detail the alleged course of events. According to the DPA, the controller in such a case had a legitimate interest in disclosing information about the former employee's dismissal to its customers and in informing the customers that, as a result, the employee could not enter into any contracts on behalf of the company. However, such a detailed description of the allegations was not necessary and thus unlawful.
- **Germany: EUR294,000** – A company was fined for 'unnecessarily long' **storage and retention** of personnel files and for 'excessive' data collection in the personnel selection process, during which also health data were requested.
- **Netherlands: EUR725,000** – The organisation had required its staff to have their **fingerprints** scanned to record attendance. However, as the decision of the data protection authority stated, the organisation could not rely on any of the exceptions to the processing of this special category of personal data (as found in Article 9) and the company could also not provide any evidence that the employees had given their consent to this data processing (which is one of the exceptions).

In Summary:

- Irrespective of technology used → keep in mind fundamental data protection principles;
- Contents of electronic communications made from business premises enjoy same rights protections as analogous communications;
- Consent is unlikely to be a legal basis for data processing at work unless employee can refuse without adverse consequences;



Cont:

- Legal Basis in Employment – performance of a contract or legal obligations ± legitimate interests as long as there is a legitimate purpose and proportionality;
- Monitoring → employees to receive information.
- International data transfers – adequate level of protection must be ensured.





Way Forward...

- Review and update current data protection policies & practices;
- Introduce policies such as: IT/security policy and BYOD policy
- Review use of employee data (**including contracts of employment**) & ways in which data is processed and stored;
- Review employee monitoring and IT practices;
- Implement procedures for reporting future data breaches;
- Consider a Data Protection Privacy Impact Assessment at the workplace when introducing new technologies.

Thank You for Your Attention

Mamo TCV Advocates

Palazzo Pietro Stiges
103, Strait Street
Valletta VLT1436
Malta

T: (+356) 25 403 000

F: (+356) 21 244 291

E: info@mamotcv.com

www.mamotcv.com

www.gdprmalta.com