Data Protection Officer Course
ADVISORY 21
2025

Erika Criscione (Attorney-at-Law) - email: erika.criscione@gvzh.mt
Ms. Hayley Ann Pisani - email: hayley.pisani@gvzh.mt
https://gvzh.mt/

Date: 6th November 2025

GDPR In The Employment Context

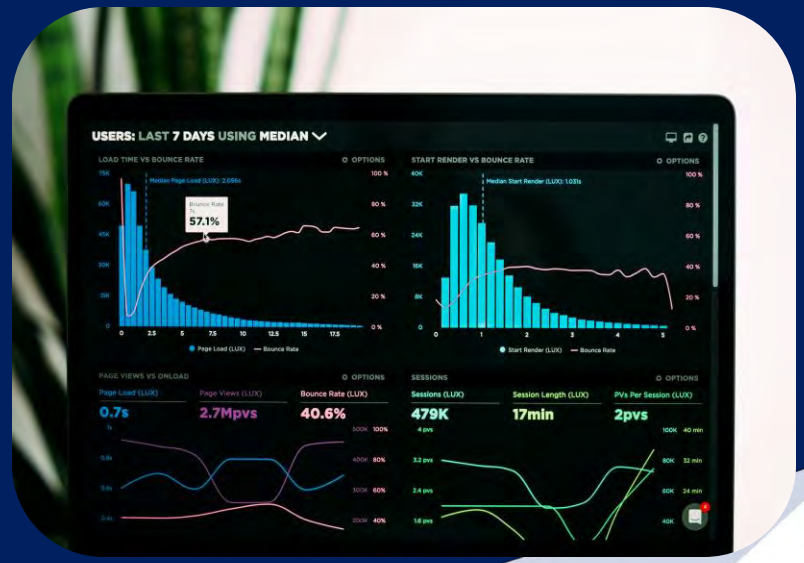
www.21Academy.education

Why Does GDPR Matter in the Workplace?

- Employees' personal data is one of the most **sensitive** categories of personal data.
- Employers must **balance** legitimate business needs (recruitment, monitoring, retention) with the **fundamental rights** of employees.
- Use of technologies create grater risks on employees monitoring and invasion of employees' privacy

What Are The Risks To Employees' Privacy?

- Excessive monitoring / surveillance (keystrokes, screen capture, webcam)
- Use of biometric & health data (wearables, fingerprint / facial scans)
- Location tracking & geofencing
- Intrusion into non-work data or communications
- BYOD (Bring Your Own Device) and mixing personal & work data
- AI and automated decision systems (profiling, performance scoring)



Special Category of Data in the Employment Context

Personal data revealing particularly sensitive information about an individual.
Processing is prohibited, unless specific conditions apply.

What is special category data?

- Health data
- Genetic & biometric data
- Religious or philosophical beliefs
- Political opinions
- Trade union membership
- Sexual orientation & sex life
- Racial or ethnic origin

When can you process it?

Explicit consent
Necessary for healthcare / public health
Needed for legal claims
For employment & social security law (with safeguards).
For research/statistics (with safeguards).

It requires extra safeguards such as encryption, Pseudonimization, DPIAs, strict access control etc.

Anonymized Data

Information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

Pseudonymised Data

Replacing any information which could be used to identify an individual with a pseudonym, or, in other words, a value which does not allow the individual to be directly identified.

Can The Employer Request the Police Conduct Certificate to Employees?

Nru. taċ-Ċertifikat:
Certificate No.: .....

FORMULA A
FORM A

PULIZIJA TA' MALTA
MALTA POLICE

ĊERTIFIKAT TAL-KONDOTTA
CERTIFICATE OF CONDUCT

Jien middikjara illi, skond l-Ordinanza dwar iċ-Ċertifikati tal-Kondotta (Kap. 77),
I declare that, in terms of the Conduct Certificates Ordinance (Chap. 77),

isem u kunjom,
name and surname

Nru. tal-Karta tal-Identita'
Identity Card No.

bin/bint
son of/daughter of

imwieled/imwielda fi'
born on the

f'
at

u joqgħod/toqgħod
and residing at

huwa/hija persuna ta' kondotta tajba
is a person of good conduct

Kwartieri Ġenerali tal-Pulizija
Police H.Q
Malta

data
date

Dritt imħallas - € 2.50
Fee paid

(Data u inizjali)
(Date and initials)

Kummissarju tal-Pulizija
Commissioner of Police

As a general rule, employers cannot retain police conduct certificates of employees, including **prospective employees.**

Employers may have a **legitimate interest** to request police conduct certificates for the purpose of verifying whether a current or prospective employee has a clean conduct and no prior criminal convictions.

Requesting employees to present their police conduct certificate is particularly relevant for certain roles which involve contact with **vulnerable individuals**. E.g. care workers, teachers etc…

Once the individual has presented the certificate, the employer may document the confirmation of the individual's (clean) conduct. However, **the certificate itself should not be retained on file.**

What are the legal grounds for processing?

In the employment context, the most common bases are:

- **Performance of a contract**
- **Legal obligation**
- **Legitimate interests**
- **Consent**

Is Consent a Valid Legal Basis In Employment?

Consent is not usually the primary legal basis for processing employee

Given the imbalance of power inherent in the employment relationship, consent is often not regarded as being “freely given.”

- Processing of employees data is generally justified on other lawful grounds, such as the necessity to perform the employment contract, compliance with a legal obligation, or the employer’s legitimate interests.

Where consent is relied upon, it must be freely given, specific, informed, and unambiguous. Employees and candidates must also be able to withdraw their consent at any time, without suffering any adverse consequences.

Consent may still be used in limited cases where no other legal **basis is appropriate, for example, in connection with optional** benefits or voluntary programmes.

The controller must be able to show that the employee has been given a **real and meaningful choice**.

Recruitment

- ❑ Identify a clear legal basis: legitimate interest or pre-contractual necessity.
- ❑ Inform candidates how and why data is processed – Privacy Notice.
- ❑ Collect only relevant data for assessing suitability.
- ❑ Retain applications only as long as needed.
- ❑ Ensure data sharing with agencies or platforms is governed by GDPR-compliant agreements.
- ❑ Process sensitive data (e.g. health, ethnicity) only under lawful grounds.

Can employers require prospective job candidates to undergo pre-employment medical examinations and/or testing?

- **General Rule**:

Pre-employment medical testing is highly intrusive and rarely justified under GDPR.Such processing does not satisfy a lawful basis during the recruitment stage.

- **When May Testing Be Permissible?**

After selection, and only if necessary to determine medical fitness for the role. Typically relevant for physically demanding or safety-critical positions. Must be proportionate and job-specific.

Can employers require prospective job candidates to undergo pre-employment medical examinations and/or testing?

- **Best Practice**
  - Include a clause in the employment contract making employment conditional on satisfactory medical results.
  - Inform candidates early, ideally during the interview stage.
  - Candidates cannot be rejected solely for refusing a medical test.

What about Medical Examinations and Testing of Current Employees?

- **Legal Basis**
  - Article 9(2)(h) permits processing of special category data where it is necessary for assessing the working capacity of an employee.
  - Applies only to existing employees, not prospective candidates

- **Purpose of Examinations**
  - Must be limited to assessing fitness for work.
  - Aimed at determining whether the employee:
    - is capable of performing assigned duties, and
    - does not suffer from a condition preventing them from safely carrying out the role.

What about Medical Examinations and Testing of Current Employees?

- **Accountability Requirements**
  - The assessment and its outcome must be documented and retained.
  - Employers must demonstrate compliance under Article 5(2) GDPR.

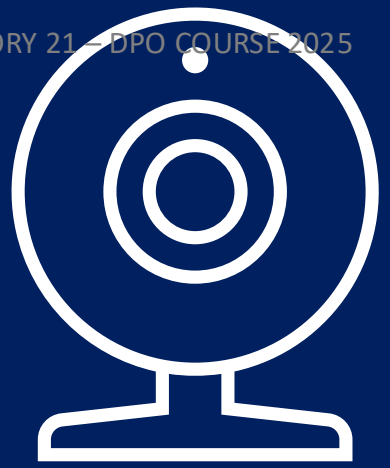
Additional Requirements For Medical Examinations

- **Keep in mind:**
  - Any such medical examinations/tests must be carried out by and under the responsibility of a healthcare professional in line with **Article 9(3)**.
  - They must only take place after the employment contract has been signed.
  - **Article 5(1)(c)** (Data Minimization) - the healthcare professional should not disclose any specific health conditions or diagnoses of the employee to the employer.
    - The employer should only be provided with a ‘fit’ or ‘not fit’ result regarding the health of the employee.

Monitoring Employees at the Workplace

- Monitoring must be justified by a legitimate purpose
- Employers must rely on a valid ground under Article 6 GDPR
- Employees must be clearly informed, in advance, of the scope and purpose of any monitoring,
- Monitoring of an employee's emails in the interest of ensuring business continuity must be carefully balanced against the individual's data protection rights under the GDPR. Such
- The parameters of any monitoring must be clearly set out in an internal policy
- Data Protection Impact Assessment (DPIA) when High risk

Webcams on a Company Device



Can an employer ask employees to switch on their webcams on the company device at any time during the workday?

Any proposed measure to monitor employees would have to be strictly **necessary** and **proportionate** when weighed against the purpose it intends to achieve.

The employer must consider what would be the **least invasive measure** that could achieve that objective (i.e., the measure that collect and processes only the minimum personal data necessary to address that risk).

Requiring an employee to keep their webcam switched on at all times or remotely accessing the employee's webcam throughout the workday involves **continuous video and/or audio surveillance.** It is highly invasive and intrusive.

By contrast, an employer may, depending on the particular context and circumstances, be able to identify a legal basis which justifies requesting the employee to enable their webcam where this is needed for **work-related interactions**.

Does the employer need to inform the employee that activity monitoring software has been installed on the company device?

Yes, the GDPR requires that the data subject, the employee, must be informed about the processing of his/her personal data, and this includes the use of activity monitoring software on company devices.

This is in line with the obligation of **transparency** imposed on the controller under the GDPR.

Additionally, employees must be given **clear information** about the processing that enables them to understand the purposes and extent of any monitoring that is being carried out.

Biometric Data

- **Legal Basis**
  - Biometric data is special category data under Article 9(1) GDPR.
  - Requires a valid condition under Article 9(2) for lawful processing.
  - Conditions are strict, reflecting the intrusive nature of biometric data

- **Necessity & Data Minimisation**
  - Processing must be genuinely necessary for the stated purpose.
  - Must show no less intrusive alternative exists.
  - Example: Using proximity cards or tokens instead of fingerprint/facial scans.

Biometric Data

- **Limited Justifications**
  - May be justified for roles involving classified information or high-security access.
  - Otherwise, explicit consent under Article 9(2)(a) may be the only viable ground, but consent must be freely given and withdrawable.

Managing Employee Email Accounts

Automatic Email Forwarding

- ❑ Generally not compliant with GDPR.
- ❑ May expose personal emails and cause unauthorised disclosure.
- ❑ Business continuity is a legitimate interest, but must be balanced with privacy rights.

Recommended Approach - Automatic Reply

Set an auto-reply stating:

- The employee has left the company.
- An alternative contact is provided.
- The account will remain active for a limited time

Managing Employee Email Accounts

The IDPC suggests a **one-month timeframe as a standard "reasonable period"** for the auto-replay to remain active.

- However, a slightly longer period can be justified where necessary, for example, if the employee held a critical role.
- In this case, organizations must be able to demonstrate that any extended period is necessary and proportionate.

Managing Employee Email Accounts

During Employment

Have a clear email management policy—communicated and signed by employees.

Encourage staff to separate personal and work emails (e.g., personal folder).

At Departure

Allow employees to retrieve or delete personal emails.

Set up the **auto-reply on the last working day .**

Consider archiving only if necessary for business continuity.

After Departure

No access to the former employee's mailbox.

No automatic forwarding or sending emails as the ex-employee.Respect data mi[illegible]

process only what's strictly necessary.

Handling DSARs in Sensitive HR Contexts

Employees have a right of access (Article 15 GDPR) to their personal data — including HR and disciplinary records.

Disclose only personal data relating to the requester.

Redact or exclude third-party data unless disclosure is lawful or fair.

Withhold legally privileged or confidential management material (e.g. internal deliberations).

Ensure secure transfer and audit trail of disclosures.Respond within 1 month (extendable to 3 months for complex cases).

Handle requests neutrally and respectfully - no retaliation or bias.

Communicate outcomes transparently, explaining withheld information.

Promote trust and fairness in disciplinary or grievance settings.

Assign a trained DPO/HR contact to review and document decisions.).

Storage Limitation/Right to be Forgotten

Retain data only for as long as necessary

It is the responsibility of the controller to ensure that the retention periods are justified and reasonable and are not longer than what is strictly necessary for the purpose for which it is processed.

IDPC guidelines:

Vacation leave records and sick leave records - where the law does not prescribe a retention timeframe – should be kept for a period it deems justifiable after making its own careful assessment - this could be **one to two years maximum**, provided that there are no disputes regarding the amount of leave days that have been taken and/or brought forward to the following year.

GDPR Compliance Practice for Employers

- Apply GDPR principles — lawfulness, fairness, transparency, minimisation, accountability
- Maintain clear privacy notices and regularly updated policies (Acceptable Use Policy, Data Protection, IT/Security, BYOD, Monitoring).
- Review use of employee data (including contracts of employment) & ways in which data is processed and stored
- Conduct Data Protection Impact Assessments (DPIAs) before introducing new systems or monitoring tools and inform the employees

GDPR Compliance Practice for Employers

- Implement proportionate monitoring only when necessary and to protect networks or prevent data leaks
- No monitoring of personal files
- Prefer lock certain websites as opposed to monitoring use.
- No continuous tracking of employees
- Provide training on data protection and reporting procedures for breaches.
- Keep records of processing, perform regular audits, and communicate compliance measures openly to build employee trust.

AI Systems Used in the Employment Sector

- **Extensive Data Processing**

AI systems in recruitment or workplace management often rely on large amounts of personal and sensitive data, including biometrics and behavioural information.

- **Imbalance of Power**

Employees' consent is rarely considered freely given, making it an unreliable legal basis for processing.

- **Opacity and Explainability**

Many AI tools operate as "black boxes", making it difficult for individuals to understand or contest automated decisions.

AI Systems Used in the Employment Sector

- **Automated Decision-Making**

Decisions taken without meaningful human input, such as in recruitment or performance assessment, may breach Article 22 GDPR.

- **Bias and Discrimination**

Algorithms can unintentionally replicate or reinforce existing inequalities.Workplace Surveillance: The use of monitoring and productivity tools raises serious concerns about proportionality and employee privacy.

- **Data Security and Retention**

Employers must safeguard collected data and avoid storing it longer than necessary..

AI Systems - GDPR Compliance Practice for Employers

- ❑ Define a Lawful Basis
- ❑ Maintain Human Oversight
- ❑ Carry Out DPIAs
- ❑ Transparency with Employees
- ❑ Data Minimisation
- ❑ Privacy and Fairness by Design
- ❑ Accountability

ANY QUESTIONS?

Erika Criscione (Attorney-at-Law) - email: erika.criscione@gvzh.mt
Ms. Hayley Ann Pisani - email: hayley.pisani@gvzh.mt
https://gvzh.mt/