Solving Privacy Paradox | KNOW YOUR RIGHTS AND OBLIGATIONS
SolPriPa 3

The „SolPriPa3“ project is partially funded by the European Union under the Citizens, Equality, Rights and Values (CERV) Programme 2021–2027.

The information provided in the project is solely that of the authors and does not necessarily reflect the position of the European Union or the European Commission. Neither the European Union nor the European Commission can be held responsible for it.

STATE DATA PROTECTION INSPECTORATE

TRACKING OF INDIVIDUALS (EMPLOYEES)

TRACKING MEANS USING TECHNOLOGY TO MONITOR A PERSON‘S LOCATION, ACTIVITIES OR BEHAVIOUR.

Tracking may involve:

- GPS tracking systems;
- video surveillance cameras;
- employee computer monitoring software;
- mobile applications;
- website cookies;
- access control systems.

TRACKING: WHAT IS ALLOWED, RESTRICTED AND PROHIBITED?

ALLOWED	RESTRICTED	PROHIBITED
GPS tracking of company vehicles.	Monitoring employees’ computer use.	Secret monitoring of employees.
Video surveillance for security purposes.	Monitoring internet browsing during working hours.	Video surveillance in changing rooms, rest areas or sanitary facilities.
Access cards used for working time recording.	Video surveillance in work areas.	Tracking employees outside working hours.
Website cookies used with the user’s consent.	Tracking employees’ location during working hours.	Tracking personal devices.

ASSESSING NECESSITY AND PROPORTIONALITY

Under the GDPR, any tracking or monitoring measure must comply with the principles of personal data protection.

Before introducing tracking, organisations should assess:

- whether there is a legitimate purpose;
- whether tracking is necessary to achieve that purpose;
- whether the measure is proportionate to the objective pursued;
- whether the same objective can be achieved through less privacy-intrusive measures.

REMEMBER
If the objective can be achieved through measures that interfere less with privacy, tracking should not be used.

INFORMING INDIVIDUALS

People must be informed about:

- who carries out the monitoring;
- why their personal data are being processed and on what legal basis;
- how long the data will be kept;
- what rights they have under the GDPR.

Clear information about the processing of personal data must be provided before or at the time the monitoring takes place.

PRIVACY AREAS

Monitoring must not take place in locations where people can reasonably expect a higher level of privacy, such as:

- toilets;
- changing rooms;
- staff rest areas;
- other private spaces.

EMPLOYEE MONITORING

Employers may monitor employees only in compliance with data protection requirements.

Employers must:

- inform employees about the processing of their personal data;
- clearly explain the purpose of the monitoring;
- ensure that the monitoring is necessary and proportionate.

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

In some cases, a Data Protection Impact Assessment (DPIA) may be required before introducing monitoring measures.

For example, a DPIA may be necessary when an organisation plans to carry out:

- employee video or audio monitoring;
- monitoring of employee communications;
- analysis of employee behaviour;
- employee location tracking.

REMEMBER

Monitoring people should never be excessive. Organisations must balance their legitimate interests with individuals' right to privacy and comply with the requirements of the GDPR.