Regulatory approaches in Europe

- Technological advances have raised the bar for legislators and policymakers in the EU and added a new layer of complexity to the regulation of monitoring and surveillance in the workplace.
- National legislation struggles to keep pace with technological advances and often does not account, sufficiently or at all, for employers' use of state-of the-art technologies for monitoring purposes.
- Employee monitoring is not addressed explicitly in EU legislation, but privacy and data protection rights that may be impinged upon by employee monitoring are.
- The most important piece of EU legislation in this regard is the General Data Protection Regulation (Regulation (EU) 2016/679), replacing Directive 95/46/EC – known as the GDPR.
- The GDPR entered into force in May 2018 and is applicable in all EU Member States.
- The GDPR regulates the collection, use and transfer of **personal data** and sets out provisions that apply to all **data-processing** operations, including employee monitoring.

Regulatory approaches in Europe

Several lawyers of European rules and regulations.

- Monitoring employees means a focus on the **GDPR**.

- Monitoring employees also means a focus on **Guidelines of the European Data Protection Board** (EDPB), for example:
  - Guidelines 04/2017 on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of the GDPR, adopted on 4 April 2017;
  - Guidelines 02/2020 on the European Essential Guarantees for surveillance measures, adopted 10 November 2020;
  - Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted 21 April 2020.

- Monitoring employees also means a focus on **case law of the European court**.

- Not only a focus on European rules and regulations, also a focus on **national rules and regulations** of an EU Member State.

Regulatory approaches in Europe

Several lawyers of national rules and regulations.

- Although the GDPR is applicable in all EU Member States, it is in the remit of each individual Member State to introduce specific provisions about the processing of employee data for a variety of purposes (article 88 GDPR).

- Besides the GDPR it is there of importance to also focus on (for example):
  - National regulatory frameworks (employment law, equal treatment legislation);
  - National Collective Bargaining Agreements;
  - National Data Protection Authorities (guidance, advice, decisions);
  - National courts (case law, precedents).

- In addition, also focus on:
  - Company handbooks, policies, regulation.

Regulatory approaches in Europe

Several lawyers of company rules and regulations.

- Nothing beats a good, clear policy about monitoring and surveillance.
- Policies (handbooks, guidelines, internal regulations) must be carefully tailored to show an organization's legitimate purpose behind the monitoring and what is acceptable or not.
- With a comprehensive and easily accessible workplace monitoring policy, employees will be aware of the monitoring.

Policies must include:

- the nature and extent of the monitoring and/or surveillance process;
- the reason for the monitoring and/or surveillance;
- the impact of the monitoring and/or surveillance on the business;
- how (if any is being processed) confidential or sensitive information is handled;
- point out and clarify acceptable and unacceptable uses;
- employers must ensure that their monitoring policies are compliant with legal requirements.

Q&A (monitoring)

Q: Is employee monitoring legal in the EU?
A: Yes

Additional remarks:

- employers in the EU in principle have the right to monitor employees at work;
- it is crucial to balance an employer's right to lawfully monitor and manage the work process and an employee's right to privacy;
- it is within the employee's right to be notified before any monitoring is carried out;
- consent is not always required and not the most solid justifying;
- the monitoring process must comply with the GDPR and possible additional (national) rules and regulations.

Q&A (phone conversations)

Q: Is it legal to monitor or record phone conversations?
A: Yes.

Additional remarks:

- under the GDPR, monitoring and recording phone conversations may be permitted under certain conditions. For example, if the party has given explicit consent or monitoring/recording is necessary to protect the employer's legitimate interests.
- a company with a works council must get permission from the works council before phone monitoring or recording is carried out. Employers intending to record telephone conversations are obliged to comply with this code.

Q&A (email)

Q: Is it legal to monitor private messages and email content?
A: Yes.

Employers are justified in controlling certain activities, such as sending or receiving private messages or emails, to ensure that employees perform their duties during working hours, particularly on the company device. The ECHR sets clear guidelines on the extent of how and when such monitoring is permitted. Businesses must develop policies that allow employees to know the extent of the monitoring. Private messages and emails fall within the category of personal data (as described in Article 4 of the GDPR). Therefore, organizations must prove that they have the legal basis to collect and monitor such information.

An employer may monitor email content received or sent on the company computer, provided that the information is not private, and the monitoring is justified on legitimate grounds. It is also crucial for businesses to distinguish between private and work-related emails. Conversely, employees should also avoid accessing personal emails on devices provided for professional purposes. To balance the monitoring of email content while respecting employees' privacy, employers should:

- ensure that the employee is aware of and has agreed to the monitoring;
- ensure that personal data collected or connected to the employee email accounts are not accessed, and where such situations arise, data should only be shared with their consent;
- ensure that they retain emails and delete them after the period is up.

Q&A (CCTV)

Q: Is it legal to use video monitoring systems in the workplace?
A: Yes.

- if there is a legitimate purpose for the surveillance (e.g., to protect persons/places);
- if the surveillance is appropriate for this purpose;
- if the monitoring is necessary and less intrusive;
- the monitoring must be reasonable, and employers must consider the employee's privacy rights.

Under the GDPR, employees must be notified of:

- the fact that they're being monitored, the purpose of monitoring, how long monitored data will be stored, who has access to the monitored data.

Under the GDPR, there are certain restrictions:

- monitoring in sensitive areas, such as restrooms, religious spaces, and break rooms, is prohibited.
- audio may not be recorded, since this is in principle not necessary to protect persons and/or places;
- it is in principle not allowed to use footage to assess the employees work.
- the use of hidden video surveillance is considered a violation of Article 8 ECHR and therefore only allowed under strict (additional) requirements.

Q&A (actions and precautions)

Q: What actions and precautions should an employer take in order to monitor an employee?
A: Several actions and precautions:

- Define the type of data that is being processed (general, or sensitive data).
- Focus on article 5, 6 (and 9) GDPR.

- Be aware that personal data of an employee needs to be:
  - processed lawfully, fairly and in a transparent manner (article 5 GDPR);
  - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (article 5 GDPR);
  - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (article 5 GDPR);
  - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (article 5 GDPR).

Q&A (actions and precautions)

- Be aware that personal data of an employee needs to be:
  - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (article 5 GDPR);
  - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (article 5 GDPR).

- Be aware that an employer needs to have a justification ground for processing the personal data of an employee (article 6 GDPR):
  - the employee has given consent to the processing of personal data for one or more specific purposes;
  - processing is necessary for the performance of the employment contract;
  - processing is necessary for compliance with a legal obligation to which the employer is subject;
  - processing is necessary for the purposes of the legitimate interests pursued by the employer.

- **Have a policy in place where articles 5 and 6 GDPR are properly addressed**.

Q&A (consent)

Q: Is consent of an employee a justification ground?
A: Not the most preferable justification ground.

- There is an imbalance of power in the employment context.
- Given the dependency that results from the employer/employee relationship, it is unlikely that the employee is able to deny its employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal.
- It is unlikely that an employee would be able to respond freely to a request for consent from its employer to, for example, activate monitoring systems such as camera observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent.
- The EDPB deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees due to the nature of the relationship between employer and employee.

Q&A (transfer)

Q: Can personal data of an employee be transferred to non-EU/third countries?
A: In principle yes.

- International transfers may take place when there is an adequate level of protection to the fundamental right of individuals (data subjects) to data protection. This is the case if there is/are:
  - an adequacy decision;
  - appropriate safeguards;
  - binding corporate rules (BCR);
  - specific exceptions.
- Adequacy assessments may be carried out by those wishing to transfer data outside the EEA themselves, or by the European Commission.
- The Commission has determined that several countries ensure an adequate level of protection by reason of their domestic law or of the international commitments they have entered into (adequacy decision).
- In the absence of an adequacy decision, it should be assessed whether the restricted transfer is subject to 'appropriate safeguards' in order to provide a sufficiently high level of protection (for example by adopting the EU Commission's 'Standard Contractual Clauses', or other binding safeguards authorized by the European Data Protection Board (EDPB).

Q&A (transfer)

Q: Can personal data of an employee be transferred to the US?
A: In principle yes.

- On 2 February 2016, the European Commission and the United States agreed on a framework for transatlantic data transfers: "the EU-U.S. Privacy Shield", which has led to the adoption of an adequacy decision by the European Commission, officially adopted on 12 July 2016, for transfers to U.S. organizations subscribing to the Privacy Shield.
- As a result of the judgement of the EU Court of Justice in the Schrems II-case (Case C-311/18), the EU-U.S. Privacy Shield is no longer a valid mechanism to transfer personal data from the EU to the US and organizations in the EU can no longer transfer personal data to the US on the basis of the Privacy Shield.
- This means that additional safeguards must be taken for transfers to the US (or other third counties). It will have to be considered on a case-by-case basis what measure or combination of measures is needed to properly protect personal data.
- For guidance: the European Data Protection Board (EDPB) adopted recommendations for complying with the GDPR requirements in relation to international transfers: “Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Adopted on 18 June 2021”.