Austria

Employee monitoring and surveillance

Phase	Labour Constitution Act (ArbVG)
Native name	Arbeitsverfassungsgesetz (ArbVG)
Type	Employee monitoring and surveillance
Added to database	24 October 2023
Access online	Click here to access online

Article

§ 96 ArbVG

Description

Video surveillance interferes with the fundamental rights to data protection and privacy. § 96 ArbVG regulates the necessity of the works council's consent when introducing control measures and technical systems for controlling employees, provided that these measures (systems) affect human dignity, in order for them to be legally effective. Without the conclusion of a corresponding work agreement, the use of such systems is against the law and the control devices must be removed by the employer.

Companies with works council

Control measures such as video surveillance at the workplace, GPS tracking of field staff or the recording of work performance by machines or work equipment, may only be used if the the owner of the company has reached a works agreement on the matter with works council. Otherwise, the control measure is against the law and the systems must be removed by the employer.

Companies without works council

In companies without a works council, such control measures may only be carried out with the consent of the individual employees. The consent should be given in writing and can be revoked at any time. It is possible to agree on a time limit.

For video surveillance to be possible, there must be a legitimate interest of the person responsible in the individual case that outweighs that of the person affected. In addition, the surveillance must also be proportionate in the individual case and no lesser measures may be possible.

Video surveillance does not have to be notified to the data protection authority, but it does have to be entered in the register of processing activities.

The General Data Protection Regulation explicitly states that persons whose personal data are processed must be informed about this. In addition, every employee has the right to information about the specific data held about him or her, about its origin, its links with other data and about any transfers.

Commentary

In practice, video surveillance can be applied if it is necessary to protect persons or property in the business due to violations of rights that have already occurred (e.g., theft or damage to property) or a particular potential danger inherent in the nature of the location. Such a potential danger is always assumed, for example, in the case of tobaco stores, jewelry stores and banks. Therefore these stores are allowed to install surveillance and do so.

Control measures that violate human dignity are absolutely inadmissible. Such measures include, for example, secret tapping of telephone conversations, surveillance cameras in washrooms or toilet facilities, body searches as a rule, the examination of private life, etc. Due to the technical circumstances, the monitoring of e-mail and Internet use not only allows access to the connection data, but usually also monitoring of the content (content of the e-mails and the www pages selected). This typically affects human dignity and leads to a duty of consent on the part of the works council or the employee. The duty of co-determination does not depend on whether the private use of the Internet and e-mail is permitted or not. It applies in any case. For example, recently, the city of Klagenfurt dismissed the municipal director Peter Jost with immediate effect because he had illegally monitored the e-mail correspondence of city employees.

Additional metadata

Cost covered by Not available

Involved actors other than national government	Trade union Works council National government Employer organisation
Involvement (others)	None
Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), Austria: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Belgium

Employee monitoring and surveillance

Phase	Protection of employees' privacy in relation to the monitoring of electronic online communication data
Native name	Bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische online communicatiegegevens
Type	Employee monitoring and surveillance
Added to database	04 October 2023
Access online	Click here to access online

Article

CAO 81 van 26 April 2002 ter Bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische online communicatiegegevens

Description

Collective Labour Agreement 81 arranges the monitoring of electronic communication data in the workplace in Belgium. It regulates the monitoring of all forms of electronic online communication data, regardless of the carrier, transmitted or received by employees in the course of their employment, both internally and externally.

Employers may carry out monitoring for four main reasons: * preventing defamatory acts and behaviours, * protecting business interests, * ensuring IT network system security, and * monitoring compliance with company rules. They may not violate the personal privacy of employees and must act proportionally, processing only necessary data.

In terms of transparency employers must provide detailed information about the monitoring system, including what is being monitored, why, the duration of monitoring, data storage, and whether monitoring is permanent. Rights, obligations, prohibitions, and sanctions must be communicated, both individually and collectively.

In case of violations, the employer must discuss the infringement with the offender, giving the employee the opportunity to justify their actions and prevent future violations.

CA 81 does not regulate how access to and the use of online communication tools in the company should be governed; this remains the responsibility of the employer.

The standards in CA 81 can be clarified, supplemented, and adapted to specific situations at the sector and/or company level.

Commentary

Since it is a National level collective agreement, all social partners had to formally agree with the CA before signing.

Additional metadata

Cost covered by	Not available
Involved actors other than national government	Trade union Employer organisation
Involvement (others)	None
Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), Belgium: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Cyprus

Employee monitoring and surveillance

Phase	The Processing of Personal Data (Protection of Individuals) Law of 2001 (138(I)/2001) (annulled); the Law on the Protection of Natural Persons Against the Processing of Personal Data and the Free Movement of such Data (125(I)/2018) of 2018
Native name	Ο Περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος του 2001 (138(I)/2001) (καταργημένος); Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018 (125(I)/2018) ()
Type	Employee monitoring and surveillance
Added to database	25 October 2023
Access online	Click here to access online

Article

Article 16 of the Processing of Personal Data (Protection of Individuals) Law of 2001 (138(I)/2001) (annulled).

Description

Until 2018 Cyprus had a law [the Processing of Personal Data (Protection of Individuals) Law] which included certain provisions regarding employment. However, this law was annulled in 2018, and replaced with a new one (the Law on the Protection of Natural Persons Against the Processing of Personal Data and the Free Movement of such Data), which made no reference to employment.

Commentary

Regarding this issue, during a relevant seminar organised by the Cyprus Bar Association and the Office of the Commissioner for Personal Data Protection of Cyprus, Cyprus'

Commissioner for Personal Data Protection stated that at present the matter is largely dependent upon the specific facts of each independent incident. Examined, as such, on a case-by case basis, the resolution of relevant issues in an employment relationship on the one hand requires compliance with national and European Union law, and on the other hand it is highly dependent on the discretion of the Commissioner.

Recognising the understandable confusion, the Commissioner provided the following guidelines, aiming to avoid any kind of violation of human rights and the law, while also to provide necessary information both to the employer as well as to the employee regarding their duties and rights respectively:

1) The company/employer should have a handbook referring to its established policy with exact precision on the regulation of data protection at the workplace and whether such company/employer allows the possibility to use their email account for personal or work use only.

2) In the cases where there is such an employment dispute/issue, it will be taken into account whether the employer is the owner of the computer and the email account while also whether the email account was solely used for work purposes. If a company's policy indicates clearly that any email accounts (in the workplace) shall be solely and strictly used for work purposes and that employees or use it for any other private purpose, then this will weigh in favour of the employer.

3) In cases where there are suspicions of criminal or unlawful use of the email, the employer has an obligation to inform the employee about accessing their email and in such a case the employee must be present. If the employee does not consent and/or approve such an act, then the employer may need to go to court in order to obtain a court order for accessing the email account.

Additional metadata

Cost covered by	Not available
Involved actors other than national government	Other
Involvement (others)	Office of the Commissioner for Personal Data Protection of Cyprus

Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), Cyprus: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Czechia

Employee monitoring and surveillance

Phase	Employee monitoring and surveillance
Native name	Monitorování a dohled nad zaměstnanci
Type	Employee monitoring and surveillance
Added to database	25 October 2023
Access online	Click here to access online

Article

Act No. 89/2012, Coll. Civil Code, §84 to §90 Act No. 262/2006, Coll. Labour Code, § 316 Act No. 101/2000, Coll. Law on Protection of Personal Data Act No. 251/2005, Coll. on labour inspection Charter of Fundamental Rights and Freedoms

Description

The protection of employee privacy is mainly regulated by the Civil Code (Act No. 89/2012 Coll.), and then the Labour Code (Act No. 262/2006 Coll.), which regulates the property interests of the employer and the protection of the basic personal rights of the employee. Privacy protection is also regulated by the Personal Data Protection Act (Act No. 101/2000 Coll.). The protection of correspondence is guaranteed by the Charter of Fundamental Rights and Freedoms. Provision § 316 of the Labour Code provides an exhaustive list of ways that the law considers to be violations of the privacy of employees. This includes open or covert monitoring, listening and recording of the employee's telephone calls, checking e-mail or checking letters addressed to the employee.

The mentioned methods of monitoring employees can be considered legal only if the employer has serious reasons for their implementation related to his activity. At the same time, in this case, the law imposes an obligation on the employer to inform the employee about the introduction of these measures. Other ways, not mentioned in the law, are not a violation of labour regulations, provided that the control is carried out for all employees in the same way and to a similar extent. e.g. monitoring the movement of a company vehicle via GPS is not an invasion of privacy.

Commentary

The State Labour Inspection Office (SUIP) is responsible for monitoring the violation of employees' privacy by wiretapping, recording telephone calls, checking e-mail or letters in the workplace. According to SÚIP's statement, the mentioned cases of privacy violations are not frequent in inspection practice and do not cause difficulties to recognise them. The use of camera systems, on the other hand, is more frequent and their application is very variable. The methodology of the Office for the Protection of Personal Data is used to determine which camera system meets legal requirements and which does not. This is a test of adequacy, which takes into account three points of view: suitability (if the chosen means will be capable of achieving the intended purpose - technical parameters and number of cameras, sufficient recording retention time, etc.), necessity (if it is not possible to ensure the intended purpose by others, objectively in a comparable way with the same or lesser interference with the protected values) and adequacy (whether the level of interference with the rights of employees is not disproportionate to the values that the employer protects with the camera system).

Based on the Annual Summary Report on the results of control actions for 2018, the office detected 39 cases, 40 cases in 2019, 97 cases in 2020, 26 cases in 2021 and 27 cases of violation of employee privacy in 2022.

The amendment to Act No. 251/2005 Coll., on labour inspection, which entered into force on July 29, 2017, allows the SUIP to fine employers for unreasonable interference with the privacy of employees according to § 316 of the Labour Code. SUIP can impose a penalty for violation of an employee's privacy up to CZK 1,000,000.

Additional metadata

Cost covered by	National government
Involved actors other than national government	National government
Involvement (others)	The State Labor Inspection Office (SUIP)
Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: no thresholds

Sources

Citation

Eurofound (2023), Czechia: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Denmark

Employee monitoring and surveillance

Phase	The Danish Act on TV-Surveillence (Consolidation Act no.182 of 24/02/2023)
Native name	Bekendtgørelse af lov om tv-overvågning (LBK nr 182 af 24/02/2023)
Type	Employee monitoring and surveillance
Added to database	20 December 2023
Access online	Click here to access online

Article

Bekendtgørelse af lov om tv-overvågning LBK nr 182 af 24/02/2023 (Especially §3 and §3A regarding surveillance at workplaces)

Description

This law (LBK nr 182 af 24/02/2023) regulates surveillance camera usage in Denmark and has been amended several times, most recently by Law No. 802 on June 9, 2020.

Regarding surveillance of employees at workplaces the law stipulates in §3 and §3a that: It is permissible for companies to monitor their employees, as long as they are notified of this. However, the purpose of the monitoring must not be to monitor the employees' efficiency, which is why it must only function preventively or to document break-ins, theft or the like.

Other key points of the law include:

General Prohibition on Private Surveillance: Private individuals are prohibited from conducting surveillance of public areas used for ordinary traffic, unless there is a legally specified exception.

Exceptions to the Prohibition: Certain exceptions permit surveillance of specific areas such as gas stations, factory premises, and other business areas, if conducted by the owner and

necessary for crime prevention.

Police Permissions: The police can grant permissions for residential areas, sports facilities, and other private or public entities to conduct surveillance for crime prevention purposes.

Municipal Authority for Surveillance: Municipalities can, after discussion with the police director, conduct surveillance to enhance safety in public places.

Registration of Surveillance Equipment: Private and public entities must register their surveillance cameras in the police register (POLCAM).

Information Duty: Entities conducting surveillance must provide clear information through signage or other means.

Data Protection Authority Oversight: The Data Protection Authority oversees the processing of personal data in connection with surveillance.

Penal Provisions: Violations of the law can be penalized with fines or imprisonment, and there are also provisions regarding the disclosure of recordings and data storage.

The law has been amended several times to adapt to developments and strengthen security and safety in society.

Commentary

.

Additional metadata

Cost covered by	Not available
Involved actors other than national government	Court National government
Involvement (others)	None
Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), Denmark: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Estonia

Employee monitoring and surveillance

Phase	Employment Contracts Act; Personal Data Protection Act
Native name	Töölepingu seadus; Isikuandmete kaitse seadus
Type	Employee monitoring and surveillance
Added to database	16 October 2023
Access online	Click here to access online

Article

Personal Data Protection Act Chapter 2 Employment Contracts Act Chapter 2, section 11 - data collection of a potential employment Employment Contracts Act Chapter 3, Division 2, section 28(2)11) - Employer's obligation to respect employee's privacy Employment Contracts Act Chapter 3, Division 2, section 41

Description

An employer will always possess an employee’s personal and work-related data, but there are regulations to the usage of that data. Trust and mutual understanding provides a foundation to a good employment relationship. This puts the principle of data processing with the knowledge of the employee in high importance. In legal terms, an employer must ensure the processing of personal data of an employee in accordance with the Personal Data Protection Act. Personal data are any data concerning an identified or identifiable natural person, regardless of the form or format in which such data exist.

The Employment Contracts Act obliges employers to respect employee privacy and control fulfilment of job tasks without unnecessary measures. Employers have the right to process employee data without employees' consent as long as it is necessary to fill employment contract and work arrangements rules at the workplace. This data however, must be collected only in legal and fair ways. At the same time, employees have the right to ask and receive information on what kind and on what purpose is information collected on them and who has access to that data (Personal Data Protection Act). An employee also has a right to demand a change or removal of false information collected about them. The data

of an employee can only be processed if they have been given an opportunity to give consent which can also be withdrawn at any moment. If an employee withdraws their consent, the employer has to stop processing that data.

In addition, the employer does not have the right to carry out couvert surveillance on their employees. If there are cameras used in the office, all employees need to have knowledge of that, which needs to be clear and unambiguous. In the case of privacy violation due to collection of data, the subject can demand compensation. Surveillance cameras can only be used for the protection of people and property, not for collecting data on the quality and quantity of the work carried out by the employees. The employer has no right to collect data of the employees outside of working hours and must provide access to the materials (including recordings) at all times if the employee finds it necessary.

However, if the employee uses computers or other devices provided by the workplace, the data collected from there can be used without consent, but this should be specifically mentioned in the work contract. Also, the employer has a right to prohibit the use of work computers or other devices for personal use but this should again be stated in the work contract.

Commentary

The processing and protection of an employee's private information has been the main area of concern for the Data Protection Inspectorate in Estonia. In the case of unavoidable data processing due to the contract or the law, the lines for asking for consent get very blurry. For example, processing data about an employee's child for childcare leave purposes does not require consent, even if the child is a minor. For further processing of the data related to the employee's children, consent is required.

In addition, due to increased demand for telework due to the COVID-19 pandemic, the relation to monitoring at work has also changed. In many cases the employers started to use extra monitoring tools for employees working from home to control their working activity and productivity. In most cases automatic, AI related tools were used, which is often failing to identify between personal and work-related data while collecting. Also, even though the pandemic has ended, many companies have continued to use the surveillance tools, which still leave ambiguous situations in relation to the Data Protection Act.

Overall, there is currently very little data collected on this topic in Estonia. In the case of privacy invasion or other guideline violation, the Labour Inspectorate should be contacted and they will look at every case separately.

Additional metadata

Cost covered by	Not available
Involved actors other than national government	Public employment service
Involvement (others)	None
Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), Estonia: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Finland

Employee monitoring and surveillance

Phase	The Employment Contracts Act (55/2001), Act on the Protection of Privacy in Working Life (759/2004), Occupational Safety and Health Act (738/2002), Co-operation Act (1333/2021)
Native name	Työsopimuslaki (55/2001), Laki yksityisyyden suojasta työelämässä (759/2004), Työturvallisuuslaki (738/2002), Yhteistoimintalaki (1333/2021)
Type	Employee monitoring and surveillance
Added to database	17 October 2023
Access online	Click here to access online

Article

- The Employment Contracts Act (55/2001) - Act on the Protection of Privacy in Working Life (759/2004): articles 4, 16, 17, 18, 19, 20, 21. - Occupational Safety and Health Act (738/2002): articles 27, 63. - Co-operation Act (1333/2021): section 12.

Description

The Finnish Act on the Protection of Privacy in Working Life (759/2004) is the most important Finnish legislation related to the processing of employees' personal data. According to this act, employers may operate camera surveillance at workplaces only for the purpose of ensuring the personal security of employees and other persons on the premises, protecting property or supervising the proper operation of production processes, and for preventing or investigating situations that endanger safety, property or the production process. The data collected through surveillance must be necessary for the employment relationship, protection of property, and ensuring the safety of employees and other persons on the premises.

Regarding electronic surveillance, employers are allowed to monitor their employees' use of e-mail and the Internet, but only under certain prerequisites. The article does not provide specific details on these prerequisites, but it does mention that the monitoring

must be necessary for the employment relationship and that the employer must inform the employees of the monitoring.

In short, the so called 'right to manage' gives the employer the right to decide who does what, where, when and how, during work hours. This includes surveillance of employees' work. The right is however limited by employment agreements, collective agreements and other labour legislation. The protection of an employee's personal data, as well as video surveillance, is regulated in the Act on the Protection of Privacy in Working Life (759/2004). According to the Occupational Safety and Health Act (738/2002), employers must constantly monitor the working environment, the state of the work community and the safety of working practices.

The collection of personal data during recruitment and employment is also subject to regulation under the Co-operation Act (1333/2021), according to which it needs to be included in workplace dialogue. This includes the purpose and methods of surveillance by technical means of employees, the use data networks and the processing of employees' e-mail and other electronic communications.

Commentary

Compliance with the law on Occupational Safety and Health Act is monitored by labor protection authorities, which is the relevant region's Regional State Administrative Agency.

Compliance with the Act on the Protection of Privacy in Working Life is supervised by the occupational safety and health authorities in accordance with their competence, together with the Data Protection Ombudsman.

Occupational health and safety authorities monitor compliance with The Employment Contracts Act. In their supervisory role and, in particular, when monitoring the observance of general binding collective agreements, the labor protection authorities must work in close cooperation with the employers' and employees' associations whose provisions of the general binding collective agreements entered into by the employers must be complied with according to Chapter 2, Section 7.

Additional metadata

Cost covered by	Not available

Involved actors other than national government	National government Employer organisation Trade union
Involvement (others)	None
Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No thresholds are set in the legislation: the regulations apply to all companies regardless of their size.

Sources

Citation

Eurofound (2023), Finland: Employee monitoring and surveillance, Restructuring legislation database, Dublin

France

Employee monitoring and surveillance

Phase	Employee monitoring
Native name	Surveillance des salariés
Type	Employee monitoring and surveillance
Added to database	01 November 2023
Access online	Click here to access online

Article

Labour code, article L2312-38 (informing staff representatives) Labour code, articles L1221-9 to L1222-4 (individual information to employees) Labour code, article L1121-1 (principle of proportionality) Internal Security Code, L223-1 et seq (fight against terrorism) Internal Security Code, L251-1 et seq., when the cameras are filming places open to the publicLoi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 104 Civil code, article 9 (Respect for privacy) Penal code, article 226-1 (recording of a person's image without their knowledge in a private place) Penal code, article 226-18 (unfair or unlawful collection) Penal code, article 226-20 (excessive storage time) Penal code, article 226-21 (misuse of the system) Penal code, article R625-10 (failure to inform persons)

Description

There is no specific legislation governing the surveillance of employees, but rather a set of rules derived from several pieces of legislation.

Surveillance cameras

Employers may not install cameras on their premises without defining a purpose, which must be legal and legitimate. For example, cameras can be installed in the workplace to ensure the safety of people and property, as a deterrent or to identify the perpetrators of theft, damage or assault. The employer's right of surveillance is recognised, but is subject to certain limits: * Respect for employees' individual rights and freedoms, which do not disappear within the company; * transparency: in principle, employees must be informed

of the monitoring system, and the social and economic committee or works council must be consulted; * compliance with the principles laid down by the GDPR; * the proportionality requirement: the control must be justified by a legitimate interest (productivity, security, company image, etc.) and must not be excessive.

Geolocation devices

These devices can be installed in vehicles used by employees to: * Monitor, justify and invoice the transport of people, goods or services directly linked to the use of the vehicle. * Ensure the safety of the employee, the goods or the vehicles in their charge, and in particular to recover the vehicle in the event of theft (for example, with an inert device that can be activated remotely as soon as the theft is reported). * Better allocation of resources for services to be provided in dispersed locations, particularly for emergency interventions. * Optionally, monitor working hours when this cannot be done by any other means. * Comply with a legal or regulatory obligation requiring the use of a geolocation system due to the type of transport or the nature of the goods being transported. * To monitor compliance with the rules governing the use of the vehicle.

However, a geolocation device installed in a vehicle made available to an employee may not be used: * to monitor compliance with speed limits. * to monitor an employee at all times. * In particular, it may not be used: in the vehicle of an employee who is free to organise his or her movements; to monitor the movements of employee representatives in the context of their mandate; to collect location data outside working hours, including to combat theft or check compliance with the conditions of use of the vehicle; * to calculate employees' working hours when another system already exists.

Video recording or screen capture coupled with telephone conversation recording

For the purposes of staff training or appraisal, employers may couple computer actions with telephone conversations, for example by recording the image of what appears on the employee's computer screen, in the form of screen captures or a video, at the same time as recording telephone conversations.

However, the use of this device can lead to employees being monitored or to private information being captured (personal emails, instant messaging conversations or confidential passwords). It is particularly intrusive and must therefore be strictly supervised. In principle, screen captures cannot be used in conjunction with recordings of telephone conversations. The CNIL considers that, whatever the purpose, a screen capture is likely to be neither relevant nor proportionate, since it is a frozen image of an isolated action by the employee, which does not faithfully reflect his or her work. There may be a link between the recording of telephone conversations and video recording of the screen, under certain conditions. In view of the impact and risks of misuse and surveillance

associated with these devices, the coupling of telephone recordings with the image (screen capture or video) of the employee's actions is disproportionate when used for purposes other than training, such as staff appraisal, combating internal fraud, etc. The employer must then use alternative means to this type of device.

Access to an employee's email in their absence

In order to avoid infringing employees' privacy, as they may make private use of their email, which is not prohibited, the employer must set the conditions for consulting email while they are absent. These rules may, for example, be set out in an IT charter specific to the company: they must be known by the employees, who will be informed of the terms and conditions for consulting and using their email during their absence. In this way, the rules laid down in advance, in complete transparency, can avoid the risk of subsequent disputes. The courts consider that any message received or sent from the workstation provided by the employer is, in principle, of a professional nature. In this case, the employer may consult them. However, if the message is clearly identified as personal, for example if the subject line clearly states that it is a private or personal message, the employer must not look at it. He must respect the confidentiality of correspondence

Commentary

A survey (https://www.softwareadvice.fr/blog/3625/controle-de-l-activite-des-salaries-avis-employeurs-managers) by Software Advice, carried out among 239 managers and company directors in April 2023 and entitled "Nearly 7 out of 10 companies want to continue investing in employee monitoring tools", reveals that, contrary to popular belief, the Covid-19 pandemic is not the origin of workplace monitoring tools. "In fact, 36% of the professionals questioned were doing so before the pandemic, whereas today 63% are doing so". Companies' relative confidence in their employees, therefore, is largely based on the very presence of employees at work. "More than a third (35%) mainly monitor employee presence (whether they are online or offline, or active or inactive)", the study reveals. Of the managers and business leaders surveyed, 27% monitor time management, 23% monitor IT activity (Internet access, searches carried out, etc.) and 21% monitor workload management.

Additional metadata

Cost covered by None

Involved actors other than national government	Works council
Involvement (others)	Commission nationale de l'informatique et des libertés - CNIL. The CNIL is an independent administrative authority responsible for overseeing the protection of personal data contained in computer files and processing, both public and private, including at the workplace.
Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), France: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Germany

Employee monitoring and surveillance

Phase	Use of technical devices to monitor employees
Native name	Einführung und Anwendung von technischen Einrichtungen zur Überwachung von Arbeitnehmenden
Type	Employee monitoring and surveillance
Added to database	09 October 2023
Access online	Click here to access online

Article

Works Constitution Act: Section 87 (1) 6., (2) Federal Data Protection Act: Section 26 (1) - (8) Telecommunications-Telemedia Data Protection Act: Paragraph 3

Description

The Works Constitution Act in its revised version of 1972 foresees co-determination rights for works councils on a number of issues in so far as they are not prescribed by legislation or collective agreement. Among others, works councils have a right of co-determination regarding the introduction and use of technical devices designed to monitor the behaviour or performance of the employees. This normally takes the form of a written agrreement between the employer and the works council. If no agreement can be reached, a conciliation committee makes a decision.

Commentary

This right to co-determination is, at least in form, comprehensive, as almost all digital technologies collect data and are therefore suitable for monitoring employees. Further, related rights of works councils concern - among others - the right to be informed and consulted in due time in case of any plans regarding technical plants as well as operations including the use of artificial intelligence (Section 90 of the Works Constitution Act).

According to the Federal Data Protection Act, the personal data of employees may be processed for employment-related purposes insofar this is necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract or to exercise rights and obligations of employees' representation laid down by law or by collective agreements or other agreements between the employer and staff council. Employees' personal data may be processed to detect crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the processing of such data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason. If personal data of employees is processed on the basis of consent, then the employee's level of dependence in the employment relationship and the circumstances under which consent was given shall be taken into account in assessing whether such consent was freely given (Section 26 of the Federal Data Protection Act).

Also for employees the principle of telecommunications secrecy for private communication according to the Telecommunications Telemedia Data Protection Act applies at the workplace (Paragraph 3 of the Telecommunications Telemedia Data Protection Act).

Additional metadata

Cost covered by	Employer
Involved actors other than national government	Works council
Involvement (others)	None
Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), Germany: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Greece

Employee monitoring and surveillance

Phase

-Law 4808/2021 (Official Government Gazette A’ 101/19.06.2021), "For Labour Protection - Establishment of an Independent Authority 'Labour Inspection' - Ratification of Convention 190 of the International Labour Organization on the Elimination of Violence and Harassment in the World of Work - Ratification of Convention 187 of the International Labour Organization on the Framework for the Promotion of Safety and Health at Work - Incorporation of Directive (EU) 2019/1158 of the European Parliament and of the Council of 20 June 2019 on the balance between professional and private life, other provisions of the Ministry of Labour and Social Affairs and other urgent regulations", as amended by Law 5053/2023 (Official Government Gazette A' 158/26.09.2023), "To strengthen work - Integration of Directive (EU) 2019/1152 of the European Parliament and of the Council of 20 June 2019 - Simplification of digital processes and strengthening of the Work Card - Upgrading the operational function of the Ministry of Labour and Social Security and the Labour Inspectorate"

Native name	-Νόμος 4808/2021 (ΦΕΚ Α' 101/19.06.2021), "Για την Προστασία της Εργασίας - Σύσταση Ανεξάρτητης Αρχής «Επιθεώρηση Εργασίας» - Κύρωση της Σύμβασης 190 της Διεθνούς Οργάνωσης Εργασίας για την εξάλειψη της βίας και παρενόχλησης στον κόσμο της εργασίας - Κύρωση της Σύμβασης 187 της Διεθνούς Οργάνωσης Εργασίας για το Πλαίσιο Προώθησης της Ασφάλειας και της Υγείας στην Εργασία - Ενσωμάτωση της Οδηγίας (ΕΕ) 2019/1158 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Ιουνίου 2019 για την ισορροπία μεταξύ της επαγγελματικής και της ιδιωτικής ζωής, άλλες διατάξεις του Υπουργείου Εργασίας και Κοινωνικών Υποθέσεων και λοιπές επείγουσες ρυθμίσεις", όπως τροποποιήθηκε από το Νόμο 5053/2023 (ΦΕΚ Α' 158.09.2023), "Για την ενίσχυση της εργασίας - Ενσωμάτωση της Οδηγίας (ΕΕ) 2019/1152 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Ιουνίου 2019 - Απλοποίηση ψηφιακών διαδικασιών και ενίσχυση της Κάρτας Εργασίας - Αναβάθμιση της επιχειρησιακής λειτουργίας του Υπουργείου Εργασίας και Κοινωνικής Ασφάλισης και της Επιθεώρησης Εργασίας"
Type	Employee monitoring and surveillance
Added to database	25 October 2023
Access online	Click here to access online

Article

-Law 4808/2021, Chapter B: 'Contemporary Types of Work', Article 67, para 8: 'Provisions on Telework', Chapter C: 'Provisions related to the “Ergani II” Information System', Article 73: 'Purpose and Operation', Article 74: 'Digital Employment Card'

Description

By virtue of art. 67, para 8, Law 4808/2021: * The employer monitors the employee's performance in a manner that respects his privacy and is in line with the protection of personal data. Employers are explicitly prohibited from monitoring the performance of teleworkers with the use of webcams. By virtue of articles 73 & 74: * Employers are obliged

to install and operate an electronic system, for the monitoring of their employees' working time, directly connected and inter-operable to the "ERGANI II" Digital Information platform (Ministry of Labour & Social Affairs). Additionally, the new Law introduces the "digital employment card", which provides, in real-time, data to the "ERGANI II" platform such as, starting and ending working time, breaks, overtime and any type of leave.

On 4 August, 2021 the Greek Data Protection Authority (DPA) issued its Guidelines 1/2021 on the protection of personal data in the context of teleworking; the teleworkers' monitoring is of pivotal importance for the Authority. The DPA recognises the right of the employer, as long as the conditions deriving from the legislation are met in principle, to monitor whether employees provide their work within the agreed working hours, and in line with the terms of employment. It considers, also, legitimate for the data controller to request additional confirmation (authentication) from the ICT user-teleworker (PC, communication software - electronic mail) - assuming that they actually provide the agreed work and keep the relevant information.

On the other hand, the DPA has judged with a series of decisions that, the ongoing surveillance of employees by means of web cams, software recognising images and movements, the shared use of the employees' screen, the installation and operation of a Keylogger, or even the performance of certain activities on a regular basis for ascertaining that the employees are teleworking, are prohibited practices, because they lead to an unjustified profiling of employees and violate the proportionality principle. In addition to the prohibitions set in relation to the use of a camera (web cam) to control the performance of the employee, the controller in the context of their responsibility should take into account that the processing of data through closed-circuit visual recording within workplaces, whether publicly accessible or not, is permitted only if it is necessary for the protection of persons and property. Data collected through closed-circuit visual recording may not be used as a criterion for evaluating employees' efficiency. In addition, the legality of taking any such relevant measure, that constitutes processing of personal data, presupposes the prior notification of the data subject.

Commentary

One of the most important regulations in Law 4808/2021 is that, for the first time, the 'right to disconnect' is regulated, which essentially consists in the self-evident observance of the schedule. It is defined as the right of the teleworker to abstain completely from the provision of his work and, in particular, not to communicate digitally and not to respond to phone calls, emails or any form of communication outside of working hours and during his legal holidays.

Unfavourable discrimination of the teleworker due to the exercise of the right to disconnection is not allowed. The employer must identify technical and organizational means to satisfy the right to disconnection. These means are recorded in an individual or collective agreement or disclosed by the employer to all employees. In addition, the Greek Data Protection Authority (DPA) responding, in a timely manner, to the extensive remote working during the COVID-19 pandemic, the issuance of Law 4808/2021 that, among others, regulates telework, and the risks lurking for employees' privacy through the use of information and communication technologies, issued its Guidelines 1/2021 on the protection of personal data in the context of teleworking; the employers' right to control their employees' performance, without circumventing the employees' individual and labour rights, is of pivotal importance to DPA and, as such, is extensively analysed.

It remains to be seen how it will be possible to exercise control -monitoring and surveillance of the employees' performance, without violating personal data requirements.

Additional metadata

Cost covered by	None
Involved actors other than national government	Trade union Other Works council National government
Involvement (others)	Labour Inspectorate, Hellenic Authority for Communication Security and Privacy, Hellenic Data Protection Authority
Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), Greece: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Hungary

Employee monitoring and surveillance

Phase	Act I of 2012 on the Labour Code
Native name	2012. évi I. törvény a Munka Törvénykönyvéről
Type	Employee monitoring and surveillance
Added to database	27 October 2023
Access online	Click here to access online

Article

Article 11(a)

Description

Under changes introduced in April 2019 to the Labour Code, providing more details on the rules on monitoring and surveillance, it is stated that the employer has a right to monitor whether employees are fulfilling their job-related tasks according to their instructions.

The employer may use technical equipment to exercise this right, but it must be justifiably in connection with the employee's work and it must be proportionate. Such justification may be the protection of employer property, but surveillance cannot be used to measure employee productivity (for example by video surveillance). An exception may be when the surveillance serves the purpose of the health and safety of the employee, such as at an industrial site. Human dignity must be observed at all times, thus cameras cannot be placed in private spaces where the employee has the right to privacy and rest (showers and dressing rooms, kitchens or dining spaces, facilities for resting).

General GDPR rules must be observed when handling all data collected in this way and employees must be duly notified of any surveillance beforehand.

Commentary

The Hungarian National Authority for Data Protection and Freedom of Information (NAIH) is authorised to impose fines for breaches of these rules. The largest fine related to data protection imposed in 2022 was HUF 250 million (€658,000). This case was related to the data handling and analysis of Budapest Bank related to recordings of telephone calls received by its call centre between May 2018 and September 2021. NAIH found it especially problematic that the analysis of the calls included examining the emotional states and reactions of participants in the call, which is in breach of handling data of clients as well as employees and rules on obtaining informed consent.

Additional metadata

Cost covered by	Not available
Involved actors other than national government	Other
Involvement (others)	Hungarian National Authority for Data Protection and Freedom of Information (NAIH)
Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), Hungary: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Italy

Employee monitoring and surveillance

Phase	Law 300/1970, Art. 4; Legislative Decree No. 152 of 26 May 1997, Implementation of Directive 91/533/EEC on an employer's obligation to inform employees of the conditions applicable to the contract or employment relationship; Privacy Code (legislative decree 196/2003), amended by legislative decree 101/2018, Legislative Decree No. 104 of 27 June 2022, Implementation of Directive (EU) 2019/1152 of the European Parliament and of the Council of 20 June 2019 on transparent and predictable working conditions in the European Union; Decree-Law No. 48 of 4 May 2023, on urgent measures for social inclusion and access to employment.
Native name	Legge 300 del 1970, Art. 4; Decreto Legislativo 26 maggio 1997, n. 152, Attuazione della direttiva 91/533/CEE concernente l'obbligo del datore di lavoro di informare il lavoratore delle condizioni applicabili al contratto o al rapporto di lavoro; Codice della Privacy (decreto legislativo 196/2003), modificato dal decreto legislativo 101/2018; Decreto Legislativo 27 giugno 2022, n. 104, Attuazione della direttiva (UE) 2019/1152 del Parlamento europeo e del Consiglio del 20 giugno 2019, relativa a condizioni di lavoro trasparenti e prevedibili nell'Unione europea; Decreto-legge 4 maggio 2023, n. 48, recante misure urgenti per l'inclusione sociale e l'accesso al mondo del lavoro.
Type	Employee monitoring and surveillance
Added to database	09 October 2023
Access online	Click here to access online

Article

Law 300/1970, Art. 4 Legislative Decree No. 152 of 26 May 1997, Art 1 Privacy Code (legislative decree 196/2003), amended by legislative decree 101/2018 Legislative Decree No. 104 of 27 June 2022 Law No. 48 of 4 May 2023, Art 26

Description

Legal framework ensures a balance between operational needs of employers and the privacy and rights of employees: the Workers' Statute (Law 300/70) sets the foundation by prohibiting audiovisual and remote monitoring systems unless there's an agreement with trade union representatives.

Employers are also bound by a comprehensive obligation to inform employees about various aspects of their employment, including the use of any monitoring systems (detailed in Legislative Decree No. 152/1997 and further elaborated in Legislative Decree No. 104/2022). The Privacy Code, as amended by Legislative Decree 101/2018, reinforces these principles by requiring a solid legal basis, such as collective agreements or administrative authorizations, for the implementation of monitoring systems. It also mandates strict adherence to data protection laws, ensuring that any data collection is relevant, limited, and respects the privacy rights of individuals.

Furthermore, recent legislative developments, such as Law No. 48/2023, introduce additional layers of employee protection, including requirements for employers to provide or make accessible collective contracts, company rules, and information about automated decision-making systems used in the workplace, unless exempted due to industrial or commercial secrecy.

Commentary

The main Italian trade unions (CGIL, CISL and UIL) have clear positions regarding the monitoring and surveillance of employees. They emphasise the importance of oversight to reduce risks, accidents, and occupational diseases. They promote access to new digital technologies, workers' participation in company management, and continuous training. The common goal is to ensure the health and safety of workers, respecting their rights and actively involving them in company management.

Additional metadata

Cost covered by	Employer
Involved actors other than national government	Trade union
Involvement (others)	None

Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), Italy: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Lithuania

Employee monitoring and surveillance

Phase	Labour Code of the Republic of Lithuania
Native name	Lietuvos Respublikos darbo kodeksas
Type	Employee monitoring and surveillance
Added to database	29 October 2023
Access online	Click here to access online

Article

Article 27 of the Labour Code

Description

Handling of employee health data following amendments to the Labour Code on quarantine, 14th, April 2020, Article 27 of the Labour Code "Workers' rights to privacy and protection of personal data" establishes employer's obligation to respect the rights of workers to privacy and protection of personal data. The employer's exercise of ownership or control over information and electronic communication technologies used in the workplace shall not violate the confidentiality of employees' private communications. Moreover, the State Data Protection Inspectorate has issued a series of recommendations and guidelines on the protection of personal data in the context of employment relationships that are applicable together with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (and Lithuanian legislation:

Guidance for employees, 2023;

3. Guidelines for small and medium-sized businesses, 2023;
4. Guidelines for public sector bodies and organisations, 2023;

5. Recommendation on the safe use of mobile applications on mobile devices, 15th June, 2023;
6. Handling of employee health data following amendments to the Labour Code on quarantine, 14th, April, 2020;
7. Processing of employees' personal data in the context of teleworking, 9th April, 2020;
8. Guidance: Adaptive and Standardised Data Protection in the Life Cycle of an Information System, 11th December, 2020;
9. Memo on video surveillance requirements, 2019.

Commentary

2021-2023 The State Data Protection Inspectorate together with Mykolas Romeris University is implementing the "SolPriPa 2 WORK" project "Resolving privacy paradox 2: promoting high standards of data protection as a fundamental right in the workplace". The two-year project is partially financed by the European Union Rights, Equality and Citizenship Program (2014-2020). This is a project to increase the awareness of employers and employees about the protection of personal data in the context of labour relations.

Project goals: 1. Give employers the opportunity to create a work environment that meets the principles of personal data processing. 2. Help employees defend their right to personal data protection as a fundamental right in the workplace.

Target audiences are employees who are the weaker party in labour relations, and employers, especially specialists such as data protection officers, personnel, communication, information technology specialists, other administration employees. During the project, great attention is paid to small and medium-sized businesses, as well as public sector organisations, such as ministries and their subordinate institutions, municipalities, courts.

Activities. During the implementation of the project, trainings are conducted, guidelines, scientific articles, podcasts are prepared, and the mobile application "ADA guide" is further developed. The SolPriPa 2 WORK project is partially financed by the European Union Rights, Equality and Citizenship Program (2014-2020) and is for the period 2018-2020 continuation of the implemented awareness raising project "SolPriPa" about personal data protection.

Additional metadata

Cost covered by Not available

Involved actors other than national government	Employer organisation National government Court
Involvement (others)	None
Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), Lithuania: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Luxembourg

Employee monitoring and surveillance

Phase	Labour code
Native name	Code du travail
Type	Employee monitoring and surveillance
Added to database	21 April 2024
Access online	Click here to access online

Article

L 261-1

Description

The legislator exercised the option to the Member States by Article 88 of the GDPR to provide for more specific rules concerning the processing of personal data for employee surveillance purposes under employment relationships.

The processing of personal data by the employer for surveillance purposes is therefore authorized: If it is necessary:

- for the performance of the contract of employment;
- for compliance with a statutory obligation of the employer;
- for legitimate interests pursued by the employer or by a third party, unless the employee's interests or fundamental rights and freedoms prevail over the former;
- for the safeguarding of the vital interests of the employee or another natural person;
- for carrying out a mission that is in the public interest or relevant for the exercise of public authority vested in the employer; Or if the person concerned has consented to the processing of his or her personal data.

In addition to an individual right of access to information for each employee by virtue of Articles 13 and 14 of the GDPR, the employer must also inform the staff delegation or, otherwise, the Inspectorate of Labour and Mines. The information must include the

following elements: * A detailed description of the purpose of the proposed processing; * The implementation methods of the surveillance system and, where applicable, the period of and criteria for data retention; * The employer's formal commitment not to use the data collected for a purpose other than that provided explicitly in the prior information.

Commentary

No more information available.

Additional metadata

Cost covered by	Not available
Involved actors other than national government	None
Involvement (others)	None
Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2024), Luxembourg: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Malta

Employee monitoring and surveillance

Phase	Cap. 586 - Data Protection Act
Native name	Kap. 586 - Att dwar il-Protezzjoni u l-Privatezza tad-Data
Type	Employee monitoring and surveillance
Added to database	11 October 2023
Access online	Click here to access online

Article

Data Protection Act (Act XX of 2018, Chapter 586 of the Laws of Malta); Articles 32 and 41 of the Constitution of Malta (1964)

Description

There is no law specifically on employee monitoring in Malta. It therefore falls under the Data Protection Act (Act XX of 2018, implementing the GDPR, Regulation (EU) 2016/679), with privacy also being constitutionally protected. The employee's consent is not usually considered sufficient justification for employee monitoring, because the power imbalance in the employer-employee relationship compromises the employee's ability to freely grant such consent. A Data Protection Impact Assessment is required for employee monitoring, including for purposes of evaluating the employee's performance at work; if risks to the 'rights and freedoms of data subjects' (GDPR, Art. 35) remain in the processing operation, the Information and Data Protection Commissioner must be consulted.

Disputes relating to dismissals on the basis of claimed breaches of privacy have come before the Industrial Tribunal. The responsibility for monitoring and enforcing the GDPR and the Data Protection Act lies with the Office of the Information and Data Protection Commissioner (IDPC), as the national supervisory authority and regulatory body. The Information and Data Protection Appeals Tribunal decides cases relating to the monitoring of employees and the use of employees' personal data, and hears appeals from the decisions of the Office of the Information and Data Protection Commissioner.

Under Article 20 of the Data Protection Act, the IDPC may impose an administrative fine for violations, by order in writing.

Commentary

The decision usually involves a balancing of the employer's legitimate interest and the employee's right to privacy. For example, IDPC's Data Protection Guidelines for Banks (2018) specify (in line with Article 29 of the Data Protection Working Party's Opinion 2/2017, adopted 8 June 2017), that employers should consider whether any processing operation in relation to employees' use of technologies is: necessary; fair; proportionate; and transparent (p. 10).

In August 2019, the bank HSBC was fined €5000 by the IDPC, in a case where a bank employee's personal data was being monitored. HSBC had investigated the employee's bank account and social media posts without the employee's consent and without notifying the employee, to find out whether the employee (an active trade unionist) was receiving another salary for part-time work, which they suspected was being undertaken in breach of the conditions set out by the bank. The Information and Data Protection Commissioner found in favour of the employee in relation to the scrutiny of his bank account, noting that the bank had abused its position of power and access, and saying that the access 'exceeded what would generally be expected in the conduct of a relationship between a bank and an account holder.' The processing was found to be outside lawful grounds, and the purpose for which the data was accessed was found to be in violation of the Data Protection Act. No violation was found in relation to the monitoring of social media posts, since these were available to the group and the bank was found to have a legitimate interest in them, because of disputes between the employee and the bank that were ongoing at the time (Agius, 2019).

Additional metadata

Cost covered by	None
Involved actors other than national government	Employer organisation
Involvement (others)	None

Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), Malta: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Netherlands

Employee monitoring and surveillance

Phase	Work Council Act/ General Data protection regulation/ GDPR implementation act
Native name	Wet op de ondernemingsraden (WOR)/ Algemeen verordening gegevensbescherming (AVG)/ Uitvoeringswet AVG (UAVG)
Type	Employee monitoring and surveillance
Added to database	18 October 2023
Access online	Click here to access online

Article

Wet op de Ondernemingsraden (WOR) , Article 27(1)(k)(l)

Description

An employer is only allowed to monitor employees if it meets the requirements of the GDPR, as well as the law implementing the GDPR. Whenever an employer monitors their employees, the employees' privacy must be protected at all times. If there are alternatives to employee monitoring, or less invasive methods for the employees' privacy, those must take precedence. In general, the employee must give their explicit informed consent for the employer to be allowed to monitor their data, however, there are exceptions to this rule. There are also instances where employee monitoring is never admissible, for example in sensitive spaces, such as toilets and religious spaces.

The GDPR requirements for employee monitoring are as follows:

- Legitimate interest: the company must have a legitimate interest in monitoring its staff. This interest must outweigh the rights and interests of its employees. Such as their right to privacy. The company must be able to substantiate this. It must comply with the principles of proportionality and subsidiarity.
- Need: monitoring staff must be a necessity. This means that the company cannot achieve its goal in another way that is less drastic for its employees' privacy.

- Inform staff: the company must inform its employees about:
- what is allowed and what is not;
- that control is possible;
- why and when to check;
- how to check;
- which data is involved.

Employees can be informed with internal guidelines, such as rules of conduct or a protocol. * Right to confidential communications: employees' right to confidential communication must be considered. For example, when checking e-mail or telephone. * Works council approval: if the organisation has a works council, then the company must request the prior approval of the Works Council for a scheme for the inspection of personnel. If the Works Council does not agree, you are not allowed to inspect. * Data protection impact assessment: if a company wants to use large-scale processing and/or systematic monitoring of personal data to monitor the activities of employees, such as checking email and internet usage, GPS tracking in employees' cars or trucks, or camera surveillance in order to combat theft and fraud, it needs to carry out a data protection impact assessment ("DPIA") first. A DPIA looks at the privacy risks of the monitoring system, so that measures can be taken to reduce risks. If the company has a data protection officer, then they can be asked for advice on carrying out the DPIA. * Prior consultation: if the DPIA shows that the intended inspection poses a high risk, and the company is unable to find measures to limit this risk, then the Dutch Data Protection Authority (AP) must be consulted before the company starts checking personnel. This is called a prior consultation. If the company has a data protection officer, they can advise on whether prior consultation is necessary.

- Covert control: if the company intends to secretly monitor employees, it must also meet the additional conditions for covert monitoring. Secret monitoring of employees is only allowed in special circumstances, such as in case of a suspected crime. In case of covert surveillance, the employer is only allowed to use the data for the initial purpose of the surveillance.

Commentary

Generally, monitoring is allowed provided companies take privacy into account. They must also comply with the General Data Protection Regulation and the law implementing the GDPR. Specifically, the employer must have a legitimate interest in monitoring their staff and they must be able to argue why it is legitimate. Furthermore, monitoring must be absolutely necessary. Employers must also inform personnel, specifically on what is and what is not allowed, that control is possible, the reason and when the employer will check,

how the monitoring takes place and what data will be monitored. The right to confidential communication must also be taken into account. When companies have a works council, according to article 27 (1) (k) (l) the company must ask the works council for permission in relation to the processing and protection of personnel and arrangements aimed at or suitable for observing or checking the presence, behaviour or performance of the staff. When the work council does not approve, the employer is not allowed to check. A data protection impact assessment must also be carried out and when this shows a high-risk, prior consultancy should be done with the Dutch Data protection authority. This applies to all forms of employee monitoring.

Employee monitoring in the Netherlands and Europe is subject to strict legal standards regarding informed consent and privacy. According to a ruling by the subdistrict court judge of the Central Netherlands District Court, Utrecht (ECLI:NL:RBMNE:2021:6071), an employee's consent to monitoring must be well-informed. A mere warning message that an employee must accept before logging in is insufficient to constitute informed consent. In this specific case, the court held that the employee did not provide informed consent because the extent and manner of monitoring were unclear, despite the warning message displayed upon login.

The European Court of Human Rights (ECHR) further clarified the principles surrounding workplace monitoring in the Bărbulescu v Romania case (ECLI:CE:ECHR:2017:0905JUD006149608). In this case, an employer sought to terminate an employee, Mr. Bărbulescu, who had his work-related account monitored. The ECHR ruled that the monitoring in this case was not legally valid.

The ECHR provided six crucial factors that an employer must consider when monitoring an employee: (i) The employee must be informed in advance about the nature of potential monitoring by the employer. (ii) The extent of monitoring and its impact on the employee's privacy. (iii) The employer should have legitimate grounds justifying the need for monitoring. (iv) Employers should explore less intrusive methods and measures when implementing monitoring. (v) The consequences of monitoring on the employee. (vi) Providing adequate safeguards, especially in cases involving highly intrusive monitoring methods (paragraphs 121 and 122).

This ruling and the stringent factors outlined emphasise that monitoring employees cannot be undertaken lightly and must adhere to clear legal standards.

The following are the extra criteria for covert control: * Reasonable Suspicion: if an employer has a reasonable suspicion that one or more employees are engaging in criminal or prohibited activities, such as theft or fraud, the employer may consider secret monitoring. * No Alternative: if the employer made efforts to stop theft or fraud but has

not succeeded, the employer may have no choice but to conduct secret monitoring. * Occasional Monitoring: covert monitoring should be occasional, meaning it is limited to a predetermined period, and continuous secret monitoring is not allowed. * Notification: regardless of the monitoring's outcome, the employer must inform the involved employee(s) after the secret monitoring has taken place. * DPIA (Data Protection Impact Assessment): for the first-time secret monitoring, perform a DPIA. If the organisation has a Data Protection Officer (DPO), the employer should seek their advice. * Subsequent Occasional Monitoring: for subsequent secret monitoring instances with the same methodology, the employer does not need to repeat the DPIA. * Periodic DPIA Review: even if the data processing remains unchanged, the employer should consider reviewing the DPIA periodically, for instance every three years. * Private Investigation Agency: if the employer hires a private investigation agency for secret monitoring, the employer should perform a DPIA. * Prior Consultation: if the DPIA indicates a high risk and the employer cannot mitigate it, the employer should consult with the Dutch Data Protection Authority before commencing secret monitoring, known as prior consultation. The employer's Data Protection Officer can advise on the need for this consultation.

Figures about monitoring employees

In 2023, a study was done on employee monitoring in the Netherlands on 910 employees (including managers and senior managers) and 126 owners and executive managers within the small and medium-sized enterprise (SME) sector. 43% of surveyed employees report that their companies use tools for employee monitoring.

Besides employees, many supervisors and managers are also under surveillance. Among respondents working for companies using monitoring software, 56% both monitor employees and are themselves monitored by their superiors or the HR department. A smaller group (27%) only supervise employees without being monitored, while 17% report being solely subject to monitoring. 73% of employees say that the HR department has explained their rights to them. However, more than a quarter of employees still respond that they either have not received information (22%) or do not know (5%).

Additional metadata

Cost covered by	Employer
Involved actors other than national government	Works council

Involvement (others)	None
Thresholds	Affected employees: 50 Company size: No, applicable in all circumstances Additional information: Works councils are only required if more than 50 employees

Sources

Citation

Eurofound (2023), Netherlands: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Poland

Employee monitoring and surveillance

Phase	Act of 1 December 2022 amending the Act - Labour Code and certain other acts; Act of 26 June 1974 Labour Code
Native name	Ustawa z dnia 1 grudnia 2022 r. o zmianie ustawy – Kodeks pracy oraz niektórych innych ustaw; Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy
Type	Employee monitoring and surveillance
Added to database	26 October 2023
Access online	Click here to access online

Article

Art. 11(1), 21(1c), 22(1e), 22(1f), 22(3), 67(28) of Act of 26 June 1974 Labour Code; Art. 1, 2, 4, 5, 7, 8, 9, 10, 12, 13, 14, 16, 17 of Act of 1 December 2022 amending the Act - Labour Code and certain other acts;

Description

Sobriety checks

An employer may introduce sobriety checks for employees if this is necessary to ensure the protection of the life and health of employees or other persons or the protection of property. The conditions of the sobriety check must be laid down in a collective agreement or in the work rules or in a notice if the employer is not subject to a collective agreement or is not obliged to issue work rules.

Remote control of work

An employer has the right to carry out an inspection of the employee's remote work, a health and safety inspection or an inspection of compliance with security and information protection requirements, including procedures for the protection of personal data, under the terms of the remote work agreement between the employer and the employee. The inspection shall be carried out in agreement with the employee at the place of remote

work during the employee's working hours. The monitoring shall not invade the privacy of the teleworking employee or any other person, nor interfere with the intended use of the home premises.

E-mail monitoring

If necessary to ensure that the work is organised in such a way that the working time can be fully utilised and the working tools are made available to the employee, the employer may introduce monitoring of the employee's business e-mails (e-mail monitoring, electronic mail monitoring). E-mail monitoring must not violate the employee's privacy and other personal rights.

Commentary

The employer must agree with the employee on the timing of the remote working check. The inspection shall take place during the employee's working hours. A negative inspection result allows the employer to revoke the permission to carry out remote working.

The employer is eligible (but not required) to impose a disciplinary sanction (a warning, a reprimand or a fine) on the intoxicated employee but also to terminate the employee's employment contract without notice through the employee's fault or with notice. The employer may apply one or both of these sanctions.

Additional metadata

Cost covered by	Companies Employer
Involved actors other than national government	Trade union Works council Employer organisation
Involvement (others)	None
Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), Poland: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Romania

Employee monitoring and surveillance

Phase	Law no 190/18 July 2018 on measures implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)
Native name	Legea nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)
Type	Employee monitoring and surveillance
Added to database	06 October 2023
Access online	Click here to access online

Article

Law no 190/18 July 2018 [Legea nr. 190 din 18 iulie 2018] - 2, 5, 7, 14,

Description

With the law, the processing of personal data is much better defined, the employee is protected against abuse by the employer. At the same time, employers are informed more specifically about how the law regulates the surveillance of employees, in order to have a balance between the two parties.

According to the provisions, the employer can monitor the work of employees only if the following conditions are met: * The employer has legitimate and well-founded interests that prevail over the interests or rights and freedoms of the employees. * The employer

has informed in advance, in a precise and explicit manner how they wish to monitor the employees' activity. * The employer has consulted in advance with the trade union or employee representatives before implementing monitoring systems. * The employer ensured that the duration of storage of personal data is directly proportional to the purpose of the processing, without exceeding the legal time limit of 30 days. An exception is made in duly justified cases.

The law clearly specifies the employer's obligation to inform employees in advance of how they choose to monitor their activity. This can be done by following certain steps. * An e-mail will be sent to the employees informing them of the intention and the way in which the monitoring of their activity will be carried out. * The necessary changes will be made in the internal rules. * The necessary changes will be made in the additional documents to the employment contract. * Minutes will be drawn up and signed by all employees.

There are some situations in which the employer must justify the need to implement supervision systems. An example is GPS tracking of the transport vehicle or any other purpose for which the employee works. If there is no reason that would give the employer reason to suspect that the employee is carrying out illegal operations and activities with the company car, then the imposition of surveillance is not justified.

As far as surveillance cameras at the workplace are concerned, employees must be informed of their location and when they are active. It is forbidden to place hidden cameras, as it violates the employee's right to privacy, even if they are in the work space.

Commentary

The same applies to monitoring activity on the internet and generally on the work computer. This situation is quite delicate, because it is not possible to impose an exclusive control on the way the employee chooses to carry out their activity. Some people may take more frequent breaks and go on social networks, but they do what their work without any problems. In this case, too, the employer must have some justified suspicion that the employee is using the computer and internet for personal, abusive and illegal activities.

Additional metadata

Cost covered by	Companies Employer National government
Involved actors other than national government	Employer organisation Trade union

Involvement (others)	None
Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), Romania: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Slovakia

Employee monitoring and surveillance

Phase	Employee monitoring and surveillance
Native name	Monitorovanie a dohľad nad zamestnancami
Type	Employee monitoring and surveillance
Added to database	20 October 2023
Access online	Click here to access online

Article

§ 13 of the Labour Code

Description

In Slovakia, the general regulation on the protection of personal data applies (the EU regulation and the Act on the Protection of Personal Data are also directly applicable in Slovakia).

Regarding the monitoring and surveillance of employees, the Labour Code (Act 311/2001 Coll.) has a very brief legal regulation in this regard, quite problematic and unclear (according to practice). This legislation was introduced by Act No. 361/1012 Coll. which amends Act no. 311/2001 Coll. Labour Code and valid from 1.1.2013.

The employer must not violate the employee's privacy at the workplace and in the employer's common areas. It is inadmissible to monitor or record the employee's phone calls using the employer's technical devices. It is also inadmissible to check the employee's e-mail sent from the work e-mail address and delivered to this address without the employer notifying them in advance. The employee has the right to file the complaint to the employer if the principles of equal treatment are violated, if the conditions for the exercise of rights and duties are not observed in accordance with good morals, if it is an unjustified unauthorised violation of the employee's privacy, if it is an unauthorized prohibition to maintain confidentiality about working conditions or if it is a prohibition to perform other gainful activity, as well as if it is a violation of rights and obligations arising from the employment relationship. The employer is obliged to respond to the employee's

complaint without undue delay, to make corrections, to refrain from such action and to eliminate its consequences.

An employee who believes that his privacy at the workplace or in common areas has been violated due to non-compliance, may turn to the court and seek legal protection.

Commentary

So far, there are no known statistically significant violations of the law regarding monitoring and supervision of employees. Even the National Labour Inspectorate, which carries out labour inspections, does not pay significant attention to compliance with the provisions of § 13 of the Labour Code.

Additional metadata

Cost covered by	Employer
Involved actors other than national government	Court Other Trade union
Involvement (others)	National Labour Inspectorate
Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), Slovakia: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Slovenia

Employee monitoring and surveillance

Phase	Personal Data Protection Act
Native name	Video nadzor in zbiranje biometričnih podatkov zaposleni
Type	Employee monitoring and surveillance
Added to database	23 October 2023
Access online	Click here to access online

Article

Personal Data Protection Act (Zakon o varstvu osebnih podatkov, ZVOP-2), Articles 76-7

Description

The Personal Data Protection Act (ZVOP-2), issued on 27 December 2022, stipulates the procedure and rules on video monitoring and biometric data collection for businesses.

First, the authorised person must issue a written decision on the use of video surveillance, detailing the reasons. Second, the domain under video surveillance must be clearly designated by a written or graphic description that alerts the subject to the fact that they are being watched. According to Regulation (EU) 2016/679, such notice must include information on the controller, the reasons for surveillance, data processing, and unusual additional data processing (for example, data transfer to third-country entities or live monitoring). However, rather than a full notification, a webpage link (URL and QR code) is adequate. Video surveillance is not permitted in elevators, restrooms, dressing rooms, or hotel rooms. The controller must document all access to and use of surveillance data. In commercial buildings, 70% of owners must approve of the surveillance before its introduction.

The following reasons may justify video monitoring of business premises access: (1) the security of people and property, (2) control of entry to those premises, or (3) the risk of injury to employees due to the nature of their employment. Monitoring should not cover other buildings, for instance, residential houses. Access surveillance may comprise a written record of names, addresses, employments, number of identity documents, and the

purpose of the visit, in addition to CCTV data (picture, date, time, and, in exceptional cases, sound).

Within work premises, video surveillance is allowed only on the grounds of (1) security of persons and property, (2) prevention and detection of offences in gambling or (3) protection of confidential information. Surveillance must be limited and should not cover workplaces where employees usually work unless necessary for one of the three reasons. Only controller's authorised employees can perform direct monitoring.

The employer must notify workers about video surveillance in advance. Before its introduction, the employer must consult the company trade union and works council (or workers' representative). The consultation should occur at least 30 days before it. If monitoring is to cover workplaces, the consultation must occur at least 60 days before. National security issues and gambling are excluded from the obligation to consultation.

The Information Commissioner issued instructions on the proper use of surveillance at the workplace in the face of the collision of the employee's right to privacy and the right of the owner to property. Surveillance must be proportionate, and it is not allowed to survey employees during the work process because the employer is, for example, afraid of theft. In this case, surveillance monitoring is more necessary during employee absence since stealing is more likely to occur at that time. It is neither possible (and even prohibited) to monitor employees for research purposes or mystery shopping, either directly or by authorising a third party. For monitoring people, one may be criminally liable for breaching human rights to personality, personal and family life.

Commentary

Not available.

Additional metadata

Cost covered by	Companies
Involved actors other than national government	Trade union Employer organisation National government
Involvement (others)	None

Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), Slovenia: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Spain

Employee monitoring and surveillance

Phase	Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights
Native name	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
Type	Employee monitoring and surveillance
Added to database	13 October 2023
Access online	Click here to access online

Article

Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights): Article 87. Right to privacy and use of digital devices in the workplace. Article 88. Right to digital disconnection in the workplace. Article 90. Right to privacy in the use of geolocation systems in the workplace. Article 91. Digital rights in collective bargaining.

Description

The new Law (Organic Law 3/2018) repeals the previous Data Protection Law (LOPD 15/1999). Organic Law 3/2018 has a twofold objective:

- to adapt Spanish legislation to the European package of measures on data protection, i.e. the General Data Protection Regulation (GDPR) and Directive (EU) 2016/680.
- guarantee the new digital rights of citizens, under the protection of the provisions of Article 18.4 of the Spanish Constitution.

Thus, the regulation incorporates a broad catalogue of digital rights. Specifically, it recognises and guarantees a new catalogue of digital rights, including the following: (i) the neutrality of the internet; (ii) universal access to the internet; (iii) digital security; (iii) digital education; (iv) the protection of minors on the internet; (v) the rectification or updating of information on the internet; (vi) the right to be forgotten in search engines and social networks; (vii) the regulation of the right to a digital will.

The law also regulates new labour rights, such as digital disconnection, and privacy against the use of a video surveillance system and geolocation in the workplace. In other words, it reinforces the employee's privacy, and therefore his or her right to digital disconnection and privacy with regard to the use of digital devices, video surveillance and geolocation in the workplace, allowing collective agreements to guarantee greater protection.

Thus, for example, Article 87 states that workers and public employees shall have the right to protection of their privacy in the use of digital devices made available to them by their employer. Likewise, the employer may access the contents derived from the use of digital media provided to workers for the sole purpose of monitoring compliance with work or statutory obligations and ensuring the integrity of such devices.

Meanwhile, Article 88 states that workers and public employees shall have the right to digital disconnection in order to guarantee, outside the legally or conventionally established working time, respect for their rest time, leave and holidays, as well as their personal and family privacy.

Article 91 indicates that collective agreements may establish additional guarantees of rights and freedoms related to the processing of workers' personal data and the safeguarding of digital rights in the workplace.

Commentary

According to the CCOO trade union, Organic Law 3/2018 seeks to reinforce the right to privacy and information, but its lack of specificity, insufficient regulation and interpretative problems, as well as the reference to collective bargaining, mean that collective bargaining plays a key role in increasing and guaranteeing the privacy and intimacy of workers.

Indeed, in the drafting of the Law, the legislator is aware that there is a wide and varied casuistry, and therefore determines that these labour rights may be modulated according to the nature and purpose of the employment relationship, deriving their specific regulation to collective bargaining, both through collective agreements and agreements between the company and the workers' representatives.

The Spanish Data Protection Agency has drafted a specific document on "Data protection in labour relations" with the participation of both the Ministry of Labour and Social Economy and business organisations (CEOE and CEPYME) and trade unions (CCOO and UGT), with the aim of structuring and summarising the legislation and offering practical (non-binding) guidance.

Additional metadata

Cost covered by	National government
Involved actors other than national government	National government
Involvement (others)	None
Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), Spain: Employee monitoring and surveillance, Restructuring legislation database, Dublin

Sweden

Employee monitoring and surveillance

Phase	Act (2018:218) with supplementary provisions to the EU's data protection regulation
Native name	Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning
Type	Employee monitoring and surveillance
Added to database	02 November 2023
Access online	Click here to access online

Article

Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning Chapter 3

Description

This Act supplements Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of persons with regard to the processing of personal data and on the free movement of such data. It is the main act referred to in stating that the following activities are forbidden by the employer:

- Searching through the browsing history of an employee without reason. Automatic collection of such data is not allowed.
- Surveillance of working activity by forcing the web camera of a work laptop to be on.
- Surveillance of email conversation can be allowed in some cases, but only when there are suspicions of disloyal activity or criminal behaviour.

Commentary

The largest trade union in Sweden, Unionen, for private sector white collar workers released a report in 2021 that argues that the existing legal framework to regulate employee monitoring and surveillance is a good foundation for future regulation but may

need supplementary regulation to be effective. This existing framework is the GDPR-law, the Swedish Codetermination Act (MBL), the Employment Protection Act (LAS), and various sectoral collective agreements. However, they also state that the legal framework lacks specific regulation on the issue of employee protection from surveillance. A dedicated legal reference that ensures employee protection from excessive surveillance would make it easier.

Additional metadata

Cost covered by	National government
Involved actors other than national government	National government
Involvement (others)	None
Thresholds	Affected employees: No, applicable in all circumstances Company size: No, applicable in all circumstances Additional information: No, applicable in all circumstances

Sources

Citation

Eurofound (2023), Sweden: Employee monitoring and surveillance, Restructuring legislation database, Dublin