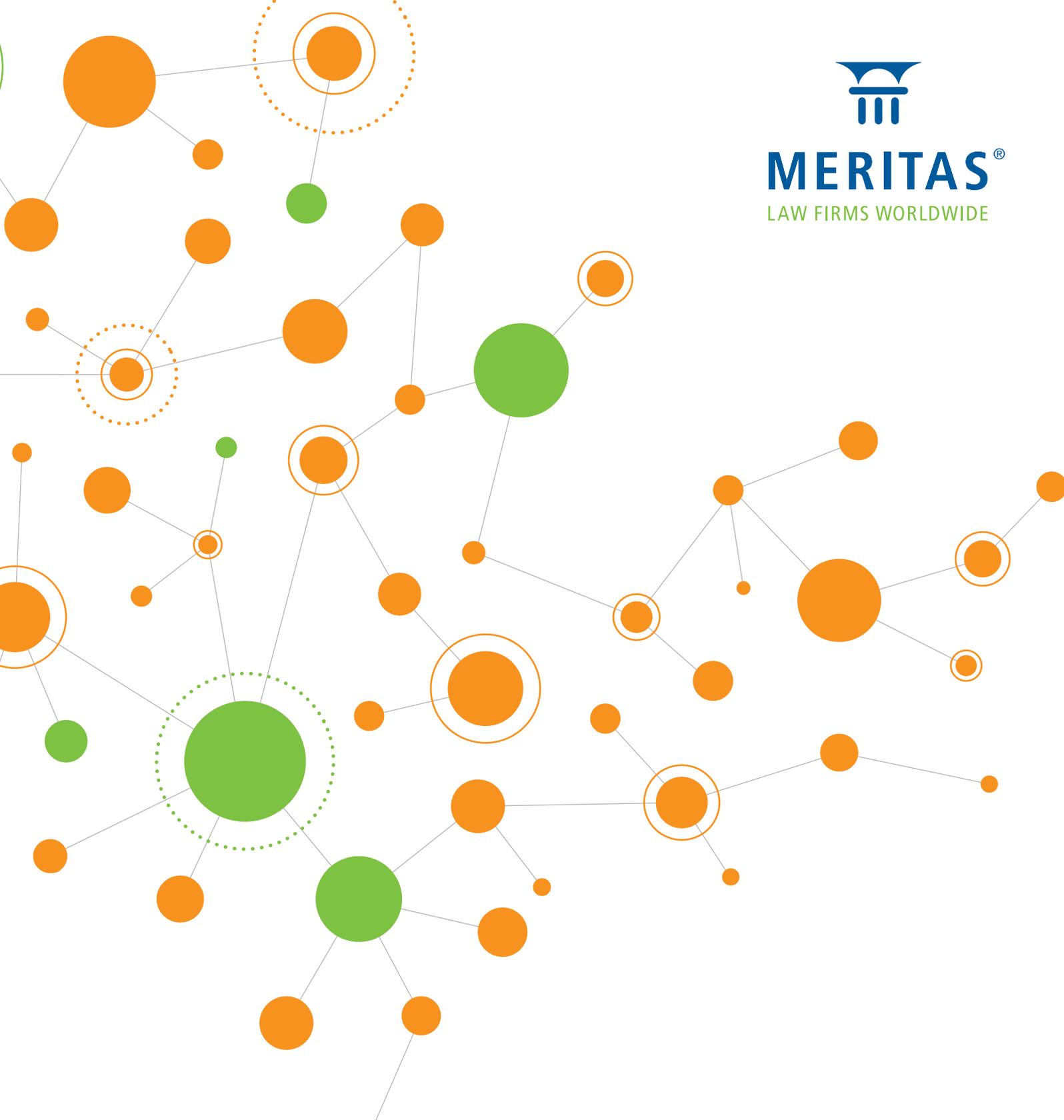




MERITAS[®]
LAW FIRMS WORLDWIDE

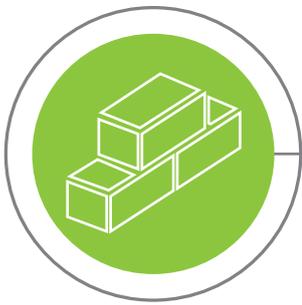


EUROPEAN & MIDDLE EAST GUIDE TO

Monitoring of Employees in the Workplace

ABOUT MERITAS

Employment, Benefits & Immigration Law Group



150

Experts
in local and
international
employment law



50

Markets served
across Europe and
the Middle East

The Meritas Employment, Benefits and Immigration (EBI) Group brings together over 150 experts in local and international employment law in 50 markets across Europe and the Middle East.

By working together, the group are able **to advise** on the local laws of different countries, project manage advice covering multiple jurisdictions and seamlessly resolve clients' **domestic and international people related legal challenges**.

The group provides a **full range of legal services** concerning the employment, incentivisation and mobility of people, including:

- Employment Contracts & Agreements
- Employment Litigation & Dispute Resolution
- HR Advisory & Restructuring
- Directors and Shareholder Duties
- Pensions, Benefits & Incentives
- Health & Safety in the Workplace
- Workers' Rights
- Employment issues regarding the sale of a business
- Business Protection related to the conduct of employees and former employees
- HR projects such as outsourcing, restructurings and incentive plans
- Immigration
- International Mobility

The EBI Group is part of Meritas - a premier global alliance of over 180 commercial law firms in 90 countries worldwide. Meritas members share common standards in providing their clients with a high quality legal service in their markets and all over the world.

www.meritas.org

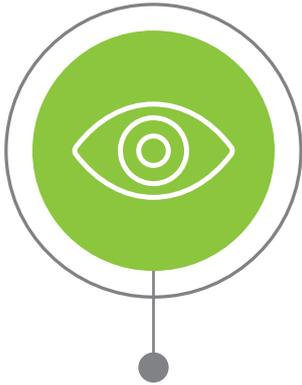
INTRODUCTION

The **monitoring of employees' activities in the work place is a sensitive and often contentious issue.** On the one hand, an employee has the right to privacy and the protection of their personal data, which is enshrined in various human rights, privacy and data protection laws and regulations. On the other hand, employers have a right to monitor their employees to protect their business from abuse, to prevent criminal activity and to ensure occupational safety.

What is key is that employers must have a legitimate reason for monitoring their employees; that the extent of **monitoring is proportionate to the need and that employees are informed** and consulted on the type of monitoring taking place. But there are important jurisdictional differences that must be understood.

In order to help both employers and employees operating across Europe and the Middle East to navigate this complex area, **the following guide provides answers to two key questions** as they relate to 25 countries across the region:

Key Questions



a) Whether the monitoring of employees is permitted from a data protection and employment law perspective?



b) Whether there are any differences or restrictions on monitoring depending on the form of monitoring used?

This guide has been produced by the **Employment, Benefits and Immigration Law Group of Meritas Law Firms Worldwide**. After reading this guide, if you have any further questions, or would like to discuss these issues in more detail, please feel free to contact any of the group's lawyers listed at the end of each chapter.

Please note: this guide is for general information purposes only and is not intended to provide comprehensive legal advice.

The information contained in this guide is accurate as at 1 December 2018. Any legal, regulatory or tax changes made after this date are not included.

Contents

PAGE

01 Austria



PAGE

04 Belgium



PAGE

07 Bulgaria



PAGE

11 Denmark



PAGE

14 Egypt



PAGE

17 Estonia



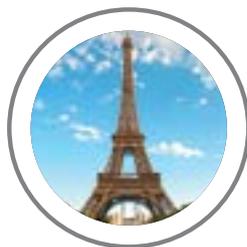
PAGE

20 Finland



PAGE

24 France



PAGE

27 Germany



PAGE
30 Greece



PAGE
33 Hungary



PAGE
36 Ireland



PAGE
39 Italy



PAGE
42 Latvia



PAGE
45 Lithuania



PAGE
48 Netherlands



PAGE
51 Norway



PAGE
54 Poland



PAGE
57 Portugal



PAGE
60 Romania



PAGE
63 Serbia



PAGE
66 Switzerland



PAGE
69 Turkey



PAGE
73 United Arab Emirates



PAGE
76 United Kingdom





AUSTRIA



Contact

Siemer-Siegl-Füreder & Partner
Rechtsanwälte
Vienna - Austria
www.ssfp-law.at

GERALD GRIES

Partner | Civil, Corporate & Labour law
T: +43 | 513 79 84
E: office@ssfp-law.at



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the prerequisites for monitoring?

Employment law perspective

A characteristic feature of Austrian labour law is the strong right of co-determination of the workforce. Although the Austrian works constitution starts from the basic sole right of the employer to decide on the management of the business, it limits this right in many different ways in favour of the workforce, as in the case of monitoring measures.

The works council plays a key role. The Austrian Labour Constitution Act regulates the possibilities of participation of the works council in detail and absolutely mandatory.

Paragraph 96 (1) (3) Austrian Labour Constitution Act provides for the widest right of participation if the employer wishes to introduce and maintain monitoring measures or technical systems for the control of workers which affect human dignity. Such monitoring measures can only be introduced and maintained with the consent of the works council. This consent cannot be replaced by an arbitration board nor by the court. Even the introduction of such monitoring measures by individual contract or instruction is not allowed. If there is no approval from the works council, the monitoring measures are not legally effective. However, if monitoring measures were to go further and even violate human dignity, they would be inadmissible in Austria with or without the consent of the works council.

If there is no works council in the workplace, the approval of each individual worker is required to introduce and maintain monitoring measures that affect human dignity.

However, the participation of the works council is not so far-reaching in the case of monitoring measures that do not affect human dignity. If the employer and works council cannot agree on the conclusion of the (enforceable) works agreement, this can be enforced before the arbitration board. The employer may unilaterally provide for the appropriate monitoring measures as long as the works council does not file an application with the arbitration board.

The conditions under which monitoring measures in Austria can be introduced by the employer thus depend on the understanding of the terms “monitoring measure” and “touching human dignity”.

The Austrian jurisdiction understands the term “monitoring measure” in a very broad sense: *It includes the systematic monitoring of the characteristics, actions or general behaviour of the employee by the employer.* It covers both mechanical (analog or manual) controls (e.g. bag checks) as well as controls carried out using special monitoring technologies (e.g. video surveillance). Also the control by other persons is covered by the term (e.g. by colleagues or private detectives). Thus, any kind of general monitoring measures must be examined for their impact on human dignity.

Austrian jurisprudence considers human dignity rights in accordance with European legal tradition to be the core area of personality. The Supreme Court always assumes that human dignity is touched, even though there is interference with the right to privacy, but this interference can be justified on objective grounds. Whether such reasons exist, can be determined by a comprehensive weighing of mutual interests in a specific case. In general, the Supreme Court assumes that human dignity is in any case affected if the employer has not chosen the gentlest means of monitoring or if the control exceeds what is typical and necessary for employment relationships of the respective species.

Recently, the Supreme Court considered telephone registration systems, which collect personal data as at least requiring approval. When they touch the human dignity, they are subject to control as absolutely necessary or if they do not touch them, as a personal data system of enforceable co-determination. A recording of the working time affects the personality of the employee just as little as a mere attendance control or the use of time clocks or magnetic cards. A time recording system that uses biometric finger scanning, however, requires approval.

If control measures serve comprehensible purposes, if they are proportionate and if they cannot be used to infer the behaviour of certain employees, then they do not affect human dignity, according to the Supreme Court.

Data protection law perspective

In Austria, the GDPR as well as the national Data Protection Act is applicable.

The GDPR contains no specific provisions regarding the monitoring of employees, it only regulates the general right on privacy. Therefore, data processing, for example, is lawful if the data subject has given its consents, the processing is necessary for the performance of a contract or for the purpose of a legitimate interest pursued by the controller. Nevertheless, the principle of data minimisation should be taken into account.

In the field of labour law, although the GDPR contains an opening clause according to which the national legislator can issue more detailed data protection provisions, this option was not used in Austria. Prior to the GDPR, the Austrian Data Protection Act only referred generally to the labour law provisions. However, this paragraph has been deleted as part of the amendment.

Currently the Austrian Data Protection Act contains only a labour law provision prohibiting image capturing for the purpose of performance controlling of employees (§ 12 Austrian Data Protection Act). However, this is not about the video surveillance itself, but rather the evaluation of such video recordings.

Even if the processing were therefore permissible under the Data Protection Act, it is also necessary in Austria to look at the labour law provisions, which may further restrict this admissibility, as mention in Point 1 and 2.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

Email Internet

The insight into screen content as well as the recording of access and movement data on the PC, is subject to the absolutely necessary co-determination, if this content is comprehensively and temporally hardly limited.

CCTV (video monitoring)

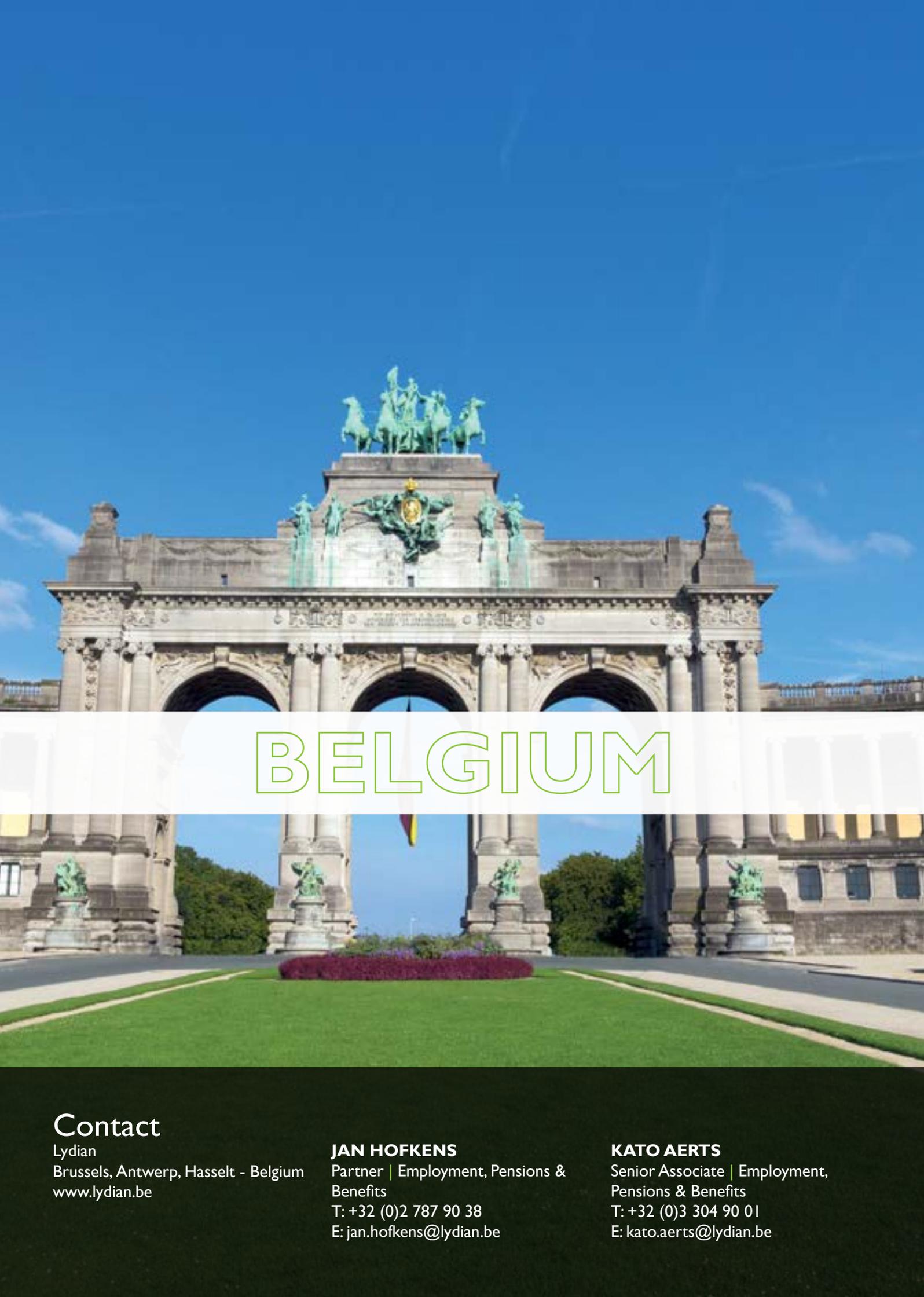
A touch of human dignity - and thus an absolutely necessary co-determination of the works council - was adopted when the employer used surplus funds to achieve a legitimate goal. This is the case, for example, with video surveillance if the employee is permanently in the field of vision of a video surveillance serving primarily other purposes.

As mentioned above, if the purpose of the video monitoring is the performance control of employees, it is prohibited by § 12 Data Protection Act. In addition, regarding the video surveillance per se, there may be an obligation to obtain a works agreement in connection with labour law conditions.

GPS Tracking

The control of, for example, field staff or professional drivers using satellite-based positioning systems will generally be subject to the absolutely necessary co-determination of the works council.

There are no specific data protection provisions in Austria, the general conditions regarding data protection are applicable.



BELGIUM

Contact

Lydian
Brussels, Antwerp, Hasselt - Belgium
www.lydian.be

JAN HOFKENS
Partner | Employment, Pensions &
Benefits
T: +32 (0)2 787 90 38
E: jan.hofkens@lydian.be

KATO AERTS
Senior Associate | Employment,
Pensions & Benefits
T: +32 (0)3 304 90 01
E: kato.aerts@lydian.be



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the prerequisites for monitoring?

The protection of employees' privacy and personal data in Belgium is guaranteed in various ways and at various levels.

On the one hand, there is the protection of privacy that exists for each individual, as laid down in Article 8 of the European Convention of Human Rights and Article 22 of the Belgian Constitution that guarantees the protection of the private life. Following these provisions, the privacy of individuals is protected, interference in the privacy of individuals is prohibited in certain circumstances, and otherwise only permissible if the principles of legality, legitimacy and proportionality are complied with. The processing of personal data is only justified if the data are lawfully processed in a transparent way.

On the other hand, specific protection mechanisms that only apply to employees are in place. In Belgium several collective bargaining agreements (CBA's) have been concluded to provide specific privacy protection for employees. CLA no. 68 of 16 June 1998 lays down the conditions and principles with regard to camera surveillance at the workplace. CLA no. 81 of 26 April 2002 develops a specific regime concerning the electronic monitoring of internet and e-mails.

It is accepted that the right to privacy at work is not absolute and that an employer can have a legitimate interest to monitor his employees. For example, the employer has the right to monitor in order to detect abuses by his employees or defend

other legitimate interests the employer might have. The monitoring must always have a legitimate purpose, be relevant and proportionate. Monitoring of employees therefore always requires a balancing between the employees' right to privacy embedded in Belgian legislation and the employer's legitimate interests to protect the business or comply with its own obligations.

In view of the above, we recommend drafting and implementing a clear policy and to inform the employees fully and clearly about the methods, objectives and duration of the monitoring. If employee consultative bodies are in place, these must be informed and consulted in accordance with the relevant legal provisions prior to implementing said policy.

Evidence that is obtained in breach of the relevant legal provisions, is in principle invalid and cannot be used in court proceedings. There is a tendency in recent case law, however, to have the illegitimately obtained evidence allowed in civil court proceedings (as has been accepted in criminal cases earlier) if certain conditions are met, for instance if the right to a fair process or the reliability or authenticity of the evidence are not compromised.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

Yes, although the principles of legality, legitimacy and proportionality apply in every case. Therefore generally speaking, the checks should be targeted and should be based on an indication that suggests an abuse. Permanent monitoring without any particular evidence of abuse is therefore in principle always prohibited. That being said, specific regulations apply to different kinds of monitoring:

Monitoring of e-mail and internet usage

The monitoring of electronic communications is only permitted for one of the exhaustively listed purposes of CBA no. 81. Monitoring is particularly permitted for the following purposes: preventing unauthorized acts, ensuring the security and/or proper technical operation of the IT network, protecting the economic, commercial and financial interests of the company and compliance with internal policies.

If the personal use of company materials is prohibited, it is not unreasonable for an employer to check whether employees are performing their professional duties during working hours and to detect abuses. However, this does not justify permanent monitoring of employees' surfing and e-mail behaviour as it would constitute a disproportionate interference of their right to privacy. The principle of proportionality, for instance, requires that checks only take place generally and are only individualised if certain anomalies are detected. This process of individualisation is specifically laid down in CBA no. 81.

Do note, however, that granting access to specific websites or allowing the private use of professional e-mail, remains a prerequisite of the employer and is not, as such, targeted by CBA no. 81.

CCTV (video monitoring)

Camera surveillance at the workplace is only permitted to attain the objectives specifically stipulated in collective bargaining agreement no. 68. These relate to health and safety, the protection of the company's goods, the monitoring of the production process or the monitoring of the employee's work. Only in the first three cases can the monitoring be continuous, provided that the monitoring of the production process relates to monitoring of machinery.

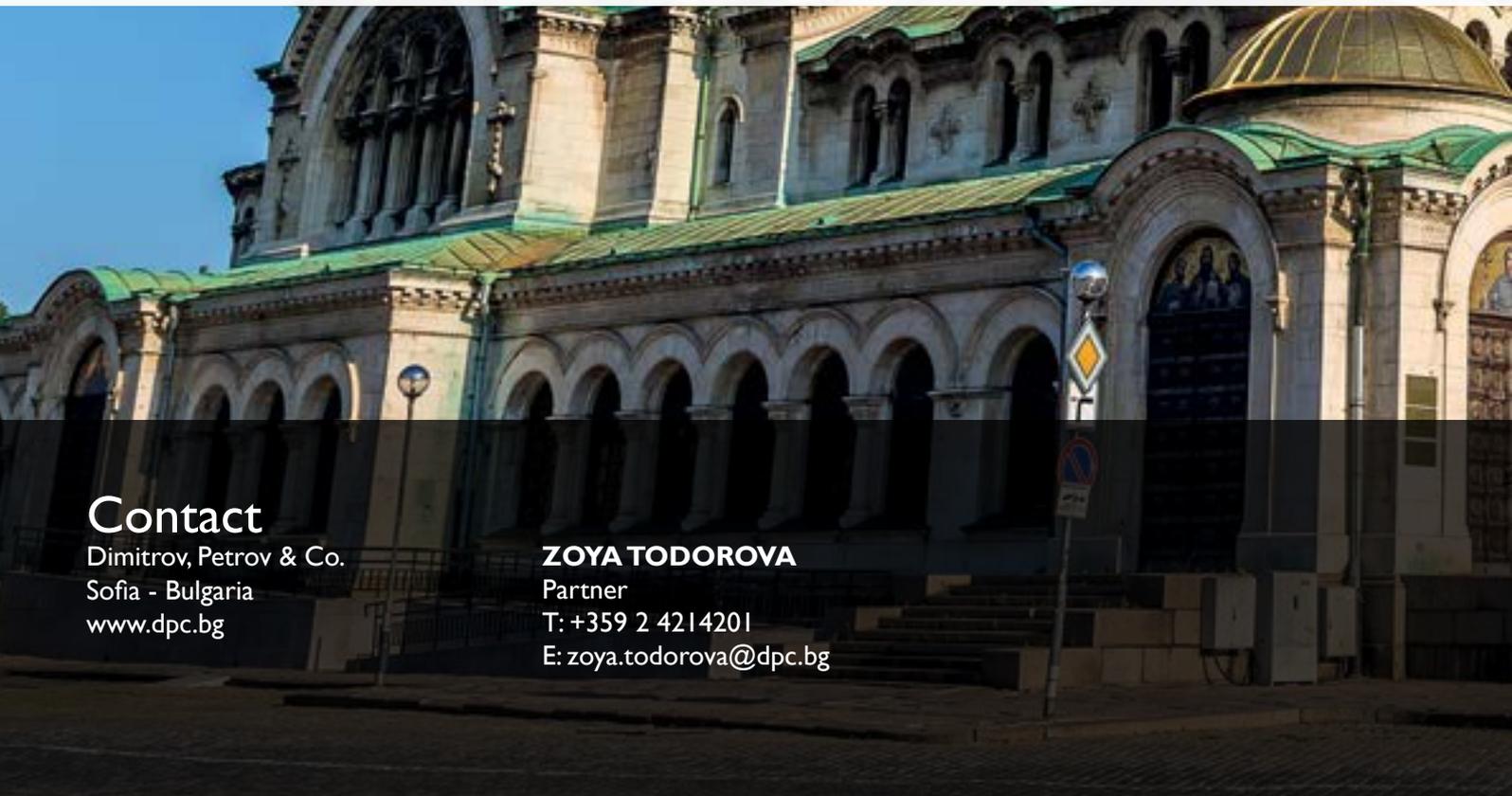
Furthermore, the monitoring must, again, be proportionate and prior to installation, the employer must provide information on the number and location of the cameras as well as on the period during which the monitoring will take place.

GPS tracking

A system that makes it possible to locate employees precisely must meet well-defined, explicitly defined objectives in order to justify its installation and use. This justification may exist, for example, in view of the safety of the employee or for the monitoring of the professional use of the service vehicle or the proper implementation of the working regime. Again, continuous monitoring is considered excessive and specific measures need to be implemented to make sure, for instance, that the GPS tracking system can be switched off outside working hours. The employees must be informed beforehand about the existence, the purpose and the duration of the monitoring.



BULGARIA



Contact

Dimitrov, Petrov & Co.
Sofia - Bulgaria
www.dpc.bg

ZOYA TODOROVA
Partner
T: +359 2 4214201
E: zoya.todorova@dpc.bg



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the prerequisites for monitoring?

The current Bulgarian data protection legislation is not harmonized with the General Data Protection Regulation (GDPR). Still, there is currently ongoing legislative procedure for adopting amendments. Publicly available is a Bill on Act for Amendment and Supplement to the Personal Data Protection Act (the Bill) that aims to achieve the necessary level of harmonisation of the national legislation with the EU data protection rules and standards. The Bill has not been officially adopted yet, but the comments and analysis below will focus mainly on its relevant provisions, as it seems very likely that the Bill would be adopted in the currently proposed version (or with minor amendments) and it provides for some new rules in terms of data processing in employment context (including related to monitoring on workplace).

According to the Bill, the employer has obligation to **adopt specific rules and procedures** regarding:

- the use of a whistleblowing systems;
- the restrictions on the use of internal company resources;
- the establishment of systems for access control, control over working time and labour discipline.

All of the above described forms of processing activities are inherently related to different forms of monitoring on the working place. Thus, it could be concluded that the legislator deems it is generally permissible for an employer to establish monitoring on the working place. Given the fact that such monitoring (regardless of the technology used) would constitute processing of personal data, all the necessary requirements of the EU data protection legislation, in particular GDPR, need to be observed.

The Bill currently contains some additional requirements for these specific rules and procedures that need to be adopted by the employers. These requirements clarify to what extent would such monitoring activities be permissible from Bulgarian data protection perspective. According to the Bill, the abovementioned rules and procedures should contain information on the

- i. scope
- ii. obligations and
- iii. methods for their implementation in practice.

The rules shall be designed in accordance with the specifics of the employer's business, the nature of the work and they cannot restrict or violate the individual rights of the natural persons under GDPR and the Bulgarian Personal Data Protection Act.

The idea of these provisions is to ensure transparency and to regulate the limits within which the employer could conduct the respective monitoring activities. They aim to achieve a proportionate balance between the fundamental rights of the employees and the legitimate interests of the employer.

In addition, there is a general rule provided for in the Bill which governs **systematical monitoring of publicly accessible areas, including through video surveillance**. The rule is directed to any controller/processor that engages in such type of processing activities, thus, employers that establish video surveillance monitoring systems in their enterprises will fall within the scope of this regulation. According to the Bill, such organizations are **obliged to adopt special rules for such processing** which should regulate:

- i. the legal basis and purposes for building a monitoring system;
- ii. the location, the scope and the means of the monitoring;
- iii. the storage period of the information records and their deletion;

- iv. the right of access by the monitored persons;
- v. informing the public about the monitoring;
- vi. restrictions on the provision of access to the information to third parties.

The Bulgarian Commission for Personal Data Protection (CPDP) is expected to give guidance on that matter through its website.

It must be noted that usually (absent specific obligations arising out of sector-specific regulation) employers have discretion whether to establish such monitoring systems. When deciding whether to establish such monitoring, the employer as data controller needs to balance:

- i. the rights, interests and freedoms of the employees – e.g. the right to privacy and right to protection against unlawful interference with one’s personal and family life and against an attack on one’s honor, dignity and reputation under Art. 32, Para 1 of the Constitution of the Republic of Bulgaria, the right not to be subject to monitoring, photography, filming, recording or other similar activities without the individual’s knowledge or despite his/her explicit disagreement except in the cases provided for by law under Art. 32, Para 2 of the Constitution of the Republic of Bulgaria, etc., on the one hand, and
- ii. the rights and the legal interests of the employer – e.g. the right to organize the working process, to control the fulfillment of the labour obligations (Art. 126 – 129 of the Labour Code), to protect his/her property and business premises and to control the access, commercial secrecy, know-how, etc. on the other hand.

From the established practice of the Bulgarian CPDP it can be concluded that:

- A case by case assessment is needed to decide what type of system is proportionate or not;
- Purposes, such as protection of the employer’s property and business premises and prevention of thefts clearly encompass legitimate interest, which could justify the installation of CCTV cameras at the entries of the office or at the working place;
- Video surveillance in places where it will cause excessive discomfort for the personnel (changing rooms, sanitary facilities, etc.) is violating the privacy legislation and should be prohibited.

In terms of the prerequisites for lawful monitoring, the monitoring on the workplace constitutes processing of personal data. Therefore, all the requirements for lawful processing of personal data under GDPR needs to be fulfilled. In addition, the national specific rules provided for in the Bill and the CPDP practice need to be respected as well, in particular:

- adopting specific rules and procedures (with the content provided for by the Bill – see Q1 above) regarding:
 - the use of a whistleblowing systems;
 - the restrictions on the use of internal company resources;
 - the establishment of systems for access control, control over working time and labour discipline;
 - systematical monitoring of publicly accessible areas, including through video surveillance;
- placing CCTV warning signs (information boards) in the premises where CCTV surveillance takes place, but the information should not contain merely a symbol (e.g. a camera).

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

The Bulgarian Data Protection Legislation¹ is currently following the tendencies carried out by the European legislation for a technologically neutral approach. The modern technical capabilities for monitoring are numerous and continually expanding, therefore the Bulgarian legislator is aiming towards universal rules, applicable to all types of processing activities that could take place at the workplace. However, there are some national specifics which should be taken into account, as described below.

Email & Internet

In terms of **Email monitoring**, the Bulgarian Constitution and Bulgarian legislation in general provide for a very high level of protection of correspondence. The Constitution proclaims that the freedom and the secrecy of correspondence and other communications shall be inviolable (Art. 34, Para 1) and that exceptions to this rule shall be allowed only with the permission of the judiciary when it is necessary to detect or prevent serious crimes (Art. 34, Para 2). According to the practice of the Bulgarian Constitutional Court, this exception is to be interpreted and applied narrowly.

There is also a criminal liability provided for in Bulgarian legislation for violation of the secrecy of the correspondence. According to the Criminal Code, various type of activities that violate the secrecy of the correspondence are punishable as crimes, among others, the unlawful learning of the content of an electronically sent message not addressed to the perpetrator or the unlawful deviating of such a message from its addressee.

Therefore, it can be concluded that the general constitutional prohibition (with a very narrow exception) and the

¹The term Bulgarian Data Protection Legislation refers to the Bulgarian Personal Data Protection Act, opinions of the Commission for Personal Data Protection (CPDP) and all the bylaws, data protection provisions in other acts, case law and all other legally binding acts and provisions on that matter

possible criminal liability constitute a serious obstacle before employers in Bulgaria desiring to establish systems for monitoring of emails.

In terms of **Internet monitoring**, there is no specific Bulgarian regulation. Internet monitoring should, in general, fall within the scope of the special rules on the restrictions on the use of internal company resources that the employers need to adopt as per the Bill. In such a case, the monitoring activities should be considered permissible in principle, unless the monitoring is not conducted in an unjustifiably intrusive way (i.e. should be subject to proportionality test).

In the practice of the Bulgarian CPDP, it is explicitly mentioned that employers have the right to control and arrange the computer systems and Internet access in a way that best suits them. Considering the fact that the employers are interested in assuring that the employees spend as much time as possible on the execution of their duties, and not on social networks or net browsing for private purposes, CPDP deems it is permissible to impose restrictions of certain websites – e.g. social networks (Facebook, Twitter, G+) – or applications (Skype). However, the restriction needs to be introduced in the rules on the internal working order. CPDP advises employers to place emphasis on the prevention of Internet abuse (implementing measures to restrict access to given websites) rather than on monitoring the employees' access.

CCTV (video monitoring)

In some cases, the use of video surveillance systems at the workplace is **mandatory under a statutory requirement**. Such scenarios include CCTV monitoring in the context of national security and defence, the protection of public order; border control, banking, casino activities. When there is no statutory requirement, employers may establish CCTV monitoring only if there is a legal ground for such processing. The old practice of CPDP acknowledged the possibility to obtain consent from employees for such processing (including by a clause in the employment contract). Given the changes introduced with GDPR in the concept of consent, it seems more reasonable to rely on another legal ground – e.g. **legitimate interest** of the employer/third party (examples given by CPDP are CCTV as a measure for working safety of the employees or protection of the life and health of individuals such as patients in reanimation chambers). The constant practice of CPDP is that video surveillance should not be too intrusive for the employees, i.e. it is prohibited in dressing rooms, toilets, bathrooms, rooms for relaxation, or premises where employees socialise. In addition, if video surveillance takes place, the employees need to be informed thereof with warning signs (information boards).

GPS Tracking

In general, in Bulgaria it is accepted that the employer has the right to install systems for surveillance and control of the company vehicles when this is substantiated by the nature of the professional activity performed or for security reasons. According to CPDP, the necessity is present for companies publicly transporting goods and passengers, performing courier services and for encashment cars. It is also accepted that such systems could be installed in other vehicles for theft prevention. If the employers decide to install such tracking systems in other scenarios, they should have a legal ground for such data processing – e.g. legitimate interest for optimizing the performed business activity by controlling the location of the fleet vehicles, reducing fuel consumption, etc. The employer must regulate via internal rules the usage of data from GPS tracking systems installed in company vehicles, especially in cases where the employee is entitled to use such vehicle for private purposes.



DENMARK



Contact

Brinkmann Kronborg Henriksen
Copenhagen - Denmark
www.bkhlaw.dk

STEFAN WESTH WIENCKEN
Attorney-at-law
T: +45 31 18 28 30
E: sww@bkhlaw.dk

MORTEN BORDRUP
Assistant attorney-at-law
T: + 45 22 89 56 41
E: mb@bkhlaw.dk



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the prerequisites for monitoring?

As the point of departure, the short answers to this question is; yes, monitoring of employees is permitted.

However, the answer is not an unambiguous ‘yes’, because the employer’s managerial right, such as their right to monitoring of employees must be assessed and balanced against the employees’ human dignity, legitimate interests and fundamental rights, including the right to respect for his or her private and family life, cf. the European Convention on Human Rights (“ECHR”) art. 8.

Monitoring of employees is, from an employment law perspective, typically permitted as long as such control measures do not offend the employees or cause them harm. It is also a condition that the control measures have a reasonable, operational purpose. The same principles can, as a main rule, be said to apply from a data protection law perspective. Different rules apply in regards to how and where the control measures are carried out, as further described below. Also, rules on implementing control measures can be set forth in collective bargaining agreements, e.g. that control measures need to be implemented with a notice, unless giving such notice would defeat the purpose of the monitoring.

Monitoring of employees can be a necessary and useful tool for an employer; but it is important to remember that workplaces are not immune to the data protection regulation. On the one hand, an employer can, based on legitimate interests, such as managerial, operational and/or security purposes, initiate monitoring of employees. On the other hand, an employee can – even at work – need space for privacy. As the former Article 29 Working Party correctly stated, workers do not leave their right to privacy at the door of their workplace every morning.

Still, it is not possible to draw a clear line in the sand in relation to what is covered by the employer’s managerial right, and what is covered by an employee’s private sphere. In Denmark, this tension field is primary regulated in the data protection regulation and collective bargaining agreements, which outline the employer’s possibilities and restrictions on monitoring of its employees.

Obviously, the new European General Data Protection Regulation (“GDPR”) sets the overriding boundaries on what is right and fair in relation to data processing, concerning an identified or identifiable natural person, in the context of employment, cf. GDPR art. 88. Whichever methods and procedures are chosen in relation to this monitoring, the fundamental principles relating to processing of personal data, cf. GDPR art. 5, and the data subjects, such as an employee’s right to clear and full information, and access to personal data, cf. GDPR section 2, sets these boundaries.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

The employer’s and the employee’s legal position in all the below mentioned types of monitoring is approximately identical, because the boundaries in the regulation do not depend on which techniques are used. However, there can be minor differences. Common for all the methods are that the employer shall treat its employees in a transparent and in a proportionate manner.

Email

As a point of departure, an employer has the right to read an employee’s emails – especially work-related emails. See for instance the European Court of Human Rights’ judgement of 12 January 2016, where the court found “[...] that it is not unreasonable for an employer to want to verify that the employees are completing their professional tasks during working hours.”

But if an email is clearly identified as private and the employer reads the email, it would be a breach of the employee's right to respect for private and family life, cf. ECHR art. 8. In order to ensure the employee's right to privacy, an email can be identified as private if the email's subject field clearly contains the word "Private" or similar. Hereby, the employee can call the employer's attention to which of the employee's emails that are covered by the private sphere. These emails may only be opened with the consent of the employee in question. This applies to both incoming and outgoing emails.

Additionally, if an employer opens a clearly identifiable private email without the employee's consent, it could be considered as criminal offence of the employer according to the Danish Criminal Code too.

It is noteworthy that the above-mentioned legislation applies both to the situation where the employer has initiated control measures according to its managerial rights, and where the employer needs to locate work-related emails due to the employee's absence.

Internet

Cyberspace can be a tempting world to venture into, and the distinction between activities, which are considered as private or corporate is not apparent. But as the point of departure, an employee's internet activities can be monitored based on a tangible balancing act of pros and cons between the above mentioned rights and

purposes. This is the main rule, because such activities do not include closed correspondence, which is protected according to ECHR art. 8.

Nonetheless, it is more unclear when the employee uses the machines to access social media, e.g. Facebook. On the one hand, an employer can have legitimate interest in monitoring its employee's activities at the "open parts" of Facebook, e.g. the "wall", because this part is accessible for everybody. Activities here can both have far-reaching negative consequences or less harmful impact on the employer. On the other hand, the "closed parts" of Facebook, e.g. the messaging functions, is a prohibited area for employers. This concerns only the sender and receiver of the message. If an employer does not want its employees to use Facebook during working hours, it is more proportionate to block the access to Facebook instead of continuously monitoring.

CCTV (video monitoring)

Video monitoring in Denmark is regulated in the Television Monitoring Act, which as main rule points out that it is not allowed for private bodies, including employers in the private sector, to monitor streets, squares or similar areas, which is considered as public accessible space. This rule does not apply to certain businesses, whose work-area can be seen as a public accessible space by default. For instance, video monitoring is allowed at gas stations, roofed shopping centers

and casinos, where the employer can monitor own entrances and frontages, including areas in connection with these. Here video monitoring is allowed to a certain extent. It must be mentioned that workplaces are not considered as a public accessible spaces by default, which is why video monitoring in general is allowed under this Act. However, video monitoring of employees will generally be considered to violate the conditions of reasonable and decent treatment of employees. It is prohibited to video monitor bathrooms, toilets and the like.

An employer's right to initiate monitoring of its employees can be further restricted under collective bargaining agreements.

GPS Tracking

The topic of monitoring employees with GPS tracking is rare in Denmark, but since the GDPR is technology neutral, the regulation applies in this situation too. By balancing the employer's interests against the employee's fundamental rights, GPS tracking can be legitimate especially within the industries of passenger and freight transportation. In these situations, an employer can have a legitimate interest in tracking the employee's vehicle, ship or plane for safety reasons – and maybe for financial reasons due to the objects value to the employer. As the former Article 29 Working Party correctly stated, the vehicle tracking devices are not staff tracking devices.



EGYPT

Contact

Shalakany Law Office
Cairo - Egypt
www.shalakany.com

SHERRY EL SHALAKANY

Senior Associate
T: +20 2 272 88 888
E: sherry.shalakany@shalakany.com



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the prerequisites for monitoring?

Employees have privacy rights which are safeguarded by piecemeal provisions in connection with data protection in different laws and regulations in Egypt, which require the prior approval and consent of the employees. In general, Egypt does not have a specific law that is in force on the protection of personal data, however the Egyptian constitution protects the citizens' private life. Private life is inviolable, safeguarded and may not be infringed upon. Correspondences, telephone calls, emails and other forms of communication are inviolable, their confidentiality shall be guaranteed. They may not be confiscated or monitored except by virtue of a judicial order and even then, this for a definite period, and according to the provisions of law.

In addition, the Egyptian Penal Code penalizes the use of electronic means to commit acts of recording, taping, transferring or eavesdropping any communications taking place via telephone or in a private place, unless these acts were committed in circumstances permitted by law or agreed upon by the parties to the communication. The Egyptian Telecommunications Law also penalises recording the content of any telecommunication message or any part of it, unless there is a legal reason for doing so.

Therefore, monitoring of employees requires a very careful act from the employer; however, its recognised in Egypt that employee's privacy right at work is not absolute, the employer may monitor the work place and materials, as long as they are not belonging to the employee(s) and are of the employer's properties, subject that the employees are clearly notified and informed that the employer's properties are monitored.

Further, Egyptian Labour Law obliges the employer to collect and receive all possible identifiable information and documents in connection with the employee's application for employment. The employer must keep a file for each employee including certain information that is required for appointment (i.e. an employee's personnel data, such as name, position, professional skills, domicile, certificates, social status, marital status, salary, a copy of his or her identification or passport, a certificate of police criminal record report, a certificate from the employee's former employer, date of employment, leaves data, data of all penalties imposed on employee during his or her employment with the employer, superiors reports on the performance of the employee, etc.). The employer may not allow anyone to review the employee's file except for those who are legally authorised to do so. Persons who are legally authorised to review employees' files are governmental authorities, courts, employees in the employer's human resources department and the employer's subsidiaries and affiliates. However, the employer may obtain the employee's approval to pass his/her data to other companies.

Accordingly, monitoring employees' personal materials is prohibited while monitoring employers' properties is not prohibited subject to the employees being aware of such monitoring.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

The Egyptian law did not differentiate between the type of monitoring, as any monitoring carried out by the employer interfering the personal privacy of the employee is prohibited. Monitoring at the work place may be permitted if it is necessary for the work's interests and to protect the employer's business, subject to the fact that the employees are aware of such monitoring and does not interfere with the personal privacy of the employees.

Email and Internet

Any monitoring carried by the employer to the work's emails and internet is permitted, subject to the fact that the devices monitored are of the employer's property and the employees are informed in advance. While in certain circumstances monitoring personal emails and internet is forbidden.

CCTV (video monitoring)

Video monitoring to the work place is permitted, provided that the employees are aware and informed that they are monitored by CCTV cameras.

GPS Tracking

As long as, the GPS tracking is carried out during the employee's working hours, then it is permitted and subject that the employees are aware of such tracking.



ESTONIA



Contact

LEXTAL

Tallinn - Estonia

www.lextal.ee

KRISTI SILD

Partner | Employment

T: +372 6400 250

E: Kristi.sild@lextal.ee



1. Is monitoring of employees permitted from a data protection and employment law perspective and what are the prerequisites for monitoring?

Employment relationships in Estonia are regulated by the Employment Contracts Act. As from 25 May 2018, data protection is regulated by the General Data Protection Regulation (GDPR). Personal data processing is also regulated by the Personal Data Protection Act, which will be updated in the near future due to enforcement of the GDPR.

The law does not provide detailed instructions with respect to employer's monitoring rights. The abovementioned legal acts provide the main principles and the employer shall establish internal regulations to implement these principles in practice.

The Estonian Data Protection Inspectorate has issued guidelines to help employers to establish such internal rules.

All employers in Estonia shall follow all data processing principles established by GDPR. Generally it can be said that personal data may be collected and processed only in an honest and lawful manner and purpose. This means that no personal data may be collected by covert surveillance. An employee must know who monitors his/her activities and how and why such monitoring occurs. Thus employers must establish internal rules and shall inform employees of any monitoring activities. The required transparency is achieved by keeping the employee informed of monitoring and this should be done before any data is collected and where any subsequent changes are made.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

In Estonia the law does not differentiate between the type of monitoring and there are no special restrictions in the national legal acts on monitoring that would depend on the form of monitoring. The type of monitoring of employees - whether it would be CCTV, email, internet or GPS Tracking, must meet the general requirements for the processing of personal data set out in the GDPR. The Estonian Data Protection Inspectorate has issued guidelines regarding processing of emails and the use of any surveillance equipment in an employment relationship.

E-mail and Internet

The following rules are only applied to the employer's e-mail addresses created for a single employee or containing the employee's name.

According to the guidelines of the Estonian Data Protection Inspectorate it is not prohibited for an employer to read the work-related e-mails of an employee. However, an employer must keep in mind that there may be private messages in an employee's mailbox.

Reading e-mail in the inboxes of employees can be usually done for two purposes: (a) obtaining the information that is required for the organisation of work and (b) checking the performance of employees.

It is not necessary for an employer to open or read the private messages of employees for the purpose of organisation of work. The private messages of an employee may be read for checking on the performance of an employee if all of the following conditions are met:

- a. the performance of an obligation which is being checked upon can be clearly ascertained and it is important;

- b. the right to read private messages arises from the employment contract or the employee has given their consent to this;
- c. the private messages contain no sensitive data;
- d. the performance of an obligation cannot be checked in any other manner;
- e. it was reasonable possible for the other party to the message to understand that the e-mail address was not the private e-mail address of the employee;
- f. the employee and the other party to the message are both notified of the message being read.

An employee's e-mail account must be closed immediately after the end of the employment relationship.

CCTV (video monitoring)

The consent of an employee is not necessary if the surveillance equipment is used only for the protection of persons or property. However, the employees must be notified if surveillance equipment is used.

Employees must also be notified if the surveillance equipment is aimed at surveying clients or third parties, but employees are also in the surveyed area.

The use of surveillance equipment to protect persons or property may not damage the rights of employees excessively. For instance, sound recording is not permitted. The security risk for which surveillance equipment is used must be clearly defined and real.

Use of surveillance equipment is not permitted:

- a. in the rooms that are not meant for performance of duties, but for private use of employees, such as toilets and shower rooms, changing rooms, the lockers and rest area of employees;
- b. in private offices;
- c. in places where it would lead to the processing of sensitive personal data, such as trade union rooms, prayer rooms, the health worker's room and entrances to them.

The data obtained with the help of surveillance equipment meant for the protection of persons or property may not be used for any other purpose. Also, use of surveillance equipment to check the quality and quantity of the work done by employees is not permitted.

Employees have the right to view the data about them, incl. recordings, collected with surveillance equipment. They have the right to view data regardless of who collected them – the employer or the security company hired by the employer.

GPS devices

An employer may not use a GPS device to track in real time outside working hours. A GPS device may be used to collect data about an employee outside working hours only to the extent it is directly necessary either pursuant to law or for the performance of a contract.



FINLAND



Contact

Lexia Attorneys
Helsinki - Finland
www.lexia.fi

TOMI KORPIOLA
Partner | Head of Labour Law
T: +358 40 753 0587
M: +358 50 593 451 |
E: tomi.korpiola@lexia.fi

TOMI TANSKANEN
Associate | Labour Law
T: +358 40 753 0587
E: tomi.tanskanen@lexia.fi

ANTONINA PAASIKIVI
Senior Associate | Labour Law
T: +358 50 548 4126
E: antonina.passikivi@lexia.fi



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the prerequisites for monitoring?

An employee's privacy is based on the Constitution of Finland. According to the section 10 of the Constitution, everyone's private life is guaranteed, and the secrecy of correspondence, telephony and other confidential communication is inviolable.

Monitoring in the workplace and the privacy of employees is strictly regulated under the Act on the Protection of Privacy in Working Life. The act is applied to the processing of data in connection with employment relationships and it contains provisions concerning specific categories of information, including camera surveillance and employees' use of email. The purpose of the Act is to promote the protection of privacy and other fundamental rights safeguarding the protection of privacy in working life.

The employer is only allowed to process personal data that is directly necessary for managing the employee's employment relationship. Under the regulation, the employer has the right to monitor employees during working hours, with some restrictions. To ensure occupational safety, the employer also has an obligation to monitor the work. Data collected through surveillance must be necessary for managing the employment relationship. The protection of property and ensuring staff and customer safety are also acceptable reasons for monitoring. The employer is obligated to inform employees about the monitoring methods and to agree on the necessary monitoring rules in the co-operation negotiations.

The purpose and introduction of any methods used in camera surveillance, access control and other technical monitoring of employees, and the use of electronic mail and other data networks, are governed by the cooperative procedure referred to in the Act on Cooperation within Undertakings and the Act on Cooperation in Government Departments and Agencies. In undertakings and in organisations subject to public law that are not governed by the legislation on cooperation, the employer must – before making any decisions on such matters – provide the employees or their representatives an opportunity to be consulted.

After the cooperative or consultative procedures, the employer must determine the purpose of the technical monitoring of employees and the methods used and inform employees about the purpose and introduction of monitoring, the methods used in the monitoring system, and the use of electronic mail and the data network.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

Email

Messages are mainly confidential, unless otherwise provided by law. The right to private communication is inviolable and without exception, even if the employer owns the technical infrastructure used for such activity. The monitoring of an employees' email box or retrieval of messages is therefore not allowed without specific legal grounds. Unless otherwise provided for in a legal provision, the employer cannot reserve the right to read or use emails received or sent by employees. Any such stipulations included in company policies are considered invalid.

By default, the employer is only entitled to retrieve or open an employee's email with the employee's consent. Consent for retrieving and opening email messages is voluntary on the part of the employee. An employee cannot be obligated to giving his/her consent and can revoke such consent at any time.

According to the Act on the Protection of Privacy in Working Life, the employer has the right to retrieve and open electronic messages sent to an electronic mail address allocated for the employee's use, or electronic messages sent by the employee from such an address, only if the employer has planned and arranged the necessary measures to protect electronic messages sent in the employee's name or by the employee.

The employer is only entitled to retrieve an employee's e-mail messages without the employee's consent, if there is justified reason to believe that the employee's e-mail contains one or more work-related messages that are crucial to the employer. A further prerequisite is that the employer has no other system for reviewing messages and their contents. The employer can also retrieve an employee's e-mail message without the employee's consent if the employee has died or is permanently prevented from performing his/her duties.

If the employee is temporarily prevented from performing his/her duties, the following conditions must be met in order for the employer to have the right to retrieve his/her e-mail messages:

1. There is no other reasonable way of obtaining the information or material contained in the e-mail message.
2. The employee's consent cannot be obtained within a reasonable time, and the investigation of the matter cannot be delayed.
3. The Director of Administration approves of the action and all of its phases are documented.

Internet

It is generally acceptable for the employer to forbid the use of the internet for personal purposes during working hours, or to restrict use of the internet by other means. Even if such restrictions cannot be controlled or monitored by the employer, employees are fully obligated to follow them. It is also legal for the employer to technically block certain websites, to prevent employees from visiting them while at work.

The employer may not extend restrictions regarding the use of the internet to outside working hours. If the employee is allowed to use the employer's equipment outside working hours, the employer may be able to restrict the employee's use of the internet outside the workplace. It is recommended that this is agreed with the employee in writing, for example in the employment contract.

CCTV (video monitoring)

According to the Act on the Protection of Privacy in Working Life, the employer may operate a system of continuous surveillance within its premises based on the use of technical equipment which transmits or records images (camera surveillance) for the purpose of ensuring the personal safety 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. Camera surveillance may not, however, be used for the surveillance of a particular employee or particular employees in the workplace. Camera surveillance may also not be used in lavatories, changing rooms or other similar places, in other staff facilities or in work rooms designated for the personal use of employees.

Notwithstanding the above, the employer may, however, direct camera surveillance at a particular work location in which employees are working, if the surveillance is essential for:

1. Preventing an apparent threat of violence related to the work of the employee or an apparent harm or danger to the employee's safety or health;
2. preventing or investigating property crimes if an essential part of the employee's work is to handle property of high value or quality, such as money, securities or valuables; or
3. Safeguarding the employee's interests and rights, where the camera surveillance is based on the request of the employee who is to be the subject of the surveillance and the matter has been agreed between the employer and the employee.

When planning and implementing camera surveillance, the employer shall ensure that:

1. The potential for using other means that interfere less with the privacy of employees is investigated before the introduction of camera surveillance;
2. The privacy of employees is not interfered with more than is necessary for achieving the aim of the measures;
3. the use and other processing of recordings of people obtained through surveillance is planned and performed with due consideration to the provisions of sections 5-7, 10 and 32-34 of the Personal Data Act, irrespective of whether the recordings constitute a personal data file under that Act;
4. Recordings are used only for the purpose for which the surveillance was carried out;

5. after the cooperative and consultative procedures referred to in section 21, employees are informed of when the camera surveillance will begin, how it will be implemented, how and in what situations any recordings would be used and, in situations referred to in section 16(2), the locations of the cameras; and
6. Prominent notification of the camera surveillance and its method of implementation is displayed in the areas in which the cameras are located.

Notwithstanding the abovementioned, the employer has the right to use recordings for:

1. Substantiating the grounds for termination of an employment relationship;
2. investigating and substantiating harassment or molestation as referred to in the Act on Equality Between Women and Men (609/1986) or harassment and inappropriate behaviour as referred to in the Occupational Safety and Health Act (738/2002), provided that the employer has a justifiable reason to suspect that the employee is guilty of harassment, molestation or inappropriate behaviour; or
3. Investigating an occupational accident or some other situation causing a danger or threat referred to in the Occupational Safety and Health Act.

GPS Tracking

Employers have the right to monitor employees by GPS only during working hours. This is allowed only if the tracking serves to ensure the employees' occupational safety or is used to coordinate the work force.

Monitoring by GPS tracking is allowed only if the employer has agreed on GPS tracking with the employees in co-operation negotiations. Co-operation negotiations are required for the arrangement of such monitoring in the same way as for CCTV monitoring.



FRANCE

Contact

Bignon Lebray

Paris, Lille, Lyon, Aix-Marseille - France

www.bignonlebray.com

JÉRÉMIE BOUBLIL

Partner | Employment & Social Security Law

T: +33 | 44 17 17 44

E: jboublil@bignonlebray.com



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the pre requisites for monitoring?

In France, any individual has the right to respect for his private life. It is a fundamental right guaranteed by internal laws, such as the French Civil Code, the French Labour Code or French Data Protection Law and European laws, such as the European Convention on Human Rights (ECHR) or the General Data Protection Regulation (GDPR).

Under Labour Law, Article L.1121-1 of the French Labour Code provides that “No person may make any restrictions to the rights of individuals and to individual and collective freedoms that are not justified by the nature of the task to be performed, nor proportionate to the aimed pursued”. This article is the “guardian” of the rights and freedoms of employees. All company decisions must be taken in strict compliance with the principles of necessity and proportionality mentioned. As a result, an employee has the right to respect for his private life and the secrecy of his correspondences [at his workplace and during his working time]; this principle was enshrined by the French Supreme Court in its decision called “Nikon” in 2001.

This protection of the employee’s privacy and their personal data, even during the performance of his employment contract, is guaranteed by the legislator, the judge, but also by the “Commission Nationale de l’Informatique et des Libertés” (CNIL) which is the French data protection authority.

Before May 25th 2018 and the entry into force of the GDPR, the system applying to the processing of personal data was mandatory reporting formalities for

the employer to the data protection authority (simplified or ordinary notification, CNIL authorisation). The control of personal data processing was *a priori*. After May 25th 2018, formalities are no longer required to process employee’s personal data. The control of processing is *a posteriori*. Today, employers must maintain a record of processing activities of its employees’ personal data, and make this record available to the supervisory authority on request.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

Email and Internet

In application of Article L.1121-1 of the French Labour Code, mentioned above, the monitoring of emails and Internet can only be implemented for certain purposes that are consistent with the interests of the company. For instance, it may be the willingness to ensure the security of computer networks, or to limit the risks of abuse from a personal use of the professional tools put at the disposal of the employees.

Nevertheless, the judge considers some processes as illicit: as example, the implementation of “keyloggers”, or the fact for an employer to receive in copy all the emails sent or received by the employees are considered as illicit and are condemned.

Moreover, the consultation of employees’ emails is possible only when they are sent/received from a professional computer. However, when the employee identifies emails or files as “personal” the employer cannot access them without first asking the employee’s permission, or after having duly called him. All control devices, information tools and software must be registered into the record of processing activities by the employer.

In addition, the implementation of technology which monitors employees is strictly regulated by the French Labour Code, which requires

- i. prior consultation of the staff representatives and
- ii. individual and prior information provided to the employees concerned by this system

CCTV (video monitoring)

CCTV is very intrusive for employees and the cases in which such systems are used are strictly supervised by the CNIL. Such systems can only be set up in a company for the purpose of protecting property or persons. For example, CCTV can be installed in a warehouse in order to protect the company from thefts. However, CCTV cannot have the purpose of filming employees' activity, break area or bathrooms. Only authorised persons in the company can access and view the videos. The videos can only be retained for a certain amount of time identified by the employer. The CCTV must be registered in the record of processing activities.

Within the company, the implementation procedure is strictly regulated by the French Labour Code, which requires

- i. prior consultation of the staff representatives,
- ii. individual and prior information of the employees concerned by this system, such as storing period, recipients of personal data, and
- iii. registration of the activity in the record of processing activities by the employer.

Failing to comply with these requirements, the data collected will be unenforceable against employees.

GPS tracking

A GPS tracker can be installed on a professional tool of an employee (e.g. a car or telephone) for different purposes, stated by the CNIL:

- to respect a legal or regulatory obligation;
- to track, justify and charge a transportation service for persons, goods or services directly related to the use of the vehicle;
- to ensure the safety of the employees, goods or vehicles for which the company is responsible;
- to better allocate resources, services that must be performed in dispersed places;
- to monitor working time, if there is no other way to do so;
- to check compliance with the rules of use of the vehicle defined by the employer.

In order to ensure the protection of the rights of the employees concerned, the data collected by these devices are limited to certain information (names, first names, professional details, internal number, license plate number of the vehicle, location data from the device, travel history, vehicle speed, number of kilometres driven, duration of use of the vehicle, driving time and number of stops). Employees must be informed of the personal data registered by the device.

Nevertheless, a GPS tracker cannot be used:

- to control working time of the employee if another way exists;
- to locate an employee who is part of the staff representative;
- to check the respect of the speed limits;
- toward an employee who is free in the organisation of his business trips;
- to collect data outside working hours.

In order to insure the respect of the private life of the employees, the system must be able to be deactivated outside working hours and the access to the data is possible only with the use of a password and a login by persons authorised. The GPS tracking device must be registered in the record of processing activities.

Access to work place and working time inspection

Most of employers implement systems of access control on their work place (e.g. badge readers, biometric devices). The control of employees' work time is legal, but new technology devices might lead to the collection of unnecessary personal data. This might be a threat to an employee's private life. The systems of access control must not be used to control work place movement.

An employer must enforce the security of the access control systems. Only authorised persons in the company can access data (security, etc.). The retention of work place data access may not exceed three months. Prior information or consultation of the staff representatives is necessary for the display of access and time work control devices. There is no need to carry out a data protection impact assessment when a badge reader device is used. However, the display of biometric devices requires an impact assessment upon personal data protection, and the respect of employee privacy. Those devices must be registered in the record of processing activities by the employer.



GERMANY

Contact

Arnecke Sibeth Dabelstein
Frankfurt, Munich, Hamburg,
Berlin, Leer, Dresden - Germany
asd-law.com

HANS HELWIG
Partner | Employment & Labour
T: +49 30 814 59 13 42
E: h.helwig@asd-law.com



I. Is monitoring of employees permitted from a data protection and employment law perspective?

Monitoring of employees requires a very careful balancing act between the rights of employees as data subjects pursuant to data protection legislation (German Data Protection Act) and the rights that employees enjoy under Article 8 of the European Convention of Human Rights. Even though monitoring of employees is always seen as an intervention in the rights that employees enjoy under Article 8 of the European Convention of Human Rights it is under restrictive conditions allowed to monitor employees. Employers may, however, only monitor to protect their legitimate interests.

Even stricter rules apply when companies in Germany are co-determined by a works council. The works council always has a codetermination right on monitoring that is performed with the help of technical facilities such as CCTV, GPS etc. (Art. 87 (1) No. 6 Works Constitution Act). The works council has a right to be involved in the introduction and use of technical systems serving to monitor the conduct and the performance of employees. If the works council has not given his approval he can intervene and demand omission of monitoring. It is therefore in any case appropriate that with regard to monitoring a shop agreement should be concluded to establish clear rules and boundaries.

In addition, the employer should obtain the employees consent which must include type and scope of the monitoring.

Without such consent, according to a recent ruling of the German Federal Labour Court German employers are not allowed to monitor employees in the workplace without a concrete suspicion of a criminal violation or, in

some cases, a serious breach of duty (judgement of July 27th, 2017, case ref. 2 AZR 681/16). That means monitoring of an employee's computer without a concrete suspicion, including the use of keylogging software that records all keyboard entries made at a desktop computer, does not comply with German data privacy laws.

The new German Data Protection Act will replace the current German Federal Data Protection Act adjusting the German legal framework to the GDPR. It will become effective along with the GDPR on 25 May 2018. However, there will be no comprehensive new regulation concerning monitoring in the workplace, except for video monitoring in publicly accessible spaces. With respect to employees and employment contracts data protection rules largely correspond to the existing rules under BDSG.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

In Germany, the law does not differentiate between the type of monitoring. The execution of monitoring at the workplace is only rectified, if it protects the legitimate interests of the employer and is therefore only allowed in case of a concrete suspicion of criminal violation or a serious breach of duty.

However, there may be a difference depending on their permission of private use of the internet and email and overt or covert CCTV.

Email and Internet

If the use of Email and Internet for private purposes is forbidden, the employer is allowed random tests of protocol data in order to check whether the Internet is used for company purposes only.

With regard to emails, the employer may look into incoming and outgoing emails sent from the personalized company account, without establishing a permanent control. Therefore the employer must not ask for an auto-forwarding of all emails. Exceptions may apply if an employee is absent and/or an out-of-office reply proves to be insufficient.

A continuous observations and monitoring of the use and content of internet and emails is only permitted to investigate crimes in case of a concrete suspicion of criminal violation or, in some cases, a serious breach of duty and if the principle of proportionality is obeyed.

If the use of Email and Internet for private purposes is permitted the employer qualifies as provider of telecommunication services. He then has to comply with the strict provisions of on the telecommunications secrecy, respectively the German Telemedia Act. Data subject to the telecommunications secrecy may only be accessed with the employees consent, unless one of the above mentioned very narrow statutory exceptions applies. Any uncontested surveillance of email traffic would then be considered a criminal offense by the employer.

CCTV (video monitoring)

Video monitoring is permitted with respect to public areas, whereby it also has to be proportionate and shall be rectified by a concrete purpose. As such a purpose are acknowledged the performance of duties of federal agencies, the execution of domestic and public authority and maintaining legitimate interests for special purposes.

For non-publicly accessible rooms the existing regulations and jurisdiction remain applicable: Permanent video surveillance of employees in the workplace without a concrete suspicion of a criminal offense is never permitted as it is considered to be a serious breach of personal rights. Limited overt video monitoring might only be permitted if legitimate interests are pursued e.g. the protection of products and assets. Covert video monitoring is only permitted to a very limited extent. Due to the jurisdiction of the German Federal Labour Court it is only allowed under the following very narrow conditions:

- a criminal offense or massive breach of contract by the employee is suspected
- all less disruptive methods have been exhausted

- video monitoring is the only means remaining to resolve the suspicion
- video monitoring is not disproportionate and there is no indication that legitimate interests of the employees are predominant

Whether covert or not, CCTV is under every circumstances strictly prohibited in bathrooms, staffrooms and changing rooms as monitoring in those areas is held to infringe the personal rights of both, the suspected employee and other employees.

GPS tracking

Collecting employee data via GPS is only allowed during work hours and only if the tracking serves to ensure the employees safety or if it is used to coordinate the work force in e.g. transport companies.

Also here permanent monitoring of employees in the workplace without a concrete suspicion of a criminal offence is never permitted.

Covert monitoring is only permitted to a very limited extent under the above mentioned very narrow conditions.



GREECE

Contact

Tsibanoulis & Partners
Athens - Greece
www.tsibanoulis.gr

MARINA PERRAKI

Partner
T: +30 210 3675 100
E: m.perraki@tsibanoulis.gr

SOFIA KIZANTIDI

Senior Associate
T: +30 210 3675 100
E: s.kizantidi@tsibanoulis.gr



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the prerequisites for monitoring?

In Greece, privacy is a constitutional right (Art. 9, 9A) that everybody enjoys. The same applies for the right of free correspondence and communication, which is inviolable by virtue of Art. 19 of the Constitution of Greece. The aforementioned rights are safeguarded by Greek Constitution and the European Convention on Human Rights (art. 8). In addition, privacy of correspondence is also protected by the Greek penal code Art. 370.

With regard to the electronic communications (emails, internet, location data etc.), the Greek law no. 3471/2006 “on the protection of personal data and privacy in the electronic communications sector” applies. According to Art. 4§2 & 3 thereof, the surveillance of electronic communications is prohibited, except when such surveillance is either legally authorized or carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication. The second exception applies under the condition that both parties have provided their consent, in writing, upon previous notification on the aim of monitoring. This law applies to the processing of personal data within the framework of the provision of publicly available electronic communications services in public communications networks including those that support devices for data collection and identification.

In view of the above, employees have the right to privacy everywhere, including in the workplace; however, such right is not absolute and has to be balanced with employer’s right to ensure the effective operation of his/her business. In accordance with the

Greek law n. 2472/1992 on personal data protection and the relevant guidelines issued by the Hellenic Data Protection Authority, monitoring in the workplace is permitted under certain conditions; namely, it must be proportionate and necessary with regard to the legal basis of the processing and the respective legitimate interest pursued by the employer. The legitimate interest of the employer is estimated in relation to a) the risk that the employer intends to face by monitoring the employees, and b) the gravity of the impact of such monitoring on the employees’ privacy.

Besides, employers are bound to inform the employees about the existence of such monitoring, and provide all necessary information related to the processing of their personal data, in accordance with the applicable legislation on personal data protection. A detailed policy on monitoring available to employees is considered as best practice.

It is noted that currently in Greece, personal data processing is governed by the General Data Protection Regulation and the Greek law n. 2472/1997, which applies to the extent it is not contradictory to the GDPR. No national law related to data protection has been issued on the basis of the GDPR yet, even though a respective draft is being prepared.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

The law does not provide any differences regarding the form of employees’ monitoring.

Greek jurisprudence and the guidelines issued by the Hellenic Data Protection Authority provide some clarifications on the lawful conditions of different forms of monitoring in the workplace. The aforementioned conditions of proportionality and transparency apply accordingly to all forms of monitoring.

Email

The employer has the right to monitor employees' emails only in exceptional circumstances and when it is necessary to defend the legitimate interests of the employer (i.e. when there are suspicions of a criminal activity). In such cases, all data must be collected for a specific, explicit and legitimate purpose; no further processing incompatible with the aforementioned purposes is permitted. Similarly, when email monitoring is being conducted exclusively for technical reasons (i.e. security of IT systems), the employer is not allowed to process those data for further purposes.

In all cases, the employer must clearly inform employees about the legitimate use of electronic communications in the workplace, and the possibility, or lack thereof, to use those facilities for private use. In this regard, the Hellenic Data Protection Authority recommends employers to set out a clear computer policy on the monitoring of employees' computers and on the presence, use and purpose of any detection equipment.

Internet

Similarly with emails, the aforementioned apply accordingly.

CCTV (video monitoring)

The Hellenic Data Protection Authority has issued the Opinion no. 1/2011 on the lawful conditions of monitoring through closed-circuit television (CCTV). According to this Guideline, the use of CCTV surveillance systems must not be used to monitor employees, except for specific reasons that are justified by the nature and the conditions of the respective activity (i.e. banks, high-risk installations). On the contrary, in a typical business office video surveillance should be limited to entry and exit areas. Office rooms or corridors must not be monitored by CCTV, without prejudice to specific areas where monitoring is justified, such as safe-deposit box and/or electromechanical equipment.

The installation of cameras in areas that are not public but however accessible to the public is permitted only upon previous assessment of the necessity

of such monitoring in relation to (a) the risk that the controller intends to address, and (b) the magnitude of the impact on the privacy of the persons concerned. Such assessment should include the implementation of more lenient measures.

In all cases, employees must be aware of video monitoring. Personal data collected from video surveillance systems should not be used as the sole criteria for assessing the behavior and the performance of employees at work.

GPS Tracking

According to the Hellenic Data Protection Authority's guidelines, in cases where GPS tracking is implemented solely for business optimisation, it does not violate employees' privacy. If such monitoring simply aims to help employees to find a given destination, the employees must be in a position to disable such device if they desire. The assessment of the employees' behaviour based on the GPS tracking violates the principle of proportionality, and consequently employees' privacy.



HUNGARY



Contact

FKLaw
Budapest - Hungary
www.fklaw.hu

NÓRA KOVÁCS
Partner
T: +36 | 266 9168
E: nkovacs@fklaw.hu



I. Is monitoring of employees permitted from a data protection and employment law perspective?

There are two confronting interests on the two sides of the employment relationship: the employer’s right to monitor the work process at the workplace and the security of company assets on one hand and the employees’ rights to privacy on the other hand.

The Hungarian Labour Code contains the following general provisions in this respect:

“Employers are allowed to monitor the behaviour of employees only to the extent pertaining to the employment relationship. The employers’ actions of control, and the means and methods used, may not be at the expense of human dignity. The private life of employees may not be monitored.”

“The rights relating to personality of employees may be restricted if deemed strictly necessary for reasons directly related to the intended purpose of the employment relationship and if proportionate for achieving its objective. The means and conditions for any restriction of rights relating to personality, and the expected duration shall be communicated to the employees affected in advance.”

The legal basis for monitoring the employees is in most cases the legitimate interest of the employer. Consequently, the employer must conduct a so-called balancing test: the legitimate interests of the employer (to monitor the workflow, safeguard work security or protect company assets) must be weighed against the employees’ rights and freedoms. The Hungarian National Authority for Data Protection and Freedom of Information has set up a recommended protocol how such balancing test should be performed:

- **Step 1:** The employer needs to verify if monitoring of the employees is inevitably necessary to achieve its goals.

- **Step 2:** The legitimate interest of the employer needs to be closely defined.
- **Step 3:** The purpose of the monitoring is to be determined along with what personal data and for how long will be controlled.
- **Step 4:** Consideration of potential conflicting interests of the employees
- **Step 5:** Why does the employer believe that certain method of monitoring proportionately restricts the privacy rights of the employees.

This should also be documented in relevant policies and procedures.

In addition, there are certain guarantees that the employers are required to ensure:

- gradation: the method applied by the employer should, if possible, not entail control of personal data. If it is not possible, then the method that least restricts the employees’ privacy rights should be used.
- The presence of the employee at the monitoring should be guaranteed.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

Email

The most common and greatest issue with monitoring email accounts is that employees very often use their company email address for private purposes even despite internal policies are in place which forbid this practice. Nevertheless, having an internal policy which prohibits the use of company email address for private purposes is considered best practice in Hungary. Such policy should also cover the rules pertaining to making backups about emails, how long the emails are retained as well as how email accounts can be monitored. It is also recommended that an automated regular message is sent to every employee (quarterly, semi-annually) which reminds them of the rules relating to the use of email accounts.

It is to be noted that in Hungary, even if there is a policy in place which prohibits the use of email accounts for private purposes, and the employee sends or receives private messages on his/her company email address in violation of this policy, the employer is still restricted from opening such private email. The rights and freedoms of the employee and its correspondence partner enjoy preference over the rights of the employer. In this case, the employer is only allowed to look at the header of the email (sender, recipient, subject line) – this should be sufficient to determine whether such email is business related or not. If it is not business related, then the mere fact of the existence of such email should be sufficient to apply the consequences set out in the internal email policy for the breach of prohibition on the use of company email addresses for private purposes.

In order for monitoring email accounts by the employer to be lawful, the employer must provide detailed prior information to the employee about such monitoring. This information should cover:

- what is the company interest that makes such monitoring necessary;
- who is entitled to conduct the investigation;
- what are the rules of the process and how is the principle of gradation applied (for instance, if the employer suspects that confidential company information was sent as a large attachment to an email during a certain period of time, then only emails with attachments sent during such time frame should be monitored);
- what are the rights and remedies available to the employees (for instance, that they can be present when the emails are being monitored).

Internet

Monitoring of internet usage by the employees is subject to similar restrictions than the monitoring of emails. The same balancing test needs to be conducted, prior notice to the employees is a must and the principle of proportionality should be enforced throughout the process.

The Hungarian data protection authority recommends the implementation of technical measurements to block access to websites which the employer does not want its employees to visit. Thereby the need to monitor internet usage significantly decreases (though does not entirely vanish, since the employer may want to check if the employees did not go “creative” and found a workaround the security measures or visited websites that are similar to the blocked ones).

CCTV (video monitoring)

The general rules regarding monitoring employees obviously apply in this case, too. However, there are some additional precautions the employers must take when using video monitoring.

Although there are no specific employment law related regulations in place about CCTV surveillance, the data protection authority has by now developed quite specific requirements in this respect. There is one act, Act Nr. CXXXIII of 2005 on Private Investigators, which deals with CCTV surveillance and the Hungarian data protection authority ruled that in lieu of specific employment law related provisions, the regulations of this act should be taken into account.

According to this act, CCTV surveillance is legal in four cases: (i) to protect human life and safety as well as personal freedom, (ii) to safeguard hazardous materials, (iii) to protect trade, payment, bank and securities secrets, and (iv) for the protection of property. CCTV surveillance is primarily allowed for these purposes – if the employer wants to use it for a different purpose, the employer must conduct the balancing test and

justify that it is both necessary and proportionate for its legitimate interest.

That said, it is illegal to operate video monitoring for the primary explicit purpose to monitor the behaviour and activity of the employees. Likewise, it is also against the law to use video surveillance in order to influence the behaviour of the employees.

There is one very important restriction in terms of video cameras: cameras may not be placed in such rooms where the cameras may hurt human dignity. These areas include changing rooms, bathrooms, toilets or medical consultation rooms. It is further recommended to proceed with special care when placing cameras in places where employees usually spend their breaks: the cafeteria, lounge etc. In this latter case, it might not be easy to find a legitimate interest why such areas are to be monitored.

Furthermore, it follows from the general principles that the employees are to be given prior notice about the use of cameras. It is to be noted that the employer is required to inform the employees about the specific whereabouts of the cameras and their angles – this is how the employer can justify the use of the camera at that specific spot.

In addition, the employer needs to implement appropriate security measures to prevent unauthorized access to the video recordings.

As a general rule, video recordings may be retained for a period of three business days (unless they will be used).

GPS Tracking

There is one important supplementary rule in relation to GPS tracking: with a few exceptions, monitoring through GPS tracking should not allow the employer to determine the whereabouts of its employee outside his/her working hours. Therefore, the employees should be enabled to turn off the GPS signal forwarding outside their working hours. Also, GPS tracking may not be justified in case of employees working in their homes.



IRELAND

Contact

Whitney Moore
Dublin - Ireland
www.whitneymoore.ie

EMMA RICHMOND

Partner | Employment
T: +353 (0)1 611 0012
E: emma.richmond@whitneymoore.ie



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the pre requisites for monitoring?

In Ireland all individuals, including employees, have privacy rights which are safeguarded under established principles and laws. Employees do not leave their privacy and data protection rights at the door when they come into work each day simply because they are an employee. In assessing what rights to privacy an individual has in Ireland, regard must be had to the following sources;

- Data Protection Act 2018 which implements the General Data Protection Regulation and confers rights on individuals and responsibilities on those processing personal data.
- *Kennedy and Arnold v. Attorney General* which clearly identifies the constitutional right to privacy is a fundamental personal right of the citizen which flows from the Christian and democratic nature of the State.
- European Convention of Human Rights Article 8 which states; “1. Everyone has the right to respect for his private and family life, his home and his correspondence.” and
- European Charter of Fundamental Rights

The Irish Data Protection Commissioner has clearly set out that she accepts that organisations have a legitimate interest in protecting their business, resources, equipment and reputation. It is recognised under Irish law that an employee’s right to privacy at work is not absolute. It is recognised that an employer may monitor to protect their legitimate interests.

If an employer intends to monitor communications or activities, they need to ensure that any such monitoring is proportionate to the likely damage to the employer’s legitimate interest.

Indeed if it is intended to monitor a clear policy should set out the extent of any such monitoring. This policy should be open and transparent, whilst maintaining fairness and proportionality. In the absence of such a clear policy, employees may have a reasonable expectation of privacy in the workplace.

Employers should also be aware that in circumstances where they are monitoring this process of collecting or storing data on employees is considered data processing. In line with the principles set out in the Data Protection Act, such monitoring or collection of data should comply with the basic principles

Policies should provide for the methods of monitoring and what the data collected by these methods may be used for. Employees should be clearly and fully informed of these policies.

1. Employees should be notified of the policy of monitoring / surveillance, the implementation of the policy, and the consequences for an employee who breaches the policy;
2. The employer should provide legitimate business reasons to justify monitoring / surveillance;
3. Employers should choose the least intrusive methods of monitoring required to achieve their goal.
4. Employers should put in place adequate safeguards in respect of monitoring and the data collected.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

Email:

Any monitoring carried out by an employer ought to be proportionate and necessary to protect the legitimate interests of the business. In circumstances where private use of an email account is forbidden entirely such terms should be clearly set out in a policy that has been communicated to all employees.

If private use of the email account is forbidden, then in the event that there is a breach by an employee this may give rise to a disciplinary sanction, up to and including dismissal. In the event of such a breach a sanction may only be imposed after the employer has carried out a full investigation and disciplinary hearing in accordance with the procedures set out in the Code of Practice on Grievance and Disciplinary Procedures. Care should be taken to ensure that such policies are applied on a consistent basis across all departments and all levels within the organisation. It should be made clear to employees that there is an expectation that they will comply with the policy and that should they fail to do so there may be serious consequences.

In the case of *Reilly v. Bank of Ireland*, internal IT security discovered that 5 employees had inappropriate email content in their inbox. However when the Bank came to address the issue only 3 out of the 5 were suspended whilst an investigation was carried out. In this instance the ultimate sanction of dismissal was overturned by the High Court and the Court noted that the policy was not applied consistently at all levels and the employees involved were treated differently. Thus in implementing such a policy an employer should ensure that there is compliance at all levels.

Another issue that arose in this case highlighted the fact that it is not merely sufficient to have a policy in place setting out that the monitoring is in place but that this policy should also make it clear what the potential sanctions are. In this case the Court noted that the Bank were aware of an increase in inappropriate emails but that they had not communicated to employees that participation in such activity could lead to sanctions up to and including dismissal. This supported the statement made by the Employment Appeals Tribunal in the case of *O’Leary v. Eagle Star*;

“If an employee is to be dismissed for breaking the rules he should know or have an opportunity to know what they are. In a plethora of documents dealing with abuse of IT systems there was not a single document clearly outlining the consequences of departing from approved procedures.”

Internet

As with email, any monitoring carried out by an employer ought to be proportionate and necessary to protect the legitimate interests of the business. An internet usage policy should be provided to all employees and this should include information on the consequences of a breach of the policy and that the policy may be relied upon in disciplinary / dismissal processes.

CCTV (video monitoring)

The statutory tribunals set up to adjudicate on employment rights have not considered or ruled directly upon the legitimacy of surveillance or monitoring of employees however complaints made to the Irish Data Protection Commissioner have been instructive in this respect.

Employees should be clearly and fully informed in advance if CCTV may be used in disciplinary or dismissal hearings.

GPS tracking

The case of *O’Connor v. Galen Ltd* is one of the few Employment Appeals Tribunal “EAT” cases in which there is discussion of surveillance and the nature of same. In this case a tracking device was placed by the respondent on the claimant’s company car, and in conjunction with the observations of a risk management company hired by the respondent to observe the claimant, it appeared that the respondent had submitted false or misleading expense claims for travel allowance and toll charges and had remained in the vicinity of his home on occasions he had claimed to have travelled on behalf of his employers.

The EAT was critical of the surveillance methods employed by the respondent noting that there was no policy on surveillance put in place by the company, despite the insistence of the respondent that the unusual circumstances of this case merited the tactics employed. Further to the detriment of the respondent’s defence was the fact that the claimant had been unaware that any aspect of his performance or behaviour was under investigation during the period of his observation. The tribunal found that the procedures used by the respondent rendered the dismissal of the claimant unfair under the Unfair Dismissal Acts because surveillance equipment was used without the claimant’s knowledge.

Again, an employer should ensure that there is a policy in place providing that such surveillance may be used in a disciplinary or dismissal process and employees should be fully informed of the policy.



ITALY



Contact

Pirola Pennuto Zei & Associati
Milano - Italy, Rome
www.piolapennutozei.it

MARCO DI LIBERTO
Junior Partner | Employment,
Labour Law and Industrial relations
T: +39 02 669951
E: marco.di.liberto@studiopirola.com

MARIA CLELIA CHINAPPI
Partner, Rome
T: +39 06 570281
E: maria.clelia.chinappi@studiopirola.com



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the prerequisites for monitoring?

In Italy monitoring of employees is a key topic, involving employment law and data protection issues and permitted only under strict rules, aimed at balancing employer's rights with workers' privacy and data protection.

From an employment legal standpoint, monitoring of employees is ruled by art. 4 of Italian Law no. 300/1970 (so-called "Workers' Statute"), as amended by the labour reform issued in 2015: this law provides that systems and instruments allowing the employer to remotely control workers' activity can be used exclusively for organizational and productive needs, for safety in the workplace, or for protecting company's assets, and shall be installed only by virtue of an agreement with the Trade Unions.

Moreover, according to the aforesaid law provision, with reference to companies without union's representatives in the workplace, or that have not reached an agreement with Trade Unions in the matter, a specific authorization shall be obtained from the territorial office of the National Labour Inspectorate before installing and using the mentioned systems.

In any case, the abovementioned provisions "does not apply to the tools used by the worker for performing duties, as well as to entry or exit recorders", while such exemption is applicable only under specific conditions, and in relation only to tools specifically dedicated to working activities (e.g., warehouse scanners, etc.), where monitoring is an indirect effect deriving from the use of these instruments.

Finally, according to art. 4 of the Workers Statute, the information acquired with such instruments can be used at every legal effects under the conditions that employees are duly informed in writing on the use of the monitoring instruments, and that such controls are performed in accordance with privacy and data protection law, so in compliance with GDPR regulation and the internal policies to be issued by the employer.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

The aforesaid legal principles are applicable to every instrument leading to possible monitoring of employees, even if case law and administrative practice have introduced specific limits depending on the form of monitoring, as follows.

Email

With reference to the control over the employee's company email account, the European Court of Human Rights (Ruling *Barbulescu c. Romania* - 5 September 2017 - No. 61496/08), as well as Italian Supreme Court (Corte di Cassazione - No. 26682 on 10 November 2017), have stated that monitoring email accounts is lawful under specific conditions:

- if the worker has been previously informed in writing that the company is entitled to monitor his/her company email correspondence, and if such policies disclose how the measures will be implemented and their scopes;
- if email controls do not exceed the purpose of the processing, so only emails work-related and for a specific purpose can be lawfully monitored;
- the employer must provide control tracking tools in order to make it clear which emails have been monitored and how it has been done;

The aforesaid principles must be applied by way of an internal company policy, duly subscribed by the employees.

Internet

Under Italian Privacy Authority guidelines and principles, the employer is entitled to process employee's personal data deriving from the use of Internet only if the employee has been previously informed with an internal policy:

- on the forms and cases of controls by the employer;
- on the methods and conditions of use of company instruments;
- on the consequences, also under a disciplinary point of view, applicable in the event of irregular use of such instruments;
- on the compliance of this data processing with GDPR principles.

CCTV (video monitoring)

Under Italian employment law, the employer may lawfully adopt a CCTV (Close Circuit TeleVision) causing a (indirect form of) control over employees' activities only under the aforesaid conditions, so on the basis of an agreement signed with Trade Unions, or by virtue of an authorization of the labour inspectorate under art. 4 of Law No. 300/1970.

Moreover, according to administrative practice (National Labour Inspectorate, circular no. 5 on 19 February 2018), installing and using audio-visual equipment are admitted under the conditions that these devices are the only instruments aimed at reaching the company's purposes (e.g., safety at the workplace, such as protection of goods and workers and preventions from illicit acts) and if they are strictly related to these purposes.

GPS Tracking

With regard to the workers movements monitoring through the use of a GPS system installed on company vehicles, Privacy Authority (Circular on 29 March 2018, n. 181) has stated specific conditions to be met in order for these devices to be lawfully installed and used:

- the employees must be informed on the data collection system and the company has to pre-allow workers to access to the collected data;
- only relevant and necessary data for monitoring shall be processed;
- periodic reports (if any) must not refer to personal data;
- the control may not exceed the purpose of the processing;
- only if anomalies are found, the detection of the position of the GPS systems of transport may be activated in real time.



LATVIA



Contact

LEXTAL
Riga - Latvia
lextal.ee

LIVITA LĀNE – STROKŠA
Senior Associate | Data Protection
T: +371 6728 3391
E: livita.lane@lextal.lv



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the prerequisites for monitoring?

Employment relationships in Latvia are regulated by the Labour Law, which transposes many aspects of EU employment law and social policy directives, such as those relating to equal treatment, collective redundancy, working hours etc.

In Latvia, data protection is regulated by the General Data Protection Regulation (GDPR), which applies from 25 May 2018 and personal data processing law.

According to the GDPR, the protection of natural persons in relation to the processing of personal data is a fundamental right.

Monitoring at the workplace should be necessary and suitable for the achievement of a legitimate aim. An employer shall only collect and process data that directly relates to the issues which the employer aims to clarify. The data should not be of an extensive scope.

According to the GDPR, personal data shall be processed lawfully for specified, explicit and legitimate purpose, limited to what is necessary in relation to purpose, accurate and kept up to date, for no longer than it is necessary for the purpose and in a manner that ensures appropriate security of the personal data.

A fair balance between two competing interests – employee’s right to private life and the legitimate interests of employer – must be found. There have to be sufficient arguments why the interests of the employer outweighs the employee’s rights and the other way around in the particular case.

According to the GDPR, processing is necessary for the purposes of the legitimate interests pursued by the controller (employer) or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Employers are, in principle, allowed to design and apply a communications monitoring policy, as it may serve a legitimate aim. Such legitimate aim could be, for example, the protection of an employer’s business secrets from being unlawfully disclosed to a competing company or the protection of an employer’s property against the excessive use of its facilities for employees’ personal purposes or even thefts. Communications monitoring should have a basis in law. Namely, it can be carried out only in situations stipulated by the GDPR and the Labour Law.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

In Latvia, the law does not differentiate between the type of monitoring.

The monitoring activities may include, but are not limited to:

- the systematic registration and reading of e-mail messages;
- the caching of web pages viewed, including the date, time and duration of the visit;
- the recording of and listening to telephone conversations;
- data analysis in order to draw certain conclusions, registration in specific databases or files and storing for a certain period of time.

E-mail and Internet

The monitoring of E-mail and Internet at the workplace has to be aimed at the protection of other legitimate interests. Such legitimate interests can, for example, be:

- an employer's interest in ensuring the safe and productive fulfilment of his/her employees' job responsibilities;
- an employer's right to protect his/her property against the excessive use of facilities for employees' personal purposes or even thefts;

Nevertheless, the controller (employer) shall be responsible for, and be able to demonstrate compliance with the GDPR.

CCTV (video monitoring)

There are many legitimate business reasons why employers monitor employees using CCTV. Lawful bases of monitoring include keeping employees safe and secure by preventing crime, preventing employee misconduct, ensuring compliance with health and safety procedures, monitoring and improving productivity, and in some cases such as the financial services sector, complying with regulatory requirements.

Employers generally rely on legitimate interests as an appropriate legal basis for processing personal data – it entails organisational accountability and enables the responsible use of personal data, while protecting employees' data privacy rights.

Employers relying on legitimate interests as the legal basis for processing need to consider the legitimacy of their stated interest (and potentially the interests of third parties)

and must balance that interest against the interests, rights and freedoms of their employees. In addition, employers also need to apply safeguards and compliance steps to ensure that employees' rights are not prejudiced in any given case.

Video cameras, however, should not be located in employees' offices or places of a very private nature, for example, in bathrooms. Their location should be limited to entrances, exits, hallways and other similar places.

According to personal data processing laws of the Republic of Latvia, if the controller (Employer) uses an informative note to inform data subjects of video surveillance, the said note shall indicate at least the name, contact information of the controller, purpose for data processing, as well as include an indication of the possibility to obtain other information.

GPS Tracking

Collecting personal data via GPS is allowed for the purposes of the legitimate interests of employer, for example to ensure employees safety or if it is used to coordinate the work hours or navigation in transport companies.

In any case, the employer is obliged to inform employees about the monitoring policy and that employees are also entitled to access personal data about them that has been collected during the monitoring process.



LITHUANIA



Contact

LEXTAL
Vilnius - Lithuania
lextal.ee

SANTA JANICKIENĖ
Associate | Personal Data Protection
T: +370 5 210 27 33
E: santa.janickiene@lextal.lt



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the pre requisites for monitoring?

Monitoring of employees means their personal data being processed and their privacy being intervened by the employer and therefore is subject to the General Data Protection Regulation (“GDPR” or “Regulation”) and other legal acts, including national labour law provisions.

In regards to personal data being processed due to monitoring, any processing of such data must comply with the requirements set out in the GDPR. The GDPR sets out principles that emphasises the primary requirements for processing personal data that must be met: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality (security); accountability.

Although the GDPR is directly applicable in all Member States, in the cases set out in the Regulation, Member States are provided with the possibility, in national law, to define more precisely the rules of the Regulation or to impose restrictions on them. Using this option, the Republic of Lithuania has adopted specific rules (requirements) in the Law on the Protection of Personal Data (“Data Protection Law”) in regard the processing of personal data in the context of an employment relationship.

Article 5 (3) of the Data Protection Law contains requirements for the implementation of one of the rights of the data subject - the right to be informed. According to the mentioned paragraph of Data Protection law, when the data controller (employer) processes video and/or audio data in the workplace and at the controller’s premises or in the areas where his

employees work, or processes personal data related to the monitoring of employee’s behavior, location or movement, the employees must be informed of such processing by signing or otherwise proving the fact of the notification by providing the information referred to in Article 13 (1) and (2) of the Regulation.

When the employer employs on average 20 and more employees, Article 206 of the Labour Code of the Republic of Lithuania determines compulsory counselling with the works council (an independent body representing employees that is formed by the employer’s initiative) or employer-level trade union (if there is no works council or employee trustee) prior to making decisions regarding approval or amendment of the local (employer’s) normative acts on the use of information and communication technologies and on the monitoring and control of employees at workplace as well as on the protection of employees’ personal data and its implementing measures.

Article 27 (2) of the Labour Code states that the employer exercising his ownership or management rights to information and communication technologies used at the workplace cannot violate the secrecy of the employee’s personal communication. Such provision of the national law corresponds with the regulation set out in the GDPR.

According to the current **draft** of the order of the State Data Protection Inspectorate Director on approval of the list of the data processing operations subject to the requirement for a data protection impact assessment, processing video and (or) audio data in workplace and at the controller’s premises or in the areas where his employee work, or processes personal data related to the monitoring of employee’s behavior, location or movement requires a data protection impact assessment.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

Article 61 (1) of Lithuanian Law on Electronic Communications forbids without the consent of the actual users of the electronic communications services to listen to, record, store or otherwise take over the contents of the messages and traffic data or access them, except some narrow exceptions (in relation to detection and investigation of crimes). According to Lithuanian Data Protection Inspectorate in employment context this provision becomes relevant only when the employer allows personal use of electronic communication. Although it should be kept in mind that consent in employment relationship is generally an undesirable and unsuitable legal basis for processing personal data therefore the application of Article 61 in employment context is doubtful in general.

Besides the above mentioned, there are no special differences or restrictions in the national legal acts on monitoring that would depend on the form of monitoring. The performed monitoring of employees - whether it would be CCTV, email, internet or GPS Tracking, must meet the general requirements for the processing of personal data set out in GDPR.



NETHERLANDS

Contact

Lexence
Amsterdam - The Netherlands
www.lexence.com

ANNEJET BALM
Partner | Employment
T: +31 20 5736 829
E: a.balm@lexence.com



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the pre requisites for monitoring?

As the General Data Protection Regulation (GDPR) entered into force on May 25th 2018 the same privacy regulations apply for the entire European Union. In the Netherlands, the GDPR is implemented by the *Algemene Verordening Gegevensbescherming* (“AVG”). In view of Art. 8 of the European Convention of Human Rights which emphasizes “everyone’s right to his private and family life, his home and correspondence” it is under strict conditions that employers may monitor their employees.

In general the processing of personal data must be based on one of the following principles:

- Permission for the processing of your personal data for one or more specific purposes.
- If the processing is necessary for the performance of an agreement to which you are a party, or to take measures at your request prior to the conclusion of an agreement;
- If processing is necessary in order to comply with a legal obligation that rests on the processor;
- If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the processor;
- If the processing is necessary for the protection of a legitimate interest of the processor or of a third party.

In the relationship between the employer and the employee, the fact that the employer must be able to execute the employment agreement, is generally the first principle that applies. Unlike in many other countries, the employee’s consent is generally

not considered a valid ground for processing personal data in the Netherlands, as it is not freely given (due to the unequal balance of power between employer and employee). The most important conditions are therefore the following:

- The employer has a legitimate interest to monitor which interest outweighs the privacy interest of the employee;
- The monitoring must be necessary in a sense that no other ways to reach the goal of the employer are available;
- The employer has informed the employee about its possibilities and rules in this respect beforehand. For example by implementing a protocol or code of conduct;
- The employer respects the right of the employee to communicate confidentially;
- The employer has acquired permission of the works council beforehand.

The legitimate interest of employers can be invoked as a legal ground, but only if the processing is strictly necessary for a legitimate purpose and the processing complies with the principles of proportionality and subsidiarity. A proportionality test should be conducted prior to the deployment of any monitoring tool to consider whether all data are necessary, whether this processing outweighs the general privacy rights of employees and what measures must be taken to ensure that infringements on the right to private life and the right to secrecy of communications are limited to the minimum. Employers must inform employees about the purposes for which their personal data is collected. Employees must be given the opportunity to access their data and, if need be, to correct, supplement or delete their data. They are entitled to request information on data held and may object to specific uses of their data. Furthermore, if a works council is established, it should render its consent for the monitoring.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

In principle, no. The conditions above apply towards all forms of monitoring. In general, the following can be added:

Email

With due regard to the above there is a general legal right of privacy of email correspondence and the employer's reading of the employee's private email is in principle not allowed.

Internet

Also, internet use by employees can be monitored without employee consent, as long on a random basis and as it cannot be traced back to individual visits. Data becomes 'personal' and therefore covered by data protection law only when it can be associated with an individual.

Telephone

In relation to telephone use, legislation permits the monitoring of telephone calls if there are legitimate operational reasons for doing so, such as for training purposes, individual assessment, as evidence of phone transactions, to control telephone costs or trace fraud.

CCTV (video monitoring)

In regard to video monitoring and surveillance, the capability to continuously capture the behaviour of the worker (especially with video analytics) and the monitoring of employees in order to establish a pattern of behavior would be disproportionate to the rights and freedoms of employees, and are therefore, generally unlawful. The processing is also likely to involve profiling, and possibly, automated decision-making. Therefore, employers should refrain from the use of facial recognition technologies. There may be some fringe exceptions to this rule, but such scenarios cannot be used to invoke a general legitimization of the use of such technology.

GPS Tracking

Monitoring using GPS services is, with due regard for the above under paragraph 1, only permitted to ensure the safety of the employee, preventing the car from theft or in case of a suspicion in regard to a criminal offense.



NORWAY

Contact

Braekhus Advokatfirma
Oslo - Norway
www.braekhus.no

JOHAN HVEDING
Partner | Employment
T: +47 902 04 995
E: hveding@braekhus.no



I. Is monitoring of employees permitted from a data protection and employment law perspective?

In general, an employer may monitor employees under Norwegian law if certain conditions are met. However, the employer's right to manage is restricted by several sets of rules, effectively securing employees right to privacy from a data protection and employment law perspective. In assessing what rights to privacy an employee has under Norwegian law, one must take into regard the following sources:

- The Working Environment Act chapter 9 regarding control measures in relation to employees
- The Personal Data Act and the Personal Data Regulations regarding the processing of personal data
- Non-statutory law supplies the statutory rules
- The Norwegian Constitution article 102: "Everyone has the right to the respect of their privacy and family life, their home and their communication."
- ECHR Article 8: "1. Everyone has the right to respect for his private and family life, his home and his correspondence."
- EU-Law (GDPR and European Charter of Fundamental Rights)

The employer may only implement control measures in relation to employees when such measures are objectively justified by circumstances relating to the undertaking and it does not involve undue strain on the employees. If there is a concrete suspicion of a criminal violation or a serious breach of duty, such measures are objectively justified. Other circumstances, e.g. health-related or security-related, may also constitute justifiable basis. In assessing whether monitoring puts undue strain on the

employee, the employee's privacy rights must be balanced with the employer's need for monitoring. Before implementing monitoring, the employer shall provide the affected employees with information concerning the purpose of the monitoring, practical consequences and the assumed duration of monitoring. Such information shall be given either directly to the employee, or indirectly through the employees' elected representatives. The employer shall also regularly evaluate the need for monitoring.

As the collection and/or storing of data on employees is considered data processing, such monitoring shall also comply with the rules set down in the Norwegian Personal Data Act and Personal Data Regulations. The new Norwegian Personal Data act comes into force during the summer 2018, effectively implementing GDPR into Norwegian law. Consequently, the basic principles regarding data processing set down in GDPR will apply as Norwegian law. During the transitional period, some legal aspects of the processing of data remain uncertain.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

Email

An employer may only explore, open or read email in an employee's email box

- a. When necessary to maintain daily operations or other justified interest of the business,
- b. In case of justified suspicion that the employee's use of email constitutes a serious breach of the duties that follow from the employment, or may constitute grounds for termination or dismissal.

Monitoring is considered necessary when the information is not accessible through less intrusive measures,

such as asking the employee directly. Additionally, the employer must pursue justified interests when monitoring the employees' email, e.g. the need for access to business-related emails when the employee is absent. The threshold depends on the gravity of the situation.

Normally, the employee enjoys weaker protection in case of justified suspicion that the employee's use of email constitutes a serious breach of the duties that follow from the employment, or may constitute grounds for termination or dismissal

Information comprised by the professional secrecy and correspondence between employees and employee representatives constitute additional exceptions from the employer's right to access.

Formally, there is no strict division between the use of email for private or business purposes. However, the purpose influences the assessment of whether access is necessary. Access to purely private emails will often be deemed not necessary to protect legitimate interests.

Certain procedural rules apply when accessing employees' email. The employee shall, insofar as this is possible, be notified and given an opportunity to speak before the employer makes the examination. In the notice the employer shall explain why the criteria are believed to be met and advise on the employee's rights. Insofar as this is possible, the employee shall have the opportunity to be present during the examination, and shall have the right to the assistance of an elected delegate or other representative. If the examination is made with no prior warning, the employee shall receive subsequent written notification of the examination as soon as it is done.

If examination of an email box reveals no documentation that the employer is entitled to examine, the email box and the documents it contains must be closed forthwith. Additionally, any copies must be deleted.

Internet

As with email, any monitoring of internet activity must be proportionate and necessary to pursue justified interests of the business. Certain additional restrictions apply. Continuous monitoring is not permitted. Employers are only entitled to monitor internet activity if the purpose of the monitoring is to administer the system or to uncover/clarify breaches of security. Other purposes cannot justify monitoring of internet activity.

CCTV (video monitoring)

The general prerequisites for monitoring also apply to CCTV, in addition to certain special regulations. As video surveillance is considered a strong interference in the employees' right to privacy, the use of such measures is also more restricted.

In general, in assessing whether video surveillance is objectively justified, one must particularly take into account whether the surveillance contributes to preventing serious or repeated criminal acts or safeguarding life and health.

Video surveillance of which the purpose is to uncover or to prevent legal offences is allowed if the surveillance is of substantial importance. In such cases, the employer has greater freedom to video monitor the employees, as the other prerequisites do not apply.

Video surveillance of a place which is regularly frequented by a limited group of people, e.g. the workplace, is only permitted if there is a distinct need for surveillance, e.g. to protect the safety of the employees and others or to prevent dangerous situations from arising.

When a place which is regularly frequented by a limited group of people is subject to video surveillance, attention shall be drawn clearly by means of a sign or in some other way to the fact that the place is under surveillance.

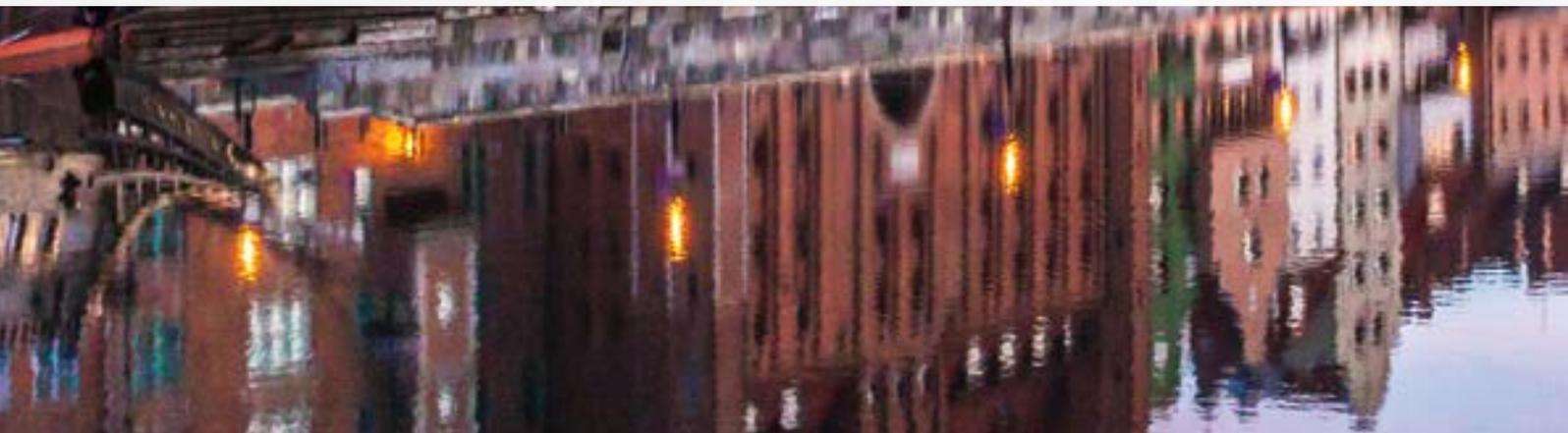
Additionally, the said regulations apply in cases when false video surveillance equipment is used.

GPS Tracking

The general prerequisites aforementioned apply to GPS tracking. GPS tracking is considered a weak interference in the employees' right to privacy. Consequently, GPS tracking is often deemed proportionate and objectively justified.



POLAND



Contact

Domański Zakrzewski Palinka
Warsaw, Poznan, Wroclaw - Poland
www.dzp.pl

BOGUSŁAW KAPŁON
Partner | Head of Labour Law
T: +48 61 642 49 81, +48 660 440 321
E: Boguslaw.Kaplon@dzp.pl



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the prerequisites for monitoring?

For many years there had been no specific regulation regarding monitoring of employees and a workplace. The above mentioned has changed on 25th May 2018 when new provisions of Polish Labour Code came into force. The new regulation was introduced by the Act on the Protection of Personal Data of 10th May 2018. The provisions of Polish Labour Code regarding monitoring in the workplace establish special requirements for implementing different forms of it. These regulations remains the only ones to which Polish employer shall refer while introducing monitoring. It is also essential to take into consideration personal rights of every person being monitored in the meaning of Polish Civil Code.

Having regard to the fact, that there was no transitional measures in the new provisions, the President of Personal Data Protection Office issued the guidance regarding CCTV monitoring and admitted that the real moment for being fully prepared to the new regulation as an employer shall be September 2018. Until this time, the authority would take into consideration only steps leading to fulfilment of obligations.

According to Polish Labour Code, monitoring is referred to workplace only. This means that there is no such term as “monitoring of employees” in Poland, nor is focusing on monitoring their performance of work allowed, e.g. by setting up camera in front of employee’s computer screen.

In terms of the prerequisites for monitoring, according to the aforementioned, there are different requirements for different types of monitoring. In general, there is a group of requirements which are:

- introducing the monitoring solutions is determined by defining a proper aim of it, resulting from the provisions of Polish Labour Code;
- using the monitoring in the way that does not infringe personal rights of employees, including a right to privacy;
- the data obtained by monitoring shall be retained for the properly established period of time;
- every employee must be informed about every form monitoring; in cases the workplace is also used by people not being the employees, it is essential to provide them with information pursuant to Article 13 of GDPR.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

Email

The circumstance justifying monitoring of employees’ e-mail is the necessity to provide proper organisation of work enabling the productive use of working hours and tools provided to the employee. Monitoring of an e-mail cannot infringe the secrecy of correspondence as well as other personal rights of an employee. Nevertheless, this does not imply that every e-mail of an employee is protected as a private correspondence. The employer still has the right to read business e-mails.

The scope of monitoring e-mails, the aim and the way of using this form of monitoring shall be stated in collective agreement, rules of work or, if none of these two apply - by notice. The employer is obliged to inform the employees about the monitoring not later than 2 weeks before its implementation. Every employee shall be informed about the monitoring on paper before the start of work.

Internet

Monitoring of Internet activity of employees is not regulated directly in the Labour Code, nevertheless it is considered to be one of “other forms of monitoring” to which the provisions regarding the monitoring of e-mails apply accordingly.

The circumstances justifying this type of monitoring is the necessity to provide proper organisation of work enabling the productive use of working hours and tools provided to the employee.

The scope of monitoring, the aim and the way of using this form shall be stated in collective agreement, rules of work or, if none of these two apply - by notice. The employer is obliged to inform the employees about the monitoring not later than 2 weeks before its implementation. Every employee shall be informed about the monitoring on paper before the start of work.

CCTV (video monitoring)

CCTV monitoring is regulated directly in Polish Labour Code. In order to implement it, a number of requirements are to be fulfilled.

The circumstance justifying monitoring of a workplace is to provide at least one listed below:

- safety of employees,
- protection of property,
- control of production,
- keeping in secret information which might cause the damage to the employer when revealed.

Video monitoring might cover the area of a workplace and the places around.

It is forbidden to use CCTV cameras in toilets, cloakrooms, canteens, smoking rooms or rooms made available for trade unions unless it would not harm the dignity of employees or their personal rights as well as the principal of trade union’s freedom e.g. by using special techniques making it impossible to recognise any person.

The scope of monitoring, the aim and the way of using this form shall be stated in collective agreement, rules of work or, if none of these two apply- by notice. The employer is obliged to inform the employees about the monitoring not later than 2 weeks before its implementation. Every employee shall be informed about the monitoring on paper before the start of work.

The employer shall mark the premises where CCTV is used by special signs (e.g. stickers) or sound announcement not later than 1 day before its activation.

GPS Tracking

Monitoring in the form of GPS Tracking is not regulated directly in Labour Code, nevertheless it is considered to be one of “other forms of monitoring” to which the provisions regarding monitoring of e-mail apply accordingly.

The circumstance justifying this type of monitoring is the necessity to provide proper organisation of work enabling to productive use of working hours and tools provided to the employee.

The scope of monitoring, the aim and the way of using this form shall be stated in collective agreement, rules of work or, if none of these two apply- by notice. The employer is obliged to inform the employees about the monitoring not later than 2 weeks before its implementation. Every employee shall be informed about the monitoring on paper before the start of work.



PORTUGAL

Contact

FCB Sociedade de Advogados
Lisbon, Porto, Faro - Portugal
www.fcblegal.com

INÊS ALBUQUERQUE E CASTRO
Partner | Employment, Benefits &
Pensions
T: + 351 213 587 500
E: ic@fcblegal.com

LEVI FRANÇA MACHADO
Associate | Employment, Benefits &
Pensions
T: + 351 213 587 500
E: lfm@fcblegal.com



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the prerequisites for monitoring?

Employers may not use remote monitoring mechanisms in the workplace by way of technological equipment for the purpose of monitoring the worker's professional performance. However, the use of such equipment shall be lawful where its purpose is the protection and security of people and goods (e.g. in a shop) or when particular requirements inherent to the nature of the activity so justify (e.g. places that need to be guarded or supervised).

Where monitoring is admitted, the employer shall inform the employees of the existence and purpose of the means of surveillance used, and shall publish a sign of such surveillance (e.g. "This place is under surveillance of an closed circuit television, proceeding to the recording of image and sound") followed by an identifying symbol.

The Labour Code protects the employee's right to privacy regarding personal messages. Nevertheless, this does not affect the employer's right to enforce policies on the use of IT tools. In any case, the employer is obliged to notify employees on the terms and restrictions of the use of company equipment and data processing.

Monitoring IT tools carry risks to the privacy of the employee and therefore should be carefully analysed and assessed on a case-by-case basis and accompanied by a set of measures that ensure a minimum level of intervention. Furthermore, control of the employees' movements during their free and personal time is inadmissible.

On the other hand, taking into account some duties of the employee (notably the duty of loyalty), employers may regulate off-duty conduct to the extent that it has a detrimental impact on the employment relationship, including in cases where the employee may disclose confidential information from the company or other content which might harm the reputation or interests of the company or respective co-employees.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

The general principle is that employees have a right to their privacy. However the employer has also the right to enforce policies on the use of company's email or internet.

As such and as rule, employers cannot monitor their employees' activity through the use of email / internet / CCTV or GPS tracking.

Email

Employers are able to enforce policies on the use of emails, notably stating that the use of the company's email for personal matters should be avoided and minimal.

Accessing the employees' emails must be a last resource measure and only in specific circumstances (e.g., employee who must be suddenly replaced or suspicion of frauds), and even in those cases the employer must avoid – as much as possible – to read the contents of personal emails.

Internet

Employers are allowed to enforce policies on the use of internet, notably by blocking the access to certain contents or by limiting the time that the employees are authorized to use the internet for personal purposes. The overall use of the internet can be monitored in order for the employer to understand if the rules are being complied.

CCTV (video monitoring)

Monitoring the employees' work through the use of CCTV is not admissible, unless such measure is necessary to protect them or the company's assets. Where monitoring is admitted, the employer shall inform the employees of the existence and purpose of the means of surveillance used, and shall publish a sign of such surveillance (e.g. "This place is under surveillance of an closed circuit television, proceeding to the recording of image and sound") followed by an identifying symbol.

GPS Tracking

GPS tracking is admissible in the companies' car but only to monitor their safety or the safety of any high-value goods in transport. GPS devices cannot monitor the employees' work. GPS trackers on mobile and / or personal computer are not allowed.



ROMANIA



Contact

Banu & Associates
Bucharest - Romania
www.brnlegal.ro

ROXANA ONUTA

Senior Associate
T: +40 21 210 65 55
E: roxana.onuta@brnlegal.ro



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the prerequisites for monitoring?

Considering the Romanian Law, the monitoring of the employees is permitted with respect to some cumulative conditions regarding the pursued interests by the employer, the preliminary information of the employees, the consultation of the trade union or of the representatives of the employees, the exhaustion of other monitoring means and the period of storage.

The specific legal provisions from this perspective are contained in Law no. 190/2018 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 of Directive 95/46 / EC (General Data Protection Regulation).

Thus, according to Art. 5 of the mentioned Law, where electronic monitoring and / or video surveillance systems are used in the workplace, processing of employees' personal data in order to achieve the legitimate interests pursued by the employer is only permitted if, in the first place, the legitimate interests pursued by the employer are duly justified and prevail over the interests or rights and freedoms of the person concerned.

The second condition provided by the law refers to the obligation of the employer to make a complete and explicit preliminary information of the employees.

Regarding this information, in our opinion, it is recommended a general information regarding the electronic

monitoring and / or video surveillance systems that would be included in the specific chapter from the Internal Rules of the company that would refer to the processing of personal data.

The specific information of the employee would be done for each employee concerned so that the employee would be aware regarding the monitoring fact, the ways and the purpose of monitoring, the modality in which the results are used and the period of storage these results, the possibility of formulating an internal appeal on monitoring and, of course, the possibility of the employee to complain to the National Supervisory Authority for Personal Data Processing, in accordance with the Decision no. 133/2018.

As a separate procedure and obligation, the employer needs to consult the trade union or, as the case may be, the representatives of the employees before the introduction of the monitoring systems.

The consultation will involve analysing and, if the conclusions are favourable, the implementation of the proposals of the trade union or employee representatives for a better policy of data processing and video monitoring.

According to the law, the electronic monitoring and / or video surveillance systems are permitted in the workplace only if all the other less intrusive forms and ways to achieve the scope pursued by the employer have not previously proved their effectiveness.

Thus, this would be the last solution the employer resorts to, when no less intrusive possibility can lead to the same result.

As a final condition, the storage period of personal data needs to be proportional to the purpose of the processing, but not more than 30 days, except in cases expressly regulated by the law or in duly justified cases.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

As mentioned in the answer to the previous question, Law no. 190/2018 includes, among others, specific rules for the processing of personal data in the context of employment relationships, referring in general to the monitoring of employees by electronic communications and / or video surveillance systems at the workplace.

So, considering that there have not been identified other specific provision depending on the form of monitoring, we appreciate the mentioned rules applicable for all the specified forms of monitoring (Email, Internet, CCTV - video monitoring under the GDPR, GPS Tracking).



SERBIA



Contact

Lalin Law Office
Novi Sad - Serbia
www.lalinlaw.com

IVAN KOVAČEVIĆ
Associate | Labour and Employment
T: +38 121 530 707
E: ivan@lalinlaw.com



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the prerequisites for monitoring?

Monitoring in the workplace, including video surveillance, e-mail monitoring, GPS tracking, monitoring employees' phone calls might be conducted to increase the efficiency of workers to protect employer legitimate business interests (business secrets for example), but if employees are monitored excessively or illegally, employee's right to privacy could be harmed.

As monitoring in workplace is very sensitive in respect with protection of employees private data, both employers and employees need to be familiar with the rules so as not to cross the delicate boundary between violating employee privacy and establishing a monitoring system.

The Constitution of the Republic of Serbia (hereinafter: the Constitution) guarantees the rights deriving from the right to privacy, among others, the right to protection of personal data. Furthermore, right to protection of personal data is further materialized under Law on privacy of personal data, all in line and in respect with principles established under European Convention of Human Rights. Law on privacy of personal data does not contain any provisions with respect to monitoring in workplace, nor does it provide any rules that regulate prerequisites for monitoring in workplace.

Monitoring of employees on their workplace e.g. collecting of personal data of employees by the employer, is not specifically regulated under Serbian Law on protection of personal data (nor under other regulation specifically aimed to provide rules for monitoring of employees in the workplace), so general legal regime and principles established under Law on protection of personal data is applicable irrespective of employment relationship.

The legal concept of personal data protection (as explained above also include protection of personal data of employees while monitored in workplace) includes the various right of employees: to know what their personal data are being processed, how they are processed, for what purposes, which entities have access to data and how employees can exercise their rights (right to insight and a copy of employee's personal data, the right to request a change of data or a temporary suspension of processing or deletion in case of unauthorized processing).

Regulatory body in charge for implementation and enforcement of law on protection of personal data, and also responsible to identify cases of abuse in respect with collection of personal data, including abuse of data collected in workplace, and to provide opinion as to whether a certain monitoring method constitutes specific risk for a citizen's (including employees) rights and freedoms is Commissioner for information of public importance and personal data protection.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

Having in mind that Serbian Law on protection of private data does not impose specific rules aimed to regulate monitoring in workplace, and considering growing need for specific regulations in respect to monitoring in workplace, Commissioner for information of public importance and personal data protection issued various opinions concerning, among other, monitoring in workplace.

Recently, the Commissioner for information of public importance and personal data protection also issued guidelines concerning protection of personal data in workplace covering whole area of privacy in workplace and collection and use of personal data of employees. Commissioner's guidelines provides rules specifically regulating various forms of monitoring in workplace.

Email and Internet

In respect with monitoring of business e-mails and use of Internet in workplace, the Commissioner's Guidelines recognise and justify employer's expectation that employees use their business e-mails and Internet only for the fulfilment of their work duties.

In that sense, since the business correspondence of the employee can be of significance to the employer, making copies of e-mail in the form of "backup" is absolutely acceptable, with the note that the making of copies and their storing on a particular memory unit does not necessarily involve performing an insight into the same.

In all other situations, and having in mind the fact that the employee, through his e-mail account, is still able to receive and send private mail, the Commissioner says, searching for official mail and conducting an insight into the same by the employer should be done in the presence of the employee himself, so that the employees would mark private messages and thus eliminate the danger that a third person will inspect in private correspondence.

On the other hand, the employee is obliged to abide by the employer's internal rules in respect of the assigned official email and even to refrain completely from using them for private purposes, in cases where a specific work process or a security aspect of daily work assignments, especially if the employers indicated in their internal rules, or the employees signed a statement that the business e-mails will be used exclusively for business purposes.

CCTV (video monitoring)

The Commissioner's Guidelines provides some rules concerning video monitoring, whereas video monitoring is not, as required by the Constitution, regulated by law.

Commissioner's Guidelines provides that starting from the standards of a democratic world, video monitoring can be done in business premises if it is necessary for the protection of security of persons or property, control of entry and exit from business premises, protection of classified information and business secrets.

In addition, video monitoring cannot or should not be done in a way that completely abolishes the right of the employee to the privacy of the workplace. Furthermore, it is necessary that the video monitoring zone be visibly marked, and it can only be performed in certain parts of the workspace, and it may not be done, for example, in rooms such as sanitary, wardrobes, etc.

Video monitoring cannot be used to control the implementation of employees' work obligations, but only to implement security measures in order to protect the property of employers and employees.

Employers are obliged to inform employees on video monitoring by setting up a notice that video surveillance is carried out in a specific area and leave a phone number that employees can call if they want to get more detailed information about the details of such monitoring.

GPS Tracking

GPS tracking has to be conducted in line with principles established under law on protection of private data.

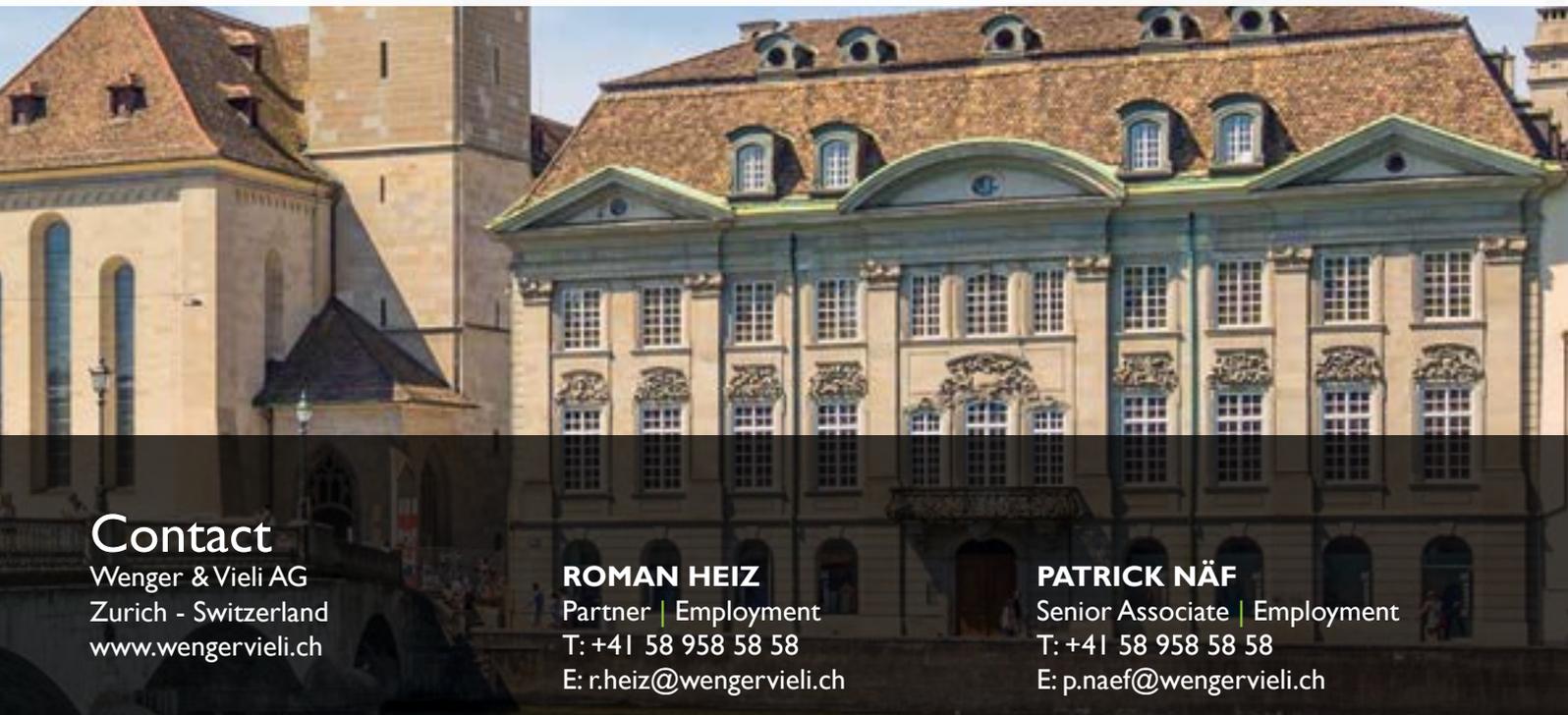
When GPS tracking is used, the employer must take into account the principles of data processing referred to in the Law of protection of private data, in particular the principles of legality, expediency and proportionality of processing, which means that, first of all, employer must have a valid legal basis for the intended GPS tracking (e.g. to obtain employees consent for GPS tracking), second, to implement proportionality for the purpose of the GPS monitoring (e.g. employer collects and continues to process only those data that are necessary for the accomplishment of the specified purpose of GPS monitoring, in the manner that at least threatens the right to privacy of employees).

Use of GPS tracking requires that the employer must, prior to intended GPS monitoring of employees, ensure that the such monitoring is justified, proportionate and properly designed, and to decide on the method of GPS monitoring suitable for achieving the intended purpose but least invasive for the privacy of employees.

In accordance with the aforementioned, from the point of view of the Law on protection of private data, the processing of personal data of employees by personal GPS locators by their employers, in a situation where the purpose of the processing would be to keep records of working time and its use, would be regarded as unauthorized, whereas prevention of misuse of employer's vehicles for private purposes shall be considered justified.



SWITZERLAND



Contact

Wenger & Vieli AG
Zurich - Switzerland
www.wengervieli.ch

ROMAN HEIZ
Partner | Employment
T: +41 58 958 58 58
E: r.heiz@wengervieli.ch

PATRICK NÄF
Senior Associate | Employment
T: +41 58 958 58 58
E: p.naef@wengervieli.ch



1. Is monitoring of employees permitted from a data protection and employment law perspective and what are the prerequisites for monitoring?

Monitoring of employees is only permitted for certain purposes and in compliance with the conditions set by the law. Generally prohibited is the monitoring of employees for the purpose of monitoring employees' behaviour only. However, monitoring of employees and the use of automatic control systems are permitted, if their use is justified by an outweighing, legitimate interest of the employer for instance if the monitoring is necessary for organisational or safety reasons or for the purpose of controlling a production process.

The monitoring measures have to be proportionate. This means that employers are required to implement monitoring measures in the least intrusive way and in such a manner that minimally infringes the employees' health and freedom of movement. For example, if a company wants to regulate the access to a certain building, it should prefer a badge access system over CCTV.

Employers must further be transparent about the monitoring system in place and must consult the workforce due to their employee participation rights. The monitoring measures must be disclosed in a written policy. If an employer fails to do act transparently, the monitoring of employees could be deemed unlawful and constitute an infringement of the employee's personality rights.

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

Email and Internet

The same principles as described under 1 apply.

It is highly recommended that the employer issues a general policy regarding the use of email and internet. This policy may then also regulate the possibility of and requirements for monitoring. As a general rule, if the employee is permitted to use e-mail for private purposes, the employer's right to monitor the emails is limited. The policy should be published in writing and brought to the employee's attention in a provable form (i.e. by written confirmation of receipt). Without such policy the employer may only monitor the emails systematically if there is a concrete suspicion of an abuse of the IT system or a criminal offense.

It is in principle not allowed to use key log software or content scanner software that monitor every single activity of an employee at the computer without a court order; as this would result in a prohibited conduct monitoring. This prohibition is not absolute; it is recognised that in some areas of the private sector, e.g. in banking a systematic monitoring of the email exchange has been deemed necessary in the past to comply with applicable compliance regulations.

CCTV (video monitoring)

As Switzerland is not a member of the EU, the GDPR does not apply to Swiss employment relationships.

CCTV is subject to the same general rules on monitoring as described under I. As monitoring by CCTV is highly intrusive, the use is to be applied very restrictedly. CCTV exclusively monitoring the employees' behaviour is not allowed. If it is inevitable to use CCTV where employees are working, the employer must position the cameras in a way that they principally focus on the production process and only occasionally film the employees.

GPS Tracking

The use of GPS is also only permitted if the preconditions named under I are fulfilled. The Swiss Federal Supreme Court has ruled that a GPS tracking system which monitored the movement of the cars of field staff during the working hours was legal. The Court found that the use of the GPS tracking system can be an appropriate and requisite measure to prevent the risk of abuse and to verify whether the employees carried out the customer visits properly. However, GPS tracking of the car must not extend to the employees' leisure time.



TURKEY



Contact

Yarsuvat & Yarsuvat Law Firm
Istanbul - Turkey
www.yarsuvat-law.com.tr

ELIFYARSUVAT KAYNAR
Partner | Employment, Criminal and
Privacy Law
T: +90 212 345 0600
E: elif@yarsuvat-law.com.tr

AYTUN BAYTEKIN HANER
Associate | Employment
T: +90 212 345 0600
E: ahaner@yarsuvat-law.com.tr



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the prerequisites for monitoring?

In Turkey, the monitoring of employees is permitted insofar as such monitoring does not infringe employees' privacy rights. These rights are governed by the following pieces of domestic legislation:

1. Law No. 6698 on the Protection of Personal Data (the "Data Protection Act"), which came into force on 7 April 2016, and
2. Articles 134-140 of the Turkish Criminal Code on the crime of violation of privacy,
3. Articles 20 and 22 of the Turkish Constitution, on the right to privacy and the freedom of correspondence, respectively.

In addition to privacy rights set out in domestic law, employees also enjoy the protection of Article 8 of the European Convention of Human Rights (ECHR) on the right to respect for one's private and family life. The protection afforded by Article 8 is upheld at the domestic level through the mechanism of individual applications to the Turkish Constitutional Court.

With regards the monitoring of employees at the workplace, the general principle enshrined in case law is that

- i. any measure which constitutes an infringement of an employee's right to privacy must be based on a legitimate purpose, and
- ii. the measure itself must be proportionate to the purpose sought.

In its *Ömür Kara and Onursal Özbek* judgment, dated March 3, 2016 (predating the Data Protection Law), the Turkish Constitutional Court held that:

"When balancing the interests of the parties and evaluating the proportionality of the measure [constituting an interference with the right to privacy], the courts must look at the manner by which restrictive and mandatory provisions of employment contracts are determined, whether the parties were notified of these provisions, whether the legitimate purposes on which measures interfering with employees' fundamental rights are based on are proportionate to the measures themselves (...) based on the facts of each individual case."

This general principle must, however, be interpreted in light of the recently introduced Data Protection Act. The Data Protection Act is based, for the most part, on Directive 95/46/EC (the EU Data Protection Directive). Under the Data Protection Act, processing of personal data is subject to the express consent of the data subject, save for the exceptions set out in the Act. These exceptions include, among others,

- i. processing of data in accordance with a provision of law,
- ii. processing of data for compliance with a legal obligation to which the data controller is subject, and
- iii. processing of data that is necessary for the legitimate interests pursued by the data controller, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

Under the Data Protection Act, data controllers are under an obligation to inform data subjects with regards the nature, purpose and grounds of the monitoring. This duty to inform is applicable even in cases where processing falls under one of the exemptions listed in the Act, whereby data can be processed without the need to acquire data subjects' express consent. Therefore, the general rule is that employees need to be notified of any form of monitoring implemented in the workplace.

Violations of the Data Protection Act entail severe administrative fines for employers, as well as criminal liability for violation of privacy under Articles 134-140 of the Turkish Criminal Code. (The latter applies only to real persons, such as directors of companies, as legal entities do not have criminal liability under Turkish law.)

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

Email

Monitoring of emails is permitted as long as this is in accordance with the abovementioned principles: The existence of a legitimate purpose on behalf of the employer and adherence to the principle of proportionality.

The Supreme Court and the Constitutional Court have consistently upheld the right of an employer to monitor corporate emails on company-owned equipment. This form of monitoring is considered proportionate in light of the employer's legitimate interests in maintaining efficiency at the workplace, limiting personal use of company equipment, acquiring evidence of criminal conduct or preventing transfer of confidential information to third parties.

One issue the courts will take into account when deciding on the issue of proportionality is whether employees are notified of email monitoring beforehand. This approach is in line with the duty to notify data subjects under the Data Protection Act, which imposes an obligation on data controllers to notify data subjects with regards the purpose, method and grounds of processing data.

Internet

The above principles on the monitoring of emails also apply to the monitoring of employees' internet activity. The monitoring of internet is permitted, but such monitoring ought to be proportionate and necessary for the legitimate interests of the employer. Furthermore, in accordance with the Data Protection Act, employers are required to notify employees that their internet activity is, or can be, monitored.

In a 2013 decision, the Supreme Court held that employers have a right to monitor internet activity other than corporate emails, such as the use of instant messaging applications for private chats.

CCTV (video monitoring)

As with email and internet monitoring, CCTV monitoring is permissible as long as employees are notified beforehand that the work premises are monitored via CCTV. Video footage of employees is considered personal data under the Data Protection Act, and can only be processed if data subjects are notified of the purpose, method and grounds of the monitoring.

The Supreme Court is yet to rule on the issue of whether employers need to acquire the express consent of employees for CCTV monitoring. However, it should be noted that the Data Protection Act allows the processing of personal data without express consent in cases where processing is necessary to protect the legitimate interests of the data controller and the processing of data does not violate data subjects' fundamental rights and freedoms. Therefore, given the approach of the courts with regards email and internet monitoring, it may be argued that overt CCTV monitoring during work hours is proportionate to the legitimate interests of the employer, such as ensuring safety in the work environment and preventing criminal conduct.

It should also be noted that the Data Protection Act allows processing of personal data in cases where processing is in accordance with a provision of law. Therefore, CCTV monitoring in work environments where employers are *required* by law to implement CCTV monitoring (such as shopping centres) is permissible without the need to acquire employees' express consent.

In the case of *covert* CCTV monitoring, satisfying the principle of proportionality will be a more difficult exercise. Under the Data Protection Act, covert surveillance in the workplace is permissible if the employee is notified of the purpose, method and legitimate grounds of such surveillance, and if the employee provides their express consent to covert surveillance. Covert surveillance in the absence of express consent by employees will only be deemed to be a proportionate measure for the protection of the employer's legitimate interests in extreme circumstances, such as the presence of a strong suspicion of criminal activity in the workplace.

One further issue worth highlighting is that under the Data Protection Act, consent is only valid if the data subject is fully informed of the nature of the processing they are consenting to and if consent is freely given. Therefore, consent given under threat of termination of employment, for instance, will not be considered valid under the Data Protection Act.

GPS Tracking

Similar to video footage obtained via CCTV monitoring, location data is considered personal data under the Data Protection Act. Therefore, employees, whose location data is obtained via a GPS tracking system, need to be informed beforehand of the purposes and grounds of GPS tracking.

With regards overt tracking via GPS, the same principles mentioned above in relation to overt CCTV monitoring apply: GPS surveillance will only be permitted where employees provide express consent to this method of monitoring, and covert GPS tracking in the absence of valid consent will only be permissible in extreme cases such as strong suspicion of criminal activity.



UNITED ARAB EMIRATES



Contact

BSA Ahmad Bin Hezeem &
Associates LLP
Dubai, Abu Dhabi, Ras Al Khaimah,
Sharjah - United Arab Emirates
www.bsabh.com

RIMA MRAD
Partner
T: +971 4 368 5555
E: rima.mrad@bsabh.com



I. Is monitoring of employees permitted from a data protection and employment law perspective?

The United Arab Emirates (the “UAE”) does not have a specific set of laws, regulations or guidelines addressing employee monitoring. As a general rule, however, employers have the right to monitor employees provided certain conditions are met:

- The employer’s purpose for monitoring an employee must be strictly related to work or legal purposes and not to their private or family life; and
- The employees must give their consent to be monitored and/or employees must be made aware that they are being monitored.

Although there are no laws regulating the monitoring of employees, certain regulations (UAE Constitution of 1971, Federal Law Number 3 of 1983 on the issuance of the Penal Code, Federal Decree-Law Number 5 of 2012 on Combatting Cybercrimes, and Federal Law by Decree Number 3 of 2003 regarding the Organisation of the Telecommunications Sector) grant employees a right to privacy. In practice, this has meant that employers can only monitor employees in so far as the monitoring does not impede on the privacy of their personal lives.

Two free zones in the UAE have issued their own data protection laws namely Abu Dhabi Global market (“ADGM”) and Dubai International Financial Centre (“DIFC”). Data protection in the ADGM is regulated by the 2015 Data Protection Regulations (as amended by the 2018 Data Protection Regulations). As for employee monitoring in the ADGM, it is covered by the ADGM Employment Regulations of 2015. In the DIFC, data protection is regulated by the DIFC Law Number 1 of 2007 and the DIFC Data Protection Regulations.

Employee monitoring is permitted in the ADGM. According to the ADGM Employment Regulations of 2015, employers are able to process personal data to monitor employees provided certain conditions are met. Processing the personal data of employees is only authorised if it is done for monitoring purposes required by law, if the processing is in the vital interest of the employees, or if it is in the legitimate commercial interest of the employers. Monitoring employees for training, quality assurance and safety purposes does fall under the scope of the legitimate commercial interest of the employer.

There are no specific guidelines on employee monitoring in the DIFC. But the DIFC Law Number 1 of 2007 on data protection does provide guidance on the processing of personal data. According to the DIFC Law Number 1 of 2007, in all circumstances where personal data is being processed, the processing will be authorized if it is required by law, if it is in the vital interest of the employee, if it is processed to pursue the legitimate interest of the data controller (of the third party, or of the parties to whom the data is disclosed), or if the data subject has given his written consent to the processing of the personal data (among other conditions).

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

Although not significant, different restrictions on monitoring do exist depending on the form of monitoring. Monitoring company property carries more lenient restrictions on the employer than CCTV monitoring does.

Email and Internet

As a general rule, employers are allowed to monitor an employee’s use of company-owned devices. This includes email servers, landlines, mobile phones, laptops, and other company-owned devices.

While there is no requirement for employers to have a written policy in place governing email and internet monitoring, it is still advisable for the employer to inform their employees of the company's right to supervise the employee's email and internet activities. This notice is generally done through the company's internal policies which the employee agrees to be bound by, or in the form of a provision included in their employment agreement.

CCTV (video monitoring)

Despite the fact that the use of CCTV remains largely unregulated for many sectors in the UAE, companies are widely equipped with these devices primarily for surveillance and security purposes. An individual's right to privacy will need to be taken into account when installing CCTV. If CCTV is installed in an office, it is recommended to make employees aware that they are being surveilled. This can be done by displaying a high-visibility sign, an identifiable video monitoring device, other forms of appropriate signage, or by announcing this directly to the employees. Recorded footage should not be used abusively by the employer. It should be noted that CCTV should only be installed in suitable places such as offices and meeting rooms, and not in private places like toilets and prayer rooms.

GPS Tracking

There are no laws addressing GPS Tracking in the UAE. Nevertheless, many businesses are required, due to the nature of the service they provide, to track the movement of their employees such as in the transportation industry (airlines, maritime transport, product transport) as a way to manage risk.

In these cases, however, the tracking device will usually be installed on the vehicle and not directly on the employee. Tracking an employee for unauthorised purposes, such as for finding out where they live or for any other matter unrelated to work and to the service provided, will be held as an invasion of an employee's privacy.



UNITED KINGDOM



Contact

Howard Kennedy LLP
London - United Kingdom
www.howardkennedy.com

SAM MURRAY-HINDE
Partner | Employment
T: +44 (0)20 3755 5619
E: sam.murray-hinde@howardkennedy.com

ALEX MIZZI
Senior Associate | Employment
T: +44 (0) 20 3755 5614
E: alexandra.mizzi@howardkennedy.com



I. Is monitoring of employees permitted from a data protection and employment law perspective and what are the prerequisites for monitoring?

Monitoring of employees, including CCTV, monitoring use of electronic and other communications systems and other forms of workplace monitoring, is lawful in the UK (and is fairly common practice) provided that obligations under data protection law and related laws are complied with. We have summarised the legal framework below.

Employee monitoring is governed by the following legal framework and principles:

- **Data protection law**
Employee monitoring almost inevitably involves processes of personal data and thus engages duties under UK and EU data protection law. The GDPR applies in the UK as to other EU member states. On the UK's departure from the EU on 29 March 2019, the GDPR will be transposed automatically into domestic legislation. The UK has also enacted the Data Protection Act 2018 which updates the previous Data Protection Act 1998. A core principle of the GDPR and Data Protection Act is that in order to process personal data a processor must have a lawful basis for doing so and must have made data subjects aware in advance that such data will be collected and the purposes for which it will be processed. Although UK employers in the past often relied on employee consent in order to process personal data, the GDPR emphasises that consent is unlikely to be effective in the context of the employment relationship and so another lawful basis for processing personal data of employees must be identified. In the context of employee monitoring the lawful basis is likely to be the 'legitimate interests' of the employer, but this entails balancing the employer's interests against the employee's privacy.

Stricter rules apply to the processing of special categories of personal data (such as data about gender, health or criminal convictions). If monitoring is likely to capture such data, this needs to be considered when determining whether a lawful basis for processing exists under the GDPR. In many cases a lawful basis will exist, but failing to consider this at the outset may expose the employer to stringent sanctions.

The GDPR stipulates that decisions which affect an individual's legal position (such as decisions about recruitment, disciplinary sanctions, promotion or dismissal) must not be based solely on automated processing – there must be a human actively interpreting the data collected and determining what consequences should flow from it.

In general, employers should carry out monitoring in the least intrusive way which achieves their lawful aims. It is also essential to have a written policy which sets out what monitoring is carried out and for what purposes, in order to comply with these data protection requirements. This should specify what systems are monitored, what categories of data will be collected and for what purposes. It should also set out for how long data will be retained before being deleted. In the absence of such a policy, monitoring is likely to be unlawful.

- **Employment Practices Code**
The Information Commissioner (the regulator responsible for data protection) issued a guide for employers called the Employment Practices Code. Although this has not yet been updated to reflect the GDPR, it is generally treated as indicative of the approach the regulator will take to any complaints about handling of employee data. The Code emphasises that employees must be told what monitoring is carried out in the workplace and that any monitoring must be proportionate and give proper weight to employees' privacy.

- **Human Rights Act 1998**
 The Human Rights Act 1998 incorporates the European Convention on Human Rights into English law. This includes the right to respect for private and family life under Article 8 of the Convention. Public authorities have direct obligations under the Human Rights Act but private sector employers do not. However, the courts are obliged to give effect to the Convention in interpreting English law, including employment law, so private sector employers are effectively caught too. This means, for example, that in an unfair dismissal case involving monitoring of the employee, the Employment Tribunal would need to take into account the employee's rights under Article 8 in assessing whether the dismissal had been fair.
- **Employment Rights Act 1996**
 The ERA 1996 is the source of many of the key employment law rights, including the right not to be unfairly dismissed. As set out above, in a case involving monitoring, the employee's privacy rights, the employer's compliance (or otherwise) with the Employment Practices Code and the extent to which any monitoring undertaken had been notified to employees may all be relevant in determining whether a dismissal was fair or whether the employer had fundamentally breached the employee's contract entitling the employee to treat themselves as dismissed (constructive dismissal).

2. Are there any differences or restrictions on monitoring depending on the form of monitoring?

Interception of certain forms of communication is governed by the Regulation of Investigatory Powers Act 2000, the Investigatory Powers Act 2016 and related regulations. Such interception (which includes recording of telephone calls but does not include monitoring of emails already read by an individual) is unlawful unless the individual has consented or certain other conditions are met.

It is also very important to consider potential criminal offences under the Computer Misuse Act - for example, hacking into an employee's personal email account may amount to such an offence, even if the employee had previously logged into that account using the employer's computer facilities.

However, in general the same principles apply to all forms of monitoring.

