GUIDANCE NOTE

Luxembourg - Employee Monitoring

Last Updated: 3 days ago

Emilia Fronczak
LOYENS & LOEFF

March 2026

1. Governing Texts

1.1. Legislation relevant to employee monitoring

- General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR).
- Act of August 1, 2018, on the Organization of the National Commission for Data Protection and Implementing the GDPR (the Act).
- Act of May 30, 2005, Laying Down Specific Provisions for the Protection of Persons with regard to the Processing of Personal Data in the Electronic Communications Sector and amending Articles 88-2 and 88-4 of the Code of Criminal Procedure, as amended (only available in French here) (the Electronic Communications Act).

- Labor Code (only available in French here) (the Labor Code).
- Collective bargaining agreement of October 20, 2020, on the legal regime of telework (only available in French here) - this agreement is of general application (Telework Agreement).
- Law of August 11, 1982, concerning the protection of private life (only available in French here) (Law of August 11, 1982).

1.2. Sector-specific legislation relevant to employee monitoring

No sector-specific legislation other than those highlighted in the previous section would be relevant for these purposes.

1.3. Guidelines from supervisory authorities

Already in 2014, the National Commission for Data Protection (CNPD) issued guidance regarding the monitoring of employees (available in French and German here). The guidelines were not updated following the adoption of the GDPR.

In addition, the CNPD issued guidelines on the processing of personal data for surveillance purposes through camera or video camera systems on August 14, 2018 (last updated on April 19, 2024, only available in French here) (Instruction 1/2006) and summary guidelines on cyber surveillance at work which were last updated on September 9, 2024 (available only in French here).

It is worth highlighting that under Luxembourg law, permanent surveillance is seen as disproportionate. Proportionality requires that employers proceed with incidental surveillance or progressive surveillance. Therefore, the employer shall first carry out general monitoring during which employees are not identified. If clues and suspicions are detected, the employer can then intensify its surveillance and carry out individualized analyses in which employees are identified.

Under the Labor Code, if a company has a staff delegation, it should be informed about the intention to put monitoring in place. If no staff delegation exists, the prior information should be given to the employees. The information shall detail the purposes of processing personal data, the operation mode of the monitoring, and the duration or the criteria used to decide on the storage

duration of personal data. The employer shall also formally confirm that personal data thus obtained will not be used for other purposes than those communicated. The staff delegation or the employees have 15 days to submit the draft information/policy to the CNPD for opinion. The CNPD has one month to issue its opinion, and during this period, the monitoring cannot be put into place.

We note that the employees concerned have the right to lodge a complaint with the CNPD. Such a complaint does not constitute valid grounds for dismissal.

1.4. Notable decisions, i.e. case law or decisions from supervisory authorities

There are no notable decisions from the CNPD with regard to employee monitoring.

There is no notable case law with regard to employee monitoring under the GDPR.

2. Telephone

2.1. What are the rules for recording telephone conversations?

Under Luxembourg law, no telephone calls can be recorded without the knowledge of the person called. As a general rule, Luxembourg law requires the consent of the person called, and only as an exception, calls can be recorded upon simple notification.

Therefore, it is not possible to record telephone calls for 'business quality, training, etc.' without the consent of the individuals whose conversation will be recorded.

As an exception, calls can be recorded upon simple notification to the data subject when the recording of communications and related traffic data is

carried out in the context of lawful professional practices, in order to provide proof of a commercial transaction. In this case, the parties to the transactions are informed in advance that recordings are likely to be made, of the reason(s) for which the communications are recorded, and of the maximum retention period of the recordings. Recorded communications must be deleted as soon as the purpose has been achieved, and in any event on expiry of the legal period for appealing against the transaction.

2.2. For which purposes may an employer carry out this type of monitoring?

The employer should, in principle, not record telephone conversations.

Only in exceptional cases, where the purpose of the recording is to provide proof of a commercial transaction, such recording could take place.

Such purposes could include:

- the need for proof of commercial transactions or communications in the event of a dispute;
- verification of commercial commitments agreed upon by telephone;
- confirmation of the details of an order/instruction to sell, buy, subscribe, deliver, etc.;
- the ability to listen again to instructions; or
- resolution of misunderstandings.

Where a telephone recording is put in place, the employer shall provide an unmonitored telephone line for employees for the purpose of private/personal communications.

2.3. Is prior notification/approval with the data protection authority required?

No, prior notification to the CNPD is not required, but the company must always comply with all relevant data protection obligations.

Processing activities that consist of or include regular and systematic monitoring of employee activities - provided that they might produce legal effects concerning the employees or similarly significantly affect them -

trigger the requirement to conduct a Data Protection Impact Assessment (DPIA). Whether a DPIA needs to be conducted shall be analyzed on a case-by-case basis.

2.4. Is prior notification/approval/consultation from works' councils required?

Yes. Without prejudice to the right to information of the person concerned, as specified above, the staff delegation should be informed about the intention to implement such monitoring to allow the staff delegation to provide their views.

For companies with more than 150 employees, such monitoring will in some instances have to be discussed and agreed upon with the staff delegation.

If the company has no staff delegation, the Inspectorate of Labour and Mines should be informed.

2.5. Is consent required from employees? If so, how should consent be sought?

No, prior consent is not required. Indeed, due to the imbalance between the parties in employment relations, consent is very rarely an appropriate legal basis, and it is doubtful that valid consent could be obtained for the processing of personal data for monitoring purposes. Given the employee's subordination, consent will in principle not be seen as freely given.

2.6. Is consent required from other parties to the call? If so, how should consent be sought?

Under Luxembourg law, in principle, the other party should consent to the recording of a telephone conversation.

If the recording falls under the abovementioned exceptions, the other parties to the call are informed in advance that recordings are likely to be made, of the reason(s) for which the communications are recorded, and of the maximum retention period of the recordings.

2.7. Is there a legal requirement for employers to have a written policy in place governing

telephone monitoring?

No, there is no legal requirement to have a written policy in place.

However, the company shall be able to demonstrate that the employees have been duly informed about the monitoring system and that they acknowledge the consequences of such a system, as well as the potential implications in case they do not comply with internal policies.

For this purpose, it would be advisable to provide the employees with a monitoring policy in writing and to collect a signed copy as evidence, or to include all the relevant provisions in the framework of the employment contract.

2.8. Are there any exemptions to the legal requirements which govern this type of monitoring?

No general exemptions apply; nevertheless, please note that these matters must be analyzed on a case-by-case basis.

2.9. What are the retention requirements applicable to data collected through telephone monitoring?

The data should be erased once the purpose for which it was collected has ceased. Therefore, once the contract is terminated, the processing should be suspended, and the data kept only for as long as the statutory limitations for the exercise of actions arising from the performance of the relationship last, or to comply with any legal obligation.

However, given the fact that the recording also concerns another caller, who is not an employee, the retention period shall be identified taking into account the overall purpose of this processing of personal data.

3. CCTV

3.1. What are the rules for CCTV surveillance?

As a general rule, under Luxembourg law, it is possible to carry out the processing of images collected by video-surveillance cameras to ensure the security of goods, people, and premises, provided that an area beyond that necessary to pursue said purpose is not recorded.

CCTV surveillance is subject to a two-tier information obligation.

First, any video-surveillance camera system should be advertised by a mandatory video-surveillance signpost, indicating:

- the existence of the processing of personal data;
- the controller's identity;
- the purposes of processing; and
- information that may be important for the data subjects.

Second, detailed information compliant with the GDPR requirements should be accessible to the data subjects.

Additionally, recourse to CCTV is possible only when the processing of images is proportional in relation to the purpose pursued, and no other measure is more suitable.

The minimization principle should be observed by limiting the number of video-surveillance cameras to those necessary for the relevant purpose, taking into account the specifications of each camera and their impact on employees' privacy (e.g., dome cameras, zoom, etc.).

External cameras installed in or around a building shall not capture the pavement, public road, or neighboring buildings.

Video surveillance systems are prohibited in spaces intended for employees' rest and other similar purposes, such as changing rooms, toilets, and canteen.

It is also prohibited to register sounds when registering images via CCTV.

3.2. For which purposes may an employer carry out this type of monitoring?

The main purposes are:

- protection of company assets (e.g., goods, installations, machines, buildings, confidential documents, etc.);
- safety of staff and customers;
- identification of perpetrators of thefts and assaults;
- security of access to the site or buildings;
- detection and identification of suspicious or dangerous behavior;
- identification of the source of an incident;
- organize and supervise the rapid evacuation of people in the event of an incident; and
- possibility to alert the emergency services, fire brigade, or police in good time and facilitate their intervention, etc.

However, the assessment of whether the purpose is sufficient to legitimize the recourse to CCTV surveillance is subject to the proportionality test.

3.3. Is prior notification/approval with the data protection authority required?

No, prior notification to the CNPD is not required, but the company must always comply with all relevant data protection obligations.

Processing activities that consist of or include regular and systematic monitoring of employee activities - provided that they might produce legal effects concerning the employees or similarly significantly affect them - trigger the requirement to conduct a DPIA. The location and context in which video surveillance cameras are used may impact the analysis of whether a DPIA shall be conducted.

3.4. Is prior notification/approval/consultation from works' councils required?

Yes. Without prejudice to the right to information of the person concerned, as specified above, the staff delegation should be informed about the intention to implement such monitoring to allow the staff delegation to provide their views.

For companies with more than 150 employees, in some instances, such monitoring will have to be discussed and agreed with the staff delegation.

If the company has no staff delegation, the Inspectorate of Labour and Mines should be informed.

3.5. Is consent required from employees? If so, how should consent be sought?

No, prior consent is not required. Indeed, due to the imbalance between the parties in employment relations, consent is very rarely an appropriate legal basis, and it is doubtful that valid consent could be obtained for the processing of personal data for monitoring purposes. Given the employee's subordination, consent will in principle not be seen as freely given.

3.6. Is there a legal requirement for employers to have a written policy in place governing CCTV surveillance?

No, there is no legal requirement to have a written policy in place.

However, the company shall be able to demonstrate that the employees have been duly informed about the monitoring system and that they acknowledge the consequences of such a system, as well as the potential implications in case they do not comply with the internal policies.

For this purpose, it would be advisable to provide the employees with a monitoring policy in writing and to collect a signed copy as evidence, or to include all the relevant provisions in the framework of the employment contract.

3.7. Are there any exemptions?

No general exemptions apply; nevertheless, please note that these matters must be analyzed on a case-by-case basis.

3.8. What are the retention requirements applicable to data collected through CCTV surveillance?

The data recorded by means of CCTV surveillance shall be erased within eight days of its collection.

Exceptionally, the employer may decide to keep data recorded by means of CCTV surveillance for 30 days. However, the reasons for such a retention period shall be duly documented in the register of processing activities.

In the event of an incident or offense, the images may be kept for longer than the above-mentioned period for the purposes of transmitting data to the competent authorities.

The CNPD recommends putting in place automatic erasure of the images.

4. Email

4.1. What are the rules regarding monitoring of employees' emails?

Under Luxembourg law, in accordance with Article 2(3) of the Law August 11, 1982, it is a criminal offense to violate the privacy of another person by opening, forwarding, or deleting a personal message sent or received without the consent of the person to whom it is addressed or by whom it is sent.

Regarding private use of emails, we may clarify that any email sent to or from a workstation provided by the employer is presumed to have been received or sent in the course of the employment relationship, i.e., the recipient or sender is deemed to be the employer. However, this is a simple presumption: the message may have the character of private correspondence if identified as such by the employee. In this case, the employer may not open the personal e-mails of the employees, as this will amount to a violation of the secrecy of correspondence, which constitutes a criminal offense. Therefore, the employers should instruct the employees to expressly and clearly mark private correspondence as 'Personal' or 'Private' and to archive personal messages in a folder called 'Private.'

Case law also admits that this prohibition on accessing private messages applies even where the employer has prohibited non-professional use of IT tools, as employees have a general fundamental right to privacy, which also applies at work. The principle of secrecy of correspondence may, however, be waived in the context of a criminal investigation.

If the employer wants to implement employee email monitoring to ensure business continuity in the employee's absence, the CNPD suggests implementing the following possibilities instead:

- set up an automatic out-of-office reply to the sender with an indication of who to contact in an emergency;
- appointment of an alternate employee who has personalized access rights to their colleague's mailbox (i.e., they can read and process work-related messages, but cannot read messages identified as personal); or
- transfer all incoming messages to the alternate employee. In any event, all employees must know the identity of their alternate, and such alternate can read and process work-related messages, but cannot read messages identified as personal.

We note that in practice set up of an automatic out-of-office reply is most common.

The CNPD suggests that, in the event of an employee leaving the company permanently, the departing employee:

- transfers all current business documents to a predefined person (e.g., their line manager);
- certifies that they have handed over all business documents to the employer; and
- copies emails and other documents of a private nature onto a private medium and then deletes them from the company's servers;

The employer undertakes to block all computer accounts and to delete the employee's mailbox(es) as soon as they leave the company. Thereafter, anyone sending a message to the blocked address will be automatically informed of the deletion of the e-mail address and given an alternative address.

With respect to access to personal messages, in principle, such access should take place in the presence of the relevant employee.

4.2. For which purposes may an employer carry out this type of monitoring?

The main purpose is to ensure the integrity of the devices, as well as to check that the IT tools provided by the company are correctly used.

However, the CNPD suggests that the employer shall first obtain traffic and log data such as the volume, frequency, size, and format of attachments. This information is checked without identifying the person concerned. If irregularities are detected, the employer can then proceed to identify the individuals concerned and check the content of work-related emails.

4.3. Is prior notification/approval with the data protection authority required?

No, prior notification to the CNPD is not required, but the company must always comply with all relevant data protection obligations.

Processing activities that consist of or include regular and systematic monitoring of employee activities - provided that they might produce legal effects concerning the employees or similarly significantly affect them - trigger the requirement to conduct a DPIA. Whether a DPIA shall be conducted shall be analyzed on a case-by-case basis.

4.4. Is notification/approval/consultation with works' council required?

Yes. Without prejudice to the right to information of the person concerned, as specified above, the staff delegation should be informed about the intention to implement such monitoring to allow the staff delegation to provide their views.

For companies with more than 150 employees, in some instances, such monitoring will have to be discussed and agreed with the staff delegation.

If the company has no staff delegation, the Inspectorate of Labour and Mines should be informed.

4.5. Is consent required from employees? If so, how should consent be sought?

No, prior consent is not required. Indeed, due to the imbalance between the parties in employment relations, consent is very rarely an appropriate legal basis, and it is doubtful that valid consent could be obtained for the processing of personal data for monitoring purposes. Given the employee's subordination, consent will in principle not be seen as freely given.

4.6. Is there a legal requirement for employers to have a written policy in place governing email monitoring?

No, there is no legal requirement to have a written policy in place.

However, the company shall be able to demonstrate that the employees have been duly informed about the monitoring system and that they acknowledge the consequences of such a system, as well as the potential implications in case they do not comply with the internal policies.

For this purpose, it would be advisable to provide the employees with a monitoring policy in writing and to collect a signed copy as evidence, or to include all the relevant provisions in the framework of the employment contract.

4.7. Are there any exemptions to the legal requirements which govern this type of monitoring?

No general exemptions apply; nevertheless, please note that these matters must be analyzed on a case-by-case basis.

4.8. What are the retention requirements applicable to data collected through email monitoring?

The data should be erased once the purpose for which it was collected no longer exists. Therefore, once the employment contract or the use of the monitoring tools is terminated, the data should be blocked and kept only for

the statutes of limitations of possible actions arising from the performance of the relationship, or to comply with any legal obligation.

If the monitoring is put in place for the monitoring of IT tools, the CNPD generally considers that a retention period of 6 months is sufficient to fulfill this purpose.

5. Biometrics

5.1. What are the rules regarding biometric monitoring?

No specific provisions regarding biometrics are envisaged in the Act.

The use of biometric systems by employers allows employers to check the identity of their employees. This objective can certainly be achieved by other methods, such as the use of badges or passwords.

Given the fact that biometric data is a special category of data, its use is subject to strict proportionality rules. Proportionality means that the employer must limit processing to data that is adequate, relevant, and not excessive in relation to the purposes.

The CNPD considers that monitoring systems using biometric data are very intrusive vis-à-vis data subjects and their fundamental rights and freedoms. To verify whether the use of biometric data is proportional, the CNPD makes a twofold distinction, on the one hand, between systems using biometric data that leave traces and those that do not, and, on the other hand, between systems that store biometric data centrally in a database and those that only store them in a decentralized manner, e.g., on a badge.

The CNPD has considered that the biometric data from employees should preferably be stored in a specific medium that can be held by the employee (e.g. a badge) rather than using a single IT system for storing the biometric data. This leaves the employee in control of the biometric data.

5.2. For which purposes may an employer carry out this type of monitoring?

The employer may wish to reinforce the protection of particularly sensitive areas of its premises, such as the server room, or to restrict access to premises containing hazardous products (e.g., viruses, chemical products, etc.).

Using biometrics to ensure that only authorized employees have access to certain parts of the premises allows for the implementation of a strong guarantee that only competent employees may access such premises, a guarantee which may be not as strong with other means of access control.

However, the assessment of whether the purpose is sufficient to legitimize the recourse to the processing of biometric data is subject to the proportionality rule, as detailed above.

5.3. Is prior notification/approval with the data protection authority required?

No, prior notification to the CNPD is not required, but the company must always comply with all relevant data protection obligations.

Processing activities that consist of or include regular and systematic monitoring of employee activities - provided that they might produce legal effects concerning the employees or similarly significantly affect them - trigger the requirement to conduct a DPIA. Whether a DPIA needs to be conducted shall be analyzed on a case-by-case basis.

As biometric data intended to identify an individual is considered a special category of data, a DPIA would always be mandatory in the event of processing biometric data on a large scale.

5.4. Is notification/approval/consultation with works' council required?

Yes. Without prejudice to the right to information of the person concerned, as specified above, the staff delegation should be informed about the intention to implement such monitoring to allow the staff delegation to provide their views.

For companies with more than 150 employees, in some instances, such monitoring will have to be discussed and agreed with the staff delegation.

If the company has no staff delegation, the Inspectorate of Labour and Mines should be informed.

5.5. Is consent required from employees? If so, how should consent be sought?

No, prior consent is not required. Indeed, due to the imbalance between the parties in employment relations, consent is very rarely an appropriate legal basis, and it is doubtful that valid consent could be obtained for the processing of personal data for monitoring purposes. Given the employee's subordination, consent will in principle not be seen as freely given.

5.6. Is there a legal requirement for employers to have a written policy in place governing biometric monitoring?

No, there is no legal requirement to have a written policy in place.

However, the company shall be able to demonstrate that the employees have been duly informed about the monitoring system and that they acknowledge the consequences of such a system, as well as the potential implications in case they do not comply with the internal policies.

For this purpose, it would be advisable to provide the employees with a monitoring policy in writing and to collect a signed copy as evidence, or to include all the relevant provisions in the framework of the employment contract.

5.7. Are there any exemptions to the legal requirements which govern this type of monitoring?

No general exemptions apply; nevertheless, please note that these matters must be analyzed on a case-by-case basis.

5.8. What are the retention requirements applicable to data collected for biometric monitoring?

The data should be erased once the purpose for which it was collected is no longer valid. Therefore, once the person concerned ceases to be authorized to enter the designated areas, the employment contract terminates, or the use of the monitoring tools ceases, the data should be blocked and kept only for the statutes of limitations of possible actions arising from the performance of the relationship, or to comply with any legal obligation.

It should be taken into account that the processing of biometric data (as a special category of data under the GDPR if used to identify an individual) is especially subject to the data minimization principle, and therefore to the storage limitation principle. In this sense, if for any reason the data is no longer being processed, analysis is required to see if the data needs to be erased. This would be the case, for example, for biometric data stored for access purposes, if another technology is used for such access (e.g., facial biometrics). In this scenario, the digital prints should be erased from any database if the relevant purpose can be achieved by other means (e.g., access log registry could be kept for security purposes, but only with code-related data, erasing the digital prints data from the database).

If the processing is put in place for access monitoring, the CNPD generally considers that a retention period of three months for the history of access from the date of their recording is sufficient to fulfill this purpose.

6. Device Monitoring

6.1. What are the rules regarding company-owned device monitoring?

The rules outlined in the section on email monitoring above are also applicable to this section.

Regarding private use of company devices, we may clarify that any document stored on a workstation provided by the employer is presumed to be employment-related. However, this is a simple presumption: the document may have a private character if identified as such by the employee. In this case, the employer may not open the document without the employee's presence. Therefore, the employers should instruct the employee to expressly and clearly mark private documents as 'Personal' or 'Private' and to archive them in a folder called 'Private.'

Case law also admits that this prohibition on accessing private documents applies even where the employer has prohibited non-professional use of IT tools, as employees have a general fundamental right to privacy, which also applies at work.

6.2. For which purposes may an employer carry out this type of monitoring?

The main purpose is to ensure the integrity of the devices, as well as to check that the IT tools provided by the company are correctly used.

However, the CNPD suggests that the employer shall first obtain traffic and log data such as volume, frequency, size, and format. This information is checked without identifying the person concerned. If irregularities are detected, the employer can then proceed to identify the individuals concerned and check the content of work-related emails.

6.3. Is prior notification/approval with the data protection authority required?

No, prior notification to the CNPD is not required, but the company must always comply with all relevant data protection obligations.

Processing activities that consist of or include regular and systematic monitoring of employee activities - provided that they might produce legal effects concerning the employees or similarly significantly affect them - trigger the requirement to conduct a DPIA. Whether a DPIA shall be conducted shall be analyzed on a case-by-case basis.

6.4. Is notification/approval/consultation with works' council required?

Yes. Without prejudice to the right to information of the person concerned, as specified above, the staff delegation should be informed about the intention to implement such monitoring to allow the staff delegation to provide their views.

For companies with more than 150 employees, in some instances, such monitoring will have to be discussed and agreed with the staff delegation.

If the company has no staff delegation, the Inspectorate of Labour and Mines should be informed.

6.5. Is consent required from employees? If so, how should consent be sought?

No, prior consent is not required. Indeed, due to the imbalance between the parties in employment relations, consent is very rarely an appropriate legal basis, and it is doubtful that valid consent could be obtained for the processing of personal data for monitoring purposes. Given the employee's subordination, consent will in principle not be seen as freely given.

6.6. Is there a legal requirement for employers to have a written policy in place governing company-owned device monitoring?

No, there is no legal requirement to have a written policy in place.

However, the company shall be able to demonstrate that the employees have been duly informed about the monitoring system and that they acknowledge the consequences of such a system, as well as the potential implications in case they do not comply with the internal policies.

For this purpose, it would be advisable to provide the employees with a monitoring policy in writing and to collect a signed copy as evidence, or to include all the relevant provisions in the framework of the employment contract.

6.7. Are there any exemptions to the legal requirements which govern this type of monitoring?

No general exemptions apply; nevertheless, please note that these matters must be analyzed on a case-by-case basis.

6.8. What are the retention requirements applicable to data collected from the company-owned devices?

The data should be erased once the purpose for which it was collected ceases. Therefore, once the employment contract or the use of the monitoring tools ends, the data should be archived and kept only for the statutes of limitations of possible actions arising from the performance of the relationship, or to comply with any legal obligation.

7. Covert Surveillance

In principle, the employer is obliged to inform the data subjects in a clear and unequivocal manner about the processing. The exceptions to this right concern notably processing necessary to safeguard national security, defense, public security, the prevention, investigation, detection, and prosecution of criminal offenses, etc.

In practice, these exceptions cannot be invoked by an employer to justify employee surveillance.

Therefore, in principle, covert surveillance by employers is prohibited.

In any case, it would be strictly forbidden to investigate employees' private lives occurring in their residences or other private places, as well as using any means that may harm the employees' right to honor, self-image, and intimacy, or the secret of communications or their personal data protection rights.

Nonetheless, in case any employer proceeds with covert surveillance, the evidence collected may not be admissible in legal proceedings, and any sanctioning measures adopted against the employee may be considered null and void.

8. Employees' Access Rights

The courts ruled that workers are entitled, in any event, to their right to privacy at the workplace, although this right can be restricted by employers in the legitimate exercise of their organizational and management powers. Employees must be entitled, at all times, to exercise those rights granted by the relevant data protection legislation.

These rights are:

Right to information and right to access their personal data

The employees may at any time request more information on the processing activities and the personal data the company processes.

Right to rectification of inaccurate or incomplete personal data

The employees have the right to require that, without undue delay, the company rectify or complete any of the employee's personal data that is inaccurate or incomplete.

Right to deletion of the personal data (right to be forgotten)

The employees may request that the company delete employee personal data or part thereof in the following situations:

- when the processing is no longer necessary for achieving the purposes for which they were collected or otherwise processed;
- when the processing was based on employee consent and the employee has decided to withdraw that consent;
- when the employee has other reasonable grounds to object to the processing of the personal data;
- when the company would unlawfully process the personal data; or
- when the personal data has to be erased in compliance with a legal obligation.

In some cases, the company may refuse to delete the personal data for exercising the right of freedom of expression and information; for compliance with a legal obligation; or for the establishment, exercise, or defense of legal claims.

Right to restrict processing

The employees may request that the company (temporarily) restrict the processing of their personal data in the following situations:

- when the employee has challenged the accuracy of the personal data, for a period enabling the company to verify this accuracy;
- when the processing appears to be unlawful, and the employee requests the restriction of the use of personal data instead of the deletion of this data; or
- when the company no longer needs the personal data for the purposes of the processing, but the employee needs them for the establishment, exercise, or defense of legal claims; or
- pending verification of whether the legitimate grounds override those of the employee in the framework of an objection.

Right to object to the processing of personal data (free of charge)

The employees may, under certain circumstances, object to the processing of personal data when such processing is based on the company's legitimate interests. If the company agrees, the company will no longer process the personal data, unless the company has compelling legitimate grounds to do so, or because such a processing is necessary.

Right to data portability

The employees have the right to receive all their personal data in a structured, commonly used, and machine-readable format and have the right to transmit those data to another controller, as this right applies:

- in case the processing is based on consent or on the necessity for the performance of a contract; and
- in case the processing is carried out by automated means.

9. Penalties

According to relevant data protection legislation, potential penalties may be up to €20 million. However, please note that the data subjects would also be entitled to initiate civil actions against the employer claiming compensation for damages.

In addition, employee monitoring that does not respect the requirements of the Labor Court constitutes a criminal offense punished by imprisonment of between eight days and one year and a fine of between €251 and €125,000, or by one of these penalties only.

The court to which the matter is referred may order the processing of personal data for monitoring purposes to be stopped, subject to a penalty payment, the maximum amount of which will be set by the said court.

Topics: Employee Monitoring

Jurisdictions: Luxembourg