GUIDANCE NOTE

Moldova - Employee Monitoring

Roger Gladei
GLADEI & PARTNERS



Tatiana Mocanu
GLADEI & PARTNERS



Last Updated: October 13, 2026

October 2026

1. Governing Texts

1.1. Legislation relevant to employee monitoring

- The Constitution of the Republic of Moldova
- The Labour Code of the Republic of Moldova of 28 March 2003 No. 154-XV (the Labour Code)
- The Law No. 133 of 8 July 2011 on the Personal Data Protection (the PDP Law)
- The Law No. 195 of 25 July 2024 on Personal Data Protection (Law No. 195/2024), which repeals and replaces the PDP Law and enters into force on August 23, 2026.

- The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (in force for the Republic of Moldova since 1 June 2008)
- The List of types of processing operations which are subject to the Data Protection Impact Assessment (DPIA), approved via the National Center for Personal Data Protection's (NCPDP) Order No. 27 dated 31 March 2022 (only available in Romanian here) (NCPDP Order No. 27)

Forthcoming legal framework:

This note describes the position under the PDP Law, which remains in force until August 22, 2026. With effect from August 23, 2026, the PDP Law is repealed and replaced by Law No. 195/2024, which substantially transposes the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR). The core requirements governing employee monitoring — a legitimate and explicit purpose (finality), transparency, proportionality, a DPIA for high-risk processing, designation of a data protection officer (DPO) where the relevant thresholds are met, and the data subject rights summarized in section 8 — are retained and reinforced under Law No. 195/2024, which also introduces enhanced accountability and documentation obligations (including records of processing activities). The corresponding article numbering, however, changes. Accordingly, references in this note to the PDP Law and to specific articles thereof should, for any processing taking place on or after August 23, 2026, be read against the equivalent provisions of Law No. 195/2024.

1.2. Sector-specific legislation relevant to employee monitoring

Not applicable.

1.3. Guidelines from supervisory authorities

Moldova's national data protection authority, the NCPDP, has issued the following guidance:

- Guidelines on the processing of personal data through video surveillance systems (only available in Romanian here);
- Guidelines on DPIA - only available in Romanian here);

- Recommendations for video surveillance system installation service providers in connection with their consultations offered to the final beneficiaries when installing video surveillance systems (only available in Romanian here);
- Practical and legal aspects related to the installation and management of means of video surveillance (only available in Romanian here);
- Considerations relating to the increasing use of video surveillance systems equipped with audio recording functions (only available in Romanian here); and
- Opinion on Processing of personal data in the context of the coronavirus pandemic (COVID-19) in the Republic of Moldova (only available in Romanian here).

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

There are no notable decisions from the supervisory authority or applicable case law.

2. Telephone

2.1. What are the rules for recording telephone conversations?

Moldovan legislation does not contain specific rules for recording the telephone conversations of employees.

However, employers must comply with Articles 5 and 6 of Law No. 195/2024, as well as Article 91 of the Labour Code (general provisions containing the requirements for the lawful processing of personal data). The main rules are:

- monitoring activity (including telephone conversation recording) must have a legitimate and explicit purpose that justifies the processing of personal data (the principle of finality);

- employees and their representatives must be familiar with the employers' internal rules on how employees' personal data is processed and stored and shall be informed about their rights and obligations in the field (the principle of transparency); and
- employers can monitor only employees' personal data which is appropriate, pertinent, and not excessive in relation to the purpose for which they are collected and/or further processed (the principle of proportionality).

Additionally, the controller may have the duty to perform the DPIA according to Article 35 of Law No. 195/2024 (the rules are similar to the ones imposed by the GDPR.

A DPIA is in particular required in the case of:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, or of personal data relating to criminal convictions and offenses; or
- a systematic monitoring of a publicly accessible area on a large scale.

The NCPDP has issued Order No. 27 with a list of cases when personal data operations are subject to the requirement to conduct an impact assessment. When performing the data DPIA, the controller shall obtain the written advice of the NCPDP.

Subsequently, employers shall designate a DPO (assuming the processing operations fall at least under one of the three legal criteria prescribed by PDP Law, outlined below).

Pursuant to Article 37 of Law No. 195/2024, the controller (employer) and its (sub)processors shall designate a DPO in any case where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope, and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data.

Telephone monitoring might fall under the above criteria, thus designating a DPO might be mandatory for employers. Subsequent regulatory orders issued by the NCPDP explain that 'on a large' scale means processing personal data of over 50,000 data subjects. Under Law No. 195/2024, which transposes the GDPR, processing on a 'large scale' is assessed qualitatively – having regard to the number of data subjects, the volume and range of data, the duration of the processing and its geographical extent – rather than by reference to a fixed numerical threshold. The figure of 50,000 derives from guidance issued under the PDP Law and should be treated with caution until NCPDP issues updated guidance under the new law. A separate legal assessment is recommended as regards the DPO designation, depending on the specifics of the processing operations planned by the employer.

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

There are no specific provisions for this matter.

As per Article 91 of the Labour Code, the purposes justifying the processing of employees' personal data are:

- fulfilling legal provisions;
- providing assistance in hiring, training, and promotions at work;
- ensuring the personal security of employees;
- controlling the volume and quality of work performed; and
- ensuring the integrity of business assets.

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

No notification/approval is required. However, within the process of performing the DPIA (in the described above cases) prior notification of the NCPDP is required.

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

Employee representatives (which sometimes can be in the form of works' councils) are to be consulted in the process of drafting the internal documents of a business (including the instructions/regulations regarding telephone monitoring), as per Article 91(h) and (j) of the Labour Code.

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

As per Article 6(1)(b) of Law No. 195/2024, the processing of personal data can be carried out without the consent of the personal data subject, if they have engaged in a contractual relationship, and the processing is necessary in order to execute the agreement. Thus, generally, employers are not required to obtain the consent of employees. Furthermore, pursuant to Article 9(2)(b) of Law No. 195/2024, even processing of special categories of personal data does not require the consent of the data subject as long as the processing is necessary for the performance of the specific obligations or rights of the controller in the field of labour law. However, the processing of these data must be carried out in accordance with the guarantees provided by law, and taking into account the fact that any disclosure to a third party of personal data processed for this purpose may only be made if the controller is legally obliged.

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

As per Articles 116(2) and 125 of the Electronic Communications Act No. 72 of March 10, 2025 (only available in Romanian here), it is prohibited for any person other than the user or users participating in the communication to listen to, record, store, or otherwise intercept or monitor communications and

the related traffic data without the consent of the user concerned, except in cases where the monitoring is carried out to defend the public interests, national security, or to investigate criminal offenses.

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

As per Articles 24 and 32 of Law No. 195/2024, employers shall have a data security policy. This policy shall contain the precise description of the security measures taken by the employer in order to secure the confidentiality of any personal data that is processed within its activity.

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

As per Article 23 of Law No. 195/2024, none of the above requirements shall apply if the processing of personal data is being carried out for the following purposes:

- national defense, state security, and the maintenance of public order; and/or
- the protection of the rights and freedoms of the personal data subject or any third person.

The exceptions will apply only if the application of the general requirements is detrimental to the effectiveness of the actions or the objectives pursued by the public authorities in the process of the execution of their legal obligations.

Please note public authorities must keep records about the application of the exceptions and shall inform the NCPDP within 10 days about the processed personal data. Under Law No. 195/2024, restrictions to data subjects' rights and to controllers' obligations must be provided by law and satisfy the specific conditions in Article 23, thus this ten-day notification requirement is not reproduced in Law No. 195/2024 and should be reverified against the new law and any implementing acts.

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

As per Article 5(1)(e) of Law No. 195/2024, the processed personal data must be stored:

- in a form that allows the identification of the personal data subjects; and
- for a period not exceeding the time required to achieve the purposes for which they are collected and subsequently processed.

The storage of personal data for a longer period, for statistical, historical, or scientific research purposes, shall be done in accordance with the guarantees regarding the processing of personal data provided by the rules governing these areas and only for the period necessary for the achievement of these purposes.

3. CCTV

3.1. What are the rules for CCTV surveillance?

The same rules as described in the section on rules for recording telephone conversations above, will apply.

Additionally, the NCPDP has published a series of advice in their guidelines on the processing of personal data through video surveillance systems according to which employers are required to:

- obtain the written consent of employees (in certain cases); and
- place an image (in a pre-set form approved by the NCPDP) next to each video camera.

Furthermore, it is forbidden for employers to:

- place hidden video cameras;

- place video cameras in areas where employees have a reasonable expectation of privacy, (e.g. bathrooms);
- audio recording through the video cameras;
- place video cameras in employee workspaces only if there is a legitimate reason to do so (such as for foreign exchange operators or bank employees);
- use video cameras to sanction employees or to track their time spent at work;
- zoom on a specific employee; and
- record public spaces without necessity.

Subsequently, employers shall designate a DPO (assuming the processing operations fall at least under one of the three legal criteria prescribed by PDP Law).

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

Unlike monitoring phone conversations, the employer may place video monitoring only under the grounds of Article 6(1)(f) of Law No. 195/2024, in order to achieve a legitimate interest (his direct interest or of the third party to whom the personal data are disclosed), provided that this interest does not prejudice the interests or fundamental rights and freedoms of the employees.

In this regard, the security of the employee's property could serve as a legitimate interest to place video monitoring. In fact, employers often place security cameras in order to protect their employees and property (for security purposes). The grounds under Article 91 of the Labour Code are more common for other types of monitoring, such as email monitoring or recording telephone conversations.

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

In general, no notification/approval is required. However, in some cases described by NCPDP and within the process of performing the DPIA the prior notification of the NCPDP is required.

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

No notification/approval/consultation from works' councils is required

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

The consent of the employees is not required, as the purpose of the video monitoring could only fall into one of the cases regulated by Article 6(1)(f) of Law No. 195/2024, exempted from the consent requirement.

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

The same rules as described in the section on legal requirement for employers to have a written policy in place governing telephone monitoring above will apply.

3.7. Are there any exemptions?

The same rules as described in the section on exemptions to the legal requirements which govern telephone monitoring above will apply.

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

The same rules as described in the section on retention requirements applicable to data collected through telephone monitoring above will apply.

4. Email

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

The same rules as described in the section on rules for recording telephone conversations above, will apply.

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

The same rules as described in the section on purposes employers may carry out telephone monitoring above will apply.

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

No notification/approval is required. However, within the process of performing the DPIA the prior notification of the NCPDP is required.

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

As described above for telephone monitoring, employee representatives, such as works' councils, must be consulted when drafting internal documents of a business, including those that relate to email monitoring.

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

The same rules as described in the section on employees' consent on telephone monitoring will apply.

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

The same rules as described in the section on legal requirement for employers to have a written policy in place governing telephone monitoring above will apply.

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

The same rules as described in the section on exemptions to the legal requirements that govern telephone monitoring above will apply.

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

The same rules as described in the section on retention requirements applicable to data collected through telephone monitoring will apply.

5. Biometrics

5.1. What are the rules regarding biometric monitoring?

The same rules as described in the section on rules for recording telephone conversations above will apply.

In addition, the monitoring of biometric data will mandatorily require the prior DPIA.

Subsequently, employers shall designate a DPO (assuming the processing operations fall at least under 1 of the 3 legal criteria prescribed by PDP Law).

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

The same rules as described in the section on purposes employers may carry out telephone monitoring above will apply.

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

Yes, within the process of performing the DPIA.

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

The same rules as described in the section on prior notification/approval/consultation from works' councils in case of telephone monitoring will apply.

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

Yes, employers must obtain prior consent from their employees before collecting their biometric data (unless the monitoring (processing) of the biometric data is required under the law).

Under Articles 4 and 7 of Law No. 195/2024, employees' consent means the manifestation of free will, express and unconditional, in written or electronic form, or by unequivocal and specific action, by which the employee agrees to the processing of personal data concerning him/her/them. This consent may be withdrawn at any time by the employee, although withdrawal of consent does not have retroactive effect (does not affect the lawfulness of personal data processing performed before the withdrawal).

In addition, employees must have alternatives offered by the employer in case they refuse to give consent for monitoring. For example, if the employer uses fingerprints/facial recognition to prevent unauthorized access to its premises, the employer must provide to, the employees refusing such monitoring alternative methods of authorization (e.g. access card/keys).

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

The same rules as described in the section on legal requirement for employers to have a written policy in place governing telephone monitoring

above will apply.

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

The same rules as described in the section on exemptions to the legal requirements which govern telephone monitoring will apply.

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

The same rules as described in the section on retention requirements above will apply.

6. Device Monitoring

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

The same rules as described in the section on rules for CCTV monitoring will apply. In addition, the all-time monitoring of the GPS location of the employees will mandatorily require the prior DPIA.

In addition, the employee must be informed in advance that the devices are not for personal use.

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

The same rules as described in the section on purposes employers may carry out CCTV monitoring will apply.

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

In general, no notification/approval is required. However, in some cases described by NCPDP and within the process of performing the DPIA the prior notification of the NCPDP is required.

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

The same rules as described in the section on prior notification/approval/consultation from works' councils above will apply.

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

The consent of the employees is not required. The same rules as described in the section on consent required from employees regarding CCTV monitoring will apply.

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

The same rules as described in the section on legal requirement for employers to have a written policy in place governing telephone monitoring above will apply.

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

The same rules as described in the section on exemptions to the legal requirements which govern CCTV monitoring will apply.

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

The same rules as described in the section on retention requirements applicable to data collected through telephone monitoring above will apply.

7. Covert Surveillance

As per Articles 2 and 27 of the Law on Special Investigations Activity No. 59/2012 (only available in Romanian here) covert surveillance of employees can be authorized only within a criminal process, and with prior authorization from competent judges.

Additionally, further to Article 9(1) of the Labour Code, employees have the right to be fully informed of the conditions of their activity. Thus, employers may not carry out covert surveillance.

8. Employees' Access Rights

As per the PDP Law, employees have the following rights:

- **the right to be informed** (Articles 13 and 14 of Law No. 195/2024): Employers are required to provide employees the following information:
  - the identity of the controller/the processor, as the case may be;
  - the purpose of personal data processing; and
  - any additional information, such as the rights of the employees concerning the protection of their personal data, the recipients of the personal data, and the possible consequences of denial to respond to questions made by the employer.
- **the right of access to personal data** (Article 15 of Law No. 195/2024): Employees have the right to obtain, free of charge, information regarding the data undergoing processing, and any other available information.

- **the right of intervention concerning their personal data** (Articles 16, 17, and 18 of Law No. 195/2024): Employees have the right to request the rectification, update, blocking, or erasure of personal data, the processing of which does not comply with the PDP Law, in particular due to the incomplete or inaccurate nature of the data held.
- **the right to object** (Article 21 of Law No. 195/2024): Employees have the right, at any time, and free of charge, to object to the processing of personal data related to them, if the processing is not in compliance with the law. Employees also have the right to object without any justification to the personal data relating to them for the purposes of direct marketing.
- **the right to data portability** (Article 20 of Law No. 195/2024): Employees have the right to receive the personal data concerning them which they have provided to the employer, in a structured, commonly used and machine-readable format, and to transmit those data to another controller, where the processing is based on consent or on a contract and is carried out by automated means. This right is newly introduced by Law No. 195/2024.
- **the right not to be subject to an automated decision** (Article 22 of Law No. 195/2024): Any person shall have the right to request for the rescinding, in whole or in part, of any individual decision, which produces legal effects concerning his/her rights and freedoms, and which, is based solely on automated processing of data intended to evaluate certain personal aspects relating to him/her such as his/her performance at work, creditworthiness, conduct, or other similar aspects.
- **the right of access to justice** (Articles 72 and 74 of Law No. 195/2024): Employees have the right to refer in a court in order to repair the possible material and moral damages.

9. Penalties

Non-compliance with the provisions of PDP Law could result in:

- Suspension of the employer's right to process personal data (the NCPDP's corrective powers under Articles 59 and 60 of Law No. 195/2024). If employers will not remove the circumstances that served as grounds for suspension within the set deadline, the NCPDP shall issue the decision to suspend the processing of personal data, with or without the provision of blocking or destruction of data unreliably or illicitly obtained;
- penalties ranging from €300 to €750 (Articles 74^1 - 74^3 of the Contravention Code No. 218-XVI of 24 October 2008 (the Contravention Code);
- the deprivation of the right to carry out certain activities for a period between three months and one year (Articles 74^1 - 74^3 of the Contravention Code); and
- tortious liability that can be invoked by any employees proving material and/or moral damages. of the employer's right to process personal data (Articles 59 and 60 of Law No. 195/2024). If employers will not remove the circumstances that served as grounds for suspension within the set deadline, the NCPDP shall issue the decision to suspend the processing of personal data, with or without the provision of blocking or destruction of data unreliably or illicitly obtained;
- penalties ranging from €225 to €750 (Article 74(1)-(3) of the Contravention Code;
- the deprivation of the right to carry out certain activities for a period between three months and one year (Article 74(1)-(3) of the Contravention Code); and
- tortious liability that can be invoked by any employees proving material and/or moral damages.

Penalties under Law No. 195/2024 (from 23 August 2026):

Administrative fines — two tiers (Moldova-specific caps, lower than the GDPR's): Law No. 195/2024 sets a two-tier structure mirroring the GDPR's split between procedural and core-principle breaches, but with its own ceilings: a lower tier of up to MDL 1 million (approx. $ 55,645) or for undertakings up to 1% of annual turnover, and a higher tier of up to MDL 2 million (approx. $ 111,290) or 2% of annual turnover, with the higher amount

being applied. 'Turnover' is total annual turnover as defined by reference to Competition Law No. 183/2012.

Phased (progressive) application in the first years: Because organizations get a runway, the fine that NCPDP calculates is only partially applied at first:

- August 23, 2026, to August 22, 2027, up to 10% of the calculated administrative fine;
- August 23, 2027, to August 22, 2028, up to 40%; and
- from August 23, 2028 onward: up to 100% of the calculated administrative fine.

Corrective powers alongside fines: Separately from monetary penalties, NCPDP has the corrective powers in Articles 59–60 (warnings, reprimands, orders to bring processing into compliance, temporary or definitive limitation or ban on processing, suspension of data flows), as detailed above.

Topics: Employee Monitoring

Jurisdictions: Moldova