Frandeș
LAW

26 Timișoara Blvd., Plaza Romania Offices
1st Floor, Offices 115-116, Sector 6, 061344, Bucharest
T: +40 746 426 538
E: office@frandes.law
W: www.frandes.law

IP, TECHNOLOGY & DATA PROTECTION · 13 NOVEMBER 2026

Does company size actually matter? GDPR, employers' obligations and the recent practice of the Romanian data protection authority

On the obligations that do not depend on headcount, the sanctions regime and the fines imposed over the last 12 months

IP, Technology & Data Protection · 13 November 2026

A company with a single employee or a neighbourhood shop is not exempt from the data protection rules. As a rule, the GDPR does not distinguish by number of employees.

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the GDPR) applies to every controller established in the European Union, whatever its legal form, turnover or headcount. The controller is the entity that decides why and how personal data are collected and used. The GDPR therefore applies to every company in Romania, however small or large.

In domestic law, Law no. 190/2018 on measures implementing the Regulation lays down special rules on the processing of the personal numeric code (CNP) and on the monitoring of employees. It, too, applies to every employer.

1. Obligations common to all controllers

The core of the obligations is the same for every controller. Each processing operation must have a lawful basis. Data subjects, whose data are processed, must be informed, and their requests must be dealt with within one month. Contracts must be concluded with processors. Processing must be secure, and personal data breaches must be notified to the National Supervisory Authority for Personal Data Processing (ANSPDCP), where feasible, within 72 hours at the latest.

Any differentiation by company size can arise only in respect of the obligations below. And even there, in reality, it arises at a single point.

2. What depends on headcount and what does not

a) Records of processing activities. This is a written document, in paper or electronic form, in which the organisation maps and inventories every process in which it collects, uses, stores or transmits personal data. For controllers with 250 or more employees, the records are mandatory. For those with fewer than 250 employees, the Regulation provides a derogation, in Article 30(5), but in practice the obligation is interpreted as applying to them as well. It is **the only obligation that distinguishes by number of employees**.

b) Designation of a data protection officer (DPO). Designation is mandatory, whatever the size of the controller, if its core activities consist of regular and systematic monitoring on a large scale or of large-scale processing of special categories of data. For security and video surveillance companies, for example, monitoring is the core activity. Likewise, telecommunications companies track traffic, geolocation through GSM relays, call history and communications metadata. Ride-hailing and transport apps track, on a large scale, GPS location, real-time routes and the movement patterns of customers and drivers. Profiling systems for targeted online advertising do the same. All of them carry out continuous, organised and extensive tracking of people's behaviour or actions.

c) Processing of the personal numeric code. Any employer that records and processes its employees' CNPs must comply with requirements of security, confidentiality, training and strict retention periods. If a company collects or processes the CNP of its customers or of other third parties on the basis of legitimate interest, it may do so only with special technical and organisational measures and **only if it designates a DPO**, under Article 4(2) of Law no. 190/2018. The typical example is a service provider that asks for its customers' CNP to make debt recovery easier, without a direct legal obligation to do so. The regime is the same for all controllers.

d) Monitoring of employees by electronic means or video. Under Article 5 of Law no. 190/2018, monitoring is permitted only if five conditions are met cumulatively: a duly justified and overriding legitimate interest, full and explicit prior information of employees, consultation of the trade union or of employee representatives, proven ineffectiveness of less intrusive means, and proportionate retention, of no more than 30 days, save for the exceptions provided by law. The conditions do not vary with the size of the employer.

e) Data protection impact assessment. It is mandatory before processing that is likely to result in a high risk, whatever the size of the controller.

> **The practical conclusion.** Company size does not exempt from liability. At most, it may exempt from a single documentation obligation, and the conditions for that exemption are rarely met.

3. The sanctions regime

The main administrative sanctions applied by ANSPDCP are the warning and the fine. In addition or separately, the authority may order corrective measures, including a limitation or a ban on processing.

For undertakings, the maximum fine depends on the nature of the infringement.

a) Obligations of the controller and the processor. Under Article 83(4) GDPR, the fine may reach EUR 10,000,000 or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

b) Principles of processing and data subjects' rights. Under Article 83(5) GDPR, infringements of the principles of processing, of the rules on lawful basis, consent and special categories of data, of data subjects' rights or of the rules on international transfers are subject to fines of up to EUR 20,000,000 or 4% of total worldwide annual turnover, whichever is higher.

c) Non-compliance with an order of the supervisory authority. Under Article 83(6) GDPR, the same statutory fine cap applies: up to EUR 20,000,000 or 4% of total worldwide annual turnover.

For public authorities and bodies, Article 14 of Law no. 190/2018 provides for fines of RON 10,000 to RON 100,000 and RON 10,000 to RON 200,000 respectively, depending on the nature of the infringement.

In setting the fine, regard is had, among other things, to the nature, gravity and duration of the infringement, its intentional or negligent character, the mitigating measures taken, the degree of cooperation and any previous infringements.

The report establishing the infringement and applying the sanction and the decision imposing corrective measures may be challenged before the administrative litigation section of the competent tribunal **within 15 days** of delivery or communication. Independently of the administrative sanction, a data subject whose rights have been infringed may claim compensation in court for the material or non-material damage suffered.

4. ANSPDCP practice over the last 12 months

The highest fines concerned insufficient security measures and direct marketing without consent. For employers, however, the most relevant cases are those involving the data of their own employees. The sanctions below are those made public by the authority and may be challenged in court.

October 2026 · Global Customer Care Services SRL · EUR 5,000. A cyberattack resulted in unauthorised access to the data of employees and former employees. ANSPDCP found an infringement of Article 32(1)(b) and (d) and Article 32(2) GDPR.

September 2026 · Tip Top Food Industry SRL · RON 26,236 (EUR 5,000). Time-keeping and access control were based on fingerprints, without a lawful basis for processing biometric data. ANSPDCP found an infringement of Article 5(1)(c) read together with Article 9 GDPR and ordered, as a corrective measure, the replacement of the biometric system.

August 2026 · Dormeo Home SRL · RON 10,517 (EUR 2,000). Commercial communications by text message and phone calls. This is the second sanction imposed on the same controller in the same year.

July 2026 · Orange România SA · RON 523,900 (EUR 100,000). Other customers' invoices were disclosed without authorisation through the mobile app, and a ticketing platform was publicly exposed, without VPN, two-factor authentication or IP restriction. ANSPDCP found an infringement of Article 25(1) and Article 32 GDPR.

June 2026 · Amato Bestseller SRL · RON 285,395 (EUR 54,361). Automated calls and commercial communications without the express consent of the recipients, in breach of the GDPR and of Law no. 506/2004. The controller received four fines.

March 2026 · Crowd Entertainment Limited · EUR 35,000. Commercial messages sent by gambling platforms. The controller had also been sanctioned at the end of 2025.

March 2026 · ING Bank NV Amsterdam – Bucharest Branch · RON 20,388 (EUR 4,000). The complainant's bank statement was released to a third party, against a background of inadequate security measures (Article 32 GDPR). As a corrective measure, ANSPDCP ordered regular staff training.

5. Checkpoints for employers

- **Records of processing activities.** Even for controllers with fewer than 250 employees.
- **A procedure for personal data breaches.** An internal procedure for handling incidents and notifying ANSPDCP within the 72-hour deadline.
- **Security of internal and publicly exposed platforms.** Multi-factor authentication, restricted access and regular testing of the effectiveness of the measures, under Article 32(1)(d) GDPR.
- **Biometric time-keeping and access control.** An exception under Article 9(1) GDPR is needed, together with a proportionality assessment showing that alternative means are not sufficient.
- **Video surveillance and monitoring of electronic communications.** The conditions in Article 5 of Law no. 190/2018 must be met cumulatively and documented before the system goes live.
- **Processing of the CNP on the basis of legitimate interest.** Designation of a data protection officer and the other safeguards in Article 4(2) of Law no. 190/2018.
- **Commercial communications.** Proof of consent, under the GDPR and Law no. 506/2004.

Conclusion

Most investigations start from a single complaint. In practice, the main line of defence is documented compliance.

Size is no defence. Documentation is.

Online version: https://www.frandes.law/en/insights/does-company-size-actually-matter-gdpr-employers-obligations-and-the-recent-prac.html