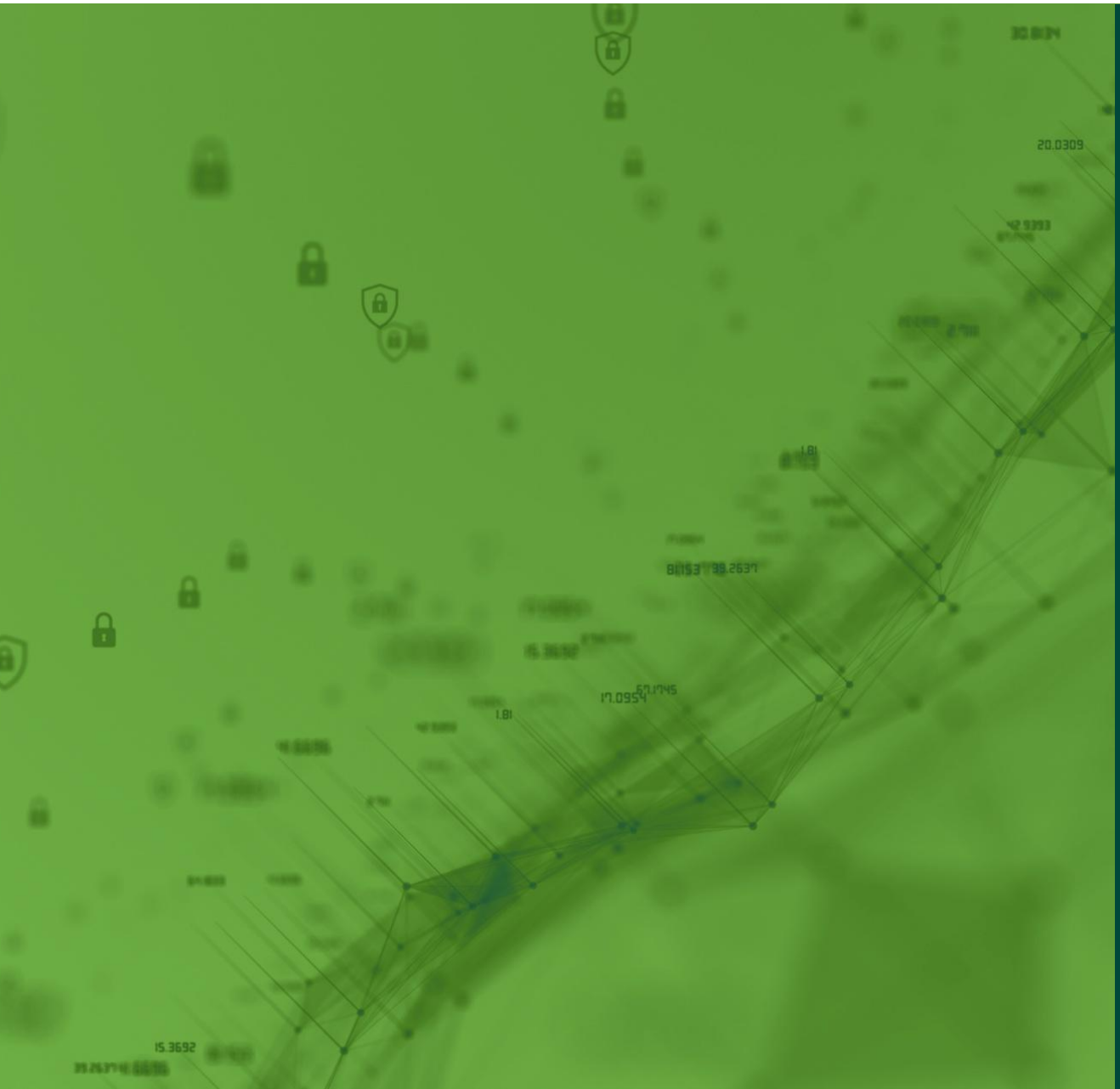
Nestor Nestor Diculescu Kingston Petersen
ATTORNEYS & COUNSELORS

Legal & Tax

Romanian DPA Report

A Year in Review - 2025



Romanian DPA case studies – our top 5 picks

1 Incomplete response to an access request involving CCTV footage

Case study: A customer filed a complaint with the Romanian DPA claiming that a financial institution had failed to fully comply with an access request. The Romanian DPA found that the controller had not demonstrated that it had provided a complete and individualized response covering the personal data and information concerning the customer. In particular, the controller had neither provided a copy of the personal data being processed nor sent its response to the address specified in the request. The DPA further concluded that the controller had not implemented adequate measures to enable data subjects to access CCTV recordings concerning them.

The controller was fined a total of EUR 11,000 and ordered to provide the customer with a complete and individualized response and a copy of the relevant personal data. It was also required to implement appropriate technical and organizational measures enabling access to CCTV recordings while protecting the rights of third parties. Both the Bucharest Tribunal and, subsequently, the Bucharest Court of Appeal upheld the sanction, with the latter's judgment being final. *(pages 58–60 of the Report)*

Why it is important: *This case highlights that controllers must provide a "complete and individualized response", adapted to the specific data and information concerning the individual, together with a copy of the personal data where required. This obligation also applies where the request concerns CCTV footage, as the presence of other individuals in the recording does not automatically justify refusing access. Instead, controllers are expected to adopt appropriate technical and organizational measures, including "software that allows information liable to adversely affect the rights and freedoms of others to be edited". The court upheld the DPA's findings, expressly confirming that "the infringement exists and was committed by the claimant".*

2 Unauthorized disclosure of payment card data following an e-commerce cyberattack

Case study: A controller operating in the tobacco products retail sector notified the Romanian DPA of a personal data breach following a cyberattack on its e-commerce platform.

The investigation revealed that the controller had failed to implement adequate security measures to ensure confidentiality of the personal data processed. The cyberattack, carried out by exploiting vulnerabilities in the platform, redirected customers to a fraudulent

payment page and resulted in the unauthorized disclosure of bank card numbers, cardholders' names and card expiry dates relating to a significant number of individuals.

Consequently, the DPA imposed a fine of EUR 20,000 and ordered the controller to implement a system for logging all access to its e-commerce platform, retain the resulting logs for at least 120 days and create backups of the log files. *(page 83 of the Report)*

Why it is important: *This case provides an indication that, depending on the circumstances, the Romanian DPA may expect access logs to remain available for at least 120 days. Although this period was imposed as a corrective measure in this specific case and does not constitute a general legal requirement, it may serve as a useful reference point when assessing whether log retention periods are sufficient to allow security incidents to be effectively identified and investigated.*

3 Inadequate security measures resulting in an employee data breach

Case study: A controller notified the Romanian DPA of a personal data breach involving unauthorized access to the personal data of a significant number of its employees following a cyberattack.

The DPA found that the controller had failed to implement adequate technical and organizational measures to ensure a level of security appropriate to the risk. The attack exploited password vulnerabilities and weaknesses in the process for resetting the authentication of a compromised user account. This resulted in the unauthorized disclosure of employees' names, internal employee numbers, work e-mail addresses, departments, job titles, office addresses, account creation dates and country codes.

Consequently, the DPA imposed a fine of EUR 10,000. However, no corrective measures were ordered, as the Authority considered the measures implemented by the controller following the incident to be adequate. *(pages 83–84 of the Report)*

Why it is important: *This case shows that the measures adopted following a personal data breach may influence the enforcement action taken by the Romanian DPA. Although the controller was fined EUR 10,000, the DPA did not impose any corrective measures, considering the measures implemented after the incident to be adequate. This suggests that prompt and effective remediation, while not precluding the imposition of a fine, may limit the need for further corrective action by the Authority.*

4 "Aggressive person" flag deemed personal data and processed without a lawful basis

Case study: A complainant reported to the Romanian DPA that a courier company had failed to comply with his requests for access and erasure. Among other information, the complainant had requested an explanation regarding an "aggressive person" flag associated with his data in the company's internal system, as well as the deletion of that flag.

The DPA found that the "aggressive person" flag constituted personal data, as it concerned an individual who could be identified by reference to the other information held in the company's database. In line with the Court of Justice of the European Union's (CJEU) judgment in Case C-434/16, the DPA noted that opinions and assessments concerning the behaviour or abilities of an identifiable individual may constitute personal data. The DPA further considered that the legitimate interest in protecting employees from potential risks had to be balanced against the individual's right to privacy, particularly as such a flag could be added arbitrarily following an unrecorded telephone conversation and could restrict access to the company's services. In this context, the DPA concluded that the company had not demonstrated a lawful basis for processing the flag and had failed to delete it following the complainant's request.

Consequently, the DPA imposed fines totalling EUR 4,000 and ordered the company to provide a complete response, reassess whether collecting and retaining the "aggressive person" flag was necessary, and implement measures to ensure the proper handling of data subject requests. The company challenged the sanction, and the case is currently pending before the courts. *(pages 109–111 of the Report)*

Why it is important: *This case highlights that internal notes and labels, such as "aggressive person", may constitute personal data where they relate to an identifiable individual. Referring to the CJEU's judgment in Case C-434/16, the Romanian DPA emphasized that opinions and assessments concerning an individual's behaviour or abilities may fall within the definition of personal data. The case therefore indicates that recording such assessments requires a legal basis and an assessment of their necessity and appropriate retention period, particularly where they may affect the individual's access to services. It also confirms that recording an assessment as an internal note does not place it outside the scope of the rights of access and erasure.*

5 Access request submitted at an incorrect e-mail address

Case study: A complainant reported to the Romanian DPA that a gambling company had failed to respond to an access request concerning his user account.

The investigation found that the requests had been sent to an e-mail address other than the DPO contact address displayed on the company's websites and had therefore not been

received by the controller. The company also provided screenshots documenting searches performed across all its platforms using the complainant's full name and surname, which did not identify any associated account. It further explained that a user could only be identified with certainty through the unique identifier required when creating an account.

No sanction was imposed, and the Romanian DPA communicated the outcome of its investigation to the supervisory authority in the complainant's country of residence. *(pages 124–125 of the Report)*

Why it is important: *This case shows that, when assessing an alleged failure to respond to an access request, the Romanian DPA may consider both whether the request was received and whether the controller can demonstrate the steps taken to locate the relevant data. In this case, the DPA took into account the searches carried out across all the controller's platforms, together with its explanation that a user could only be identified with certainty through the unique identifier required when creating an account. The case also underlines the importance of clearly communicated contact channels and keeping appropriate records of internal searches where the individual or the requested data cannot be identified.*

Statistics on complaints, notices (Romanian: *sesizări*) and data breach notifications received by the authority

1 Statistics

Category	2025	2024
COMPLAINTS		
Complaints Received	11,278	4,887
Investigations Opened	332	258
– Fines Issued	46	29
– Fine Amount (RON)	584,320 RON	485,077 RON
– Fine Amount (EUR)	116,500 EUR	97,500 EUR
– Reprimands	91	100
– Corrective Measures	118	89
NOTICES & DATA BREACHES		
Notices Received	814	297
Data Breach Notifications Received	202	170
– Fines Issued	50	51

– Fine Amount (EUR)	357,500 EUR	237,600 EUR
– Reprimands	54	61
– Corrective Measures	64	91
Total (Complaints + Notices + Breaches)	**12,297**	**5,354**
– Total Fines Issued	**96**	**83**
– Total Fine Amount (RON)	**2,565,020 RON**	**1,855,807 RON**
– Total Fine Amount (EUR)	**511,400 EUR**	**335,100 EUR**
– Total Reprimands	**145**	**161**
– Total Corrective Measures	**182**	**180**

2 The most frequent cases of complaints

- Processing of personal data in breach of the principles of lawfulness, fairness and transparency, as well as the lawfulness requirements under Articles 5 and 6 GDPR;
- Infringements of data subject rights, particularly the rights of access and erasure;
- Disclosure of personal data to third parties in the public space, online, including on social networks;
- Processing of personal data through video surveillance systems, including between individuals, in residential buildings and in the workplace;
- Sending unsolicited commercial communications by e-mail, telephone or other means.

3 The most frequent cases of notified data breaches

- Unauthorized disclosure of and/or unauthorized access to personal data, particularly online or following a ransomware attack;
- Failure to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Failure to ensure that individuals acting under the controller's authority process personal data only on the controller's instructions, particularly in the financial and banking sector;
- Breaches of online data confidentiality resulting from the inadequate configuration of websites or applications;
- Unauthorized access to closed-circuit television (CCTV) systems.

4 The most frequent cases of notices

- Misconfiguration of applications using databases containing personal data, resulting in their public exposure, with or without their indexing by search engines;
- Video surveillance/monitoring of the operator's own employees;
- Disclosure of personal data without the consent of the data subjects;
- Compromised confidentiality of personal data due to failure to comply with the principles of privacy by design and privacy by default, as a result of insufficient testing of IT applications prior to their deployment in the production environment and their default monitoring in the production environment;
- Implementation of an employee access control system based on biometric data (fingerprints).

Other statistics

Category	2025	2024
Requests received for points of view on matters related to the protection of personal data	934	882
Legislative drafts on which the Romanian DPA issued its notice	84	99
Cases pending before the Court of Justice of the European Union in which the Romanian DPA has issued its opinion	25	15
Files pending in court dealt by the Romanian DPA, out of which:	195	173
– New claims	55	55
– Claims against acknowledging/sanctioning minutes of the Romanian DPA	35	16
Preliminary complaints received by the Romanian DPA from persons unsatisfied with the answer of this authority; in the context of the administrative dispute resolution procedure, out of which:	27	50
– Accepted preliminary claims	9	9

Multinational companies that made requests analyzed by the Romanian DPA for the approval of binding corporate rules - BCRs	35	40

The press release is available **here** and the 2025 Annual Report is available **here** (both available only in Romanian).