Nestor Nestor Diculescu Kingston Petersen
ATTORNEYS & COUNSELORS

Legal & Tax

35 YEARS ANNIVERSARY

Romanian DPA Report - A Year in Review - 2024

Romanian DPA case studies – our top 5 picks

1

Refusal to provide actual call recording and provision of transcript only

Case study: A customer filed a complaint with the Romanian DPA, claiming that a mobile phone company had denied her right of access by refusing to provide the recording of a phone conversation she had with one of its employees about an offer. The company justified its refusal by stating that calls to/from its Customer Service line are used only for improving services, as evidence or for legal requests from authorities.

The DPA found that the customer had requested access to her personal data (her voice in the call recording) while the data was still available in the company's systems, within the storage period set by the controller. The investigation confirmed that the controller had not provided the requested audio recording. The DPA noted that, as a rule, a copy of the actual recording must be provided and only exceptionally – for example, if both the individual and the controller agree – may access be granted via a transcript. The controller was sanctioned with a warning. *(page 83-84 of the Report)*

Why it is important: *This case highlights that, as a rule, individuals are entitled to receive a copy of their own calls when exercising their right of access. Providing a transcript may be acceptable from the perspective of the Romanian DPA only as an exception to this rule. While the DPA gives one example (where both the data subject and the controller agree), the wording suggests that this is not the only situation envisaged by the authority. It is important to note that, according to the DPA, a copy of the recording/document does not have to be provided in all cases. It remains to be seen whether the Romanian DPA will fully align its practice with the case law of the Court of Justice of the European Union (CJEU), which clearly distinguishes between a "copy of the data" and a "copy of the documents."*

2

Lack of website transparency and cookie consent

Case study: The Romanian DPA received a complaint about a commercial website that did not provide information regarding users' GDPR rights or its cookie policy. The investigation found that the website did not clearly display the identity of the controller responsible for personal data processing.

In addition, cookies were installed when accessing the website before the user had given consent, even if these cookies were not technically necessary for the website's operation. The DPA sanctioned the controller with a warning for failing to provide transparency and a fine of RON 10,000 for installing non-essential cookies without consent. *(page 68 of the Report)*

Why it is important: *The Romanian DPA shows increased interest in the matter of cookie-related compliance. Since 2023 only, according to public sources, it applied no less than 3 fines and one warning in the context of cookie-related violations. While the amounts are not high, the fact that certain violations can be easily identified simply by accessing a website increases the risks for organizations.*

3 Delayed and inadequate response to access and deletion requests

Case study: A complainant reported to the Romanian DPA that an entertainment event organizer failed to respond to his repeated requests to exercise his rights of access and deletion of personal data. The investigation revealed that the controller responded only after six months, confirmed the deletion of the complainant's data, but did not provide the information requested under his access rights.

During the investigation, the controller justified the delays by citing emails ending in the *"spam"* folder, internal restructuring and the recruitment of a new data protection officer. These explanations were rejected, as the controller did not demonstrate that it had monitored and managed incoming requests appropriately during the restructuring period, nor did it provide alternative contact channels to ensure timely responses. Redirecting the complainant to the company's privacy policy was also deemed insufficient, as it did not provide individualized information regarding the processing of his personal data.

The controller was sanctioned with an EUR 10,000 fine for failing to provide access to personal data and an EUR 5,000 fine for inadequate handling of deletion requests and corrective measures regarding the necessary technical and organizational measures were imposed as well. *(pages 80-82 of the Report)*

Why it is important: *Organizations should establish a clear internal workflow to ensure that the relevant personnel know, among other things, where data subject requests can be received, who must be notified internally, and within what timeframe a response must be provided. Clear internal procedures and regular trainings are essential. Under the GDPR, the general rule is that requests must be answered within one month, the Romanian DPA shows that a response after six months is clearly too late.*

4 Improper employee surveillance through laptop monitoring application

Case study: A complainant notified the Romanian DPA that their employer, a debt collection company, had tested employee monitoring software on laptops used by remote workers. The software tracked internet activity, application usage, productivity and workplace presence and could potentially collect data such as document titles, web pages visited, search history and personal identifiers.

Although the software was no longer in use and had only been tested with limited access, the employer did not demonstrate that less intrusive methods previously used were ineffective. Furthermore, the employer failed to inform or consult employees before implementing the monitoring software. The DPA determined that the employer's actions violated employees' rights to privacy and protection of personal data and issued a formal warning. *(pages 97-99 of the Report)*

Why it is important: *This case shows that demonstrating the ineffectiveness of less intrusive means requires solid internal analyses, such as data protection impact assessments (DPIAs) or legitimate interest assessments (LIAs). Employers must be able to justify monitoring measures with strong arguments, especially as employees are increasingly aware of their rights. Even if the Romanian DPA applied only a warning, the employers must be aware of a potential reputational risk in this type of cases.*

5 Unauthorized disclosure of e-mail addresses due to missing BCC

Case study: A complainant reported to the Romanian DPA that a mobile company had unauthorizedly disclosed her personal email address to multiple recipients. The emails, sent over two separate months, included multiple recipients, and the controller did not use the "*BCC" (blind carbon copy)* function to hide recipients' addresses, which resulted in the disclosure of the email addresses to the other recipients.

The investigation found that the controller had not implemented adequate technical and organizational measures to ensure the confidentiality of personal data. Consequently, the DPA imposed a fine of EUR 5,000 and required the controller to reevaluate its security measures, including staff training and regular compliance checks. *(pages 92-93 of the Report)*

Why it is important: *Disclosing the identity of an e-mail recipient to unauthorized persons (even if they are included in the same communication) may create risks for that recipient, depending on the content and context of the message. Organizations should therefore provide adequate instructions to their staff (through trainings and internal policies) on how to send e-mails to multiple recipients and on the data breach risks that may result from failing to observe this rule.*

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

I. Statistics

- **4.887 complaints** received *(as compared to 4.380 complaints in 2023)*;
- based on them, **258 investigations** were opened *(as compared to 207 investigations in 2023)*, resulting in:
  - **29 fines** totally amounting to RON 485.077 (equivalent of EUR 97.500) *(in 2023, there were 39 fines applied, totally amounting to RON 717,102 (equivalent of EUR 144,150)*;
  - **100 reprimands** *(as compared to 120 reprimands in 2023)*;
  - **89 corrective measures** *(as compared to 80 corrective measures in 2023)*;
- **297 notices** and **170 data breach notifications** received *(as compared to 211 notices and 181 data breach notifications in 2023)*;
- based on them, **342 investigations** were opened *(as compared to 341 investigations in 2023)*, resulting in:
  - **51 fines** totally amounting to EUR 237.600 *(as compared to 31 fines in 2023 totally amounting to EUR 309.900)*;
  - **61 reprimands** *(as compared to 66 reprimands in 2023)*;
  - **91 corrective measures** *(as compared to 58 corrective measures in 2023)*;
- in total: **5,354 complaints**, **notices** and **data breach notifications** received *(as compared to 4,772 in 2023)*;
- based on them, **476 investigations** were opened *(as compared to 548 investigations in 2023)*, resulting in:
  - **83 fines** totally amounting to RON 1.855.807 – approx. EUR 335.100 *(as compared to 73 fines in 2023, totally amounting to RON 2,348,265 – approx. EUR 472,041)*;
  - **161 reprimands** *(as compared to 186 reprimands in 2023)*;
  - **180 corrective measures** *(as compared to 138 corrective measures in 2023)*.

II. The most frequent cases of complaints

- Failure to respect the rights of data subjects;
- Violation of data processing principles;
- Disclosure of personal data to third parties in the public space, online, including on social networks;

III. The most frequent cases of notified data breaches

- Illegal processing of personal data as a result of sending copies of several employees' identity documents by email;
- Violation of data processing principles;
- Disclosure of personal data without the consent of the data subjects;

IV. The most frequent cases of notices

- Confidentiality/availability/integrity of data affected as a result of the unauthorized disclosure or as a result of a cyber incident such as a ransomware attack;
- Confidentiality of personal data in the online environment;
- Loss of confidentiality and unauthorized access to personal data (including medical data) in the online environment;

V.

Other statistics

- **882 requests** received for points of view on matters related to the protection of personal data *(as compared to 970 requests in 2023)*;
- **99 legislative drafts** on which the Romanian DPA issued its notice *(as compared to 103 legislative drafts in 2023)*;
- **15 cases pending before the Court of Justice of the European Union** in which the Romanian DPA has issued its opinion *(as compared to 21 cases in 2023)*;
- **173 files pending in court dealt by the Romanian DPA** *(as compared to 155 files in 2023)*, out of which:
  - **55 new claims** (as compared to 47 new claims in 2023);
  - **16 claims** against acknowledging/sanctioning minutes of the Romanian DPA *(in 2023, from 47 new claims, 28 were against such minutes)*;
- **50 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; 9 of such preliminary complaints were accepted *(in 2023, 28 preliminary complaints were received and 5 were accepted)*;
- **40 multinational companies** made requests analyzed by the Romanian DPA for the approval of binding corporate rules - BCRs *(as compared to 14 companies in 2023)*.

The press release is available **here** and the 2024 Annual Report is available **here** (both available only in Romanian).