



Nestor Nestor Diculescu Kingston Petersen  
ATTORNEYS & COUNSELORS

Legal & Tax



# Romanian DPA Report - A Year in Review - 2023

## Romanian DPA case studies – our top 5 picks

1

### Unlawful disclosure of a photo

→ **Case study:** A doctor complained to the Romanian DPA that the public hospital where she is employed published her personal data without her consent. The hospital (acting as controller) published the personal data of the doctor (including her photo, together with her name, surname and the title of doctor) on its webpage ( “Doctors” section).

The Romanian DPA considered that the public hospital violated the GDPR requirements by publishing the photo of the doctor without an adequate legal ground and applied the sanction of warning. (pages 86-87 of the Report)

→ **Why it is important:** *Any processing of data (even the processing of data which may seem usual or unarmful) must rely on a legal ground. To the extent the processing is based on a legitimate interest (as it may seem to be the case in this situation), the controller must also prepare a legitimate interest assessment substantiating the reasons of data processing and proving that its legitimate interests are not overridden by the rights, freedoms and interests of the data subjects (the doctors in this case).*

2

### Processing personal data of own employees for the purpose of redirecting income tax

→ **Case study:** Several data subjects complained about receiving pre-filled tax forms from their employer (acting as data controller). During the investigation, the Romanian DPA found the controller had partially filled in Form 230 (i.e., a voluntary declaration that employees can fill to redirect up to 3.5% of their income tax to non-profit organizations, religious institutions, or private scholarships, supporting social causes or education) with employee data, i.e. name, surname and personal identification number, without being legally obliged to do so and without proving that any of the conditions of legality of processing had been met. The employees received the form prefilled with their data, the designated beneficiary being a foundation belonging to the controller.

The Romanian DPA concluded that the controller has failed to process the personal data of its employees with the observance of the lawfulness principle imposed by the GDPR and applied a fine of EUR 5,000 (in RON equivalent). (page 63 of the Report)

- **Why it is important:** *When processing personal data, even when it is made to ease employees' work, controllers must always ensure that such processing (i) observes the principles laid down in the GDPR and (ii) is based on a legal ground of processing.*

## 3

## Disclosure of personal data by a group of company employees

- **Case study:** A company acting in the retail industry filed a data breach notification following the unauthorized disclosure of CCTV footage by a group of company employees. The employees of the controller recorded with their personal phones the screen on which the CCTV footage was being recorded and then transmitted the footage to an unauthorized person, the latter uploading the footage on social media. The incident resulted in the disclosure of an individual's image, license plate number, vehicle color and mark, which led to the loss of confidentiality of personal data.

The Romanian DPA found that the controller failed to implement adequate technical and organizational measures to ensure an adequate level of security appropriate to the processing risk. The authority applied a fine of EUR 8,000 (in RON equivalent) and imposed on the controller the corrective measure of implementing monitoring solutions aimed at preventing similar incidents in the future. (pages 66-67 of the Report)

- **Why it is important:** *The organizations may be held liable for the acts of their personnel. Therefore, they must implement adequate organizational measures to ensure that their personnel know how to deal with the processed data (e.g., by holding periodical trainings and adopting adequate internal policies and procedures). Moreover, the organizations must implement adequate technical systems limiting access of the personnel to the processed data (e.g., strictly on a need-to-know basis and according to their role). The measures must not only be declarative, but also implemented effectively and tailored to the specific activity of the organizations.*

## 4

## Failure to offer support to the DPO

- **Case study:** The Romanian DPA received a complaint from a data protection officer (DPO), the latter claiming that the organization where he acted in this capacity (a public institution) violated the DPO-related provisions from GDPR.

The Romanian DPA found that the public institution did not offer the needed support to the DPO in (i) carrying out his duties of monitoring the GDPR compliance and (ii) accessing the personal data and the information on data processing activities. The DPA applied a warning, also imposing upon the public institution the obligation to offer the needed support (for example, issuing a decision applicable to the

departments/structures of the public institution to put at the disposal of the DPO the required information on personal data and data processing activities). (page 55 of the Report)

- **Why it is important:** *The DPO does not have a decorative role but is a key actor in ensuring the data protection-related compliance within the organization. Providing the DPO the necessary information and documents related to data processing must not be neglected, as failure to do so may lead to compliance gaps.*

## 5

## Unlawful GPS-related monitoring

- **Case study:** An individual complained that his employer installed a GPS monitoring system on the vehicles used by its employees without informing them. Moreover, the complainant indicated that the information collected via GPS was used in a court case in which the complainant was involved.

During the investigation, the Romanian DPA found that the GPS monitoring system was used outside the working hours, while the employer was not able to prove that (i) it had exhausted all the less intrusive means for reaching the same objective and (ii) it had adequately informed the individuals on such GPS monitoring. Moreover, the employer could not prove the justified reasons which would allow to keep the GPS-collected data for more than the 30-day maximal term provided by law.

The Romanian DPA applied in this case fines amounting to EUR 5,000 in total. (pages 85-86 of the Report)

- **Why it is important:** *The controllers must be particularly careful when deciding to use GPS systems and must be able to prove that less intrusive means would not have been efficient for attaining the same purpose. This is all the more important if the controllers intend to (i) undergo GPS monitoring outside the working hours and (ii) keep the GPS-collected data for more than 30 days. The adequate information of data subjects is a particularly important measure, considering the level of intrusiveness.*

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

## I.

### Statistics

- › **4380 complaints** received (as compared to 3,899 complaints in 2022);
- › based on them, **207 investigations** were opened (as compared to 281 investigations in 2022), resulting in:
  - **39 fines** totally amounting to RON 717,102 (equivalent of EUR 144,150) (in 2022, there were 25 fines applied, totally amounting to RON 253,382.28 (equivalent of EUR 51,300));
  - **120 reprimands** (as compared to 90 reprimands in 2022);
  - **80 corrective measures** (as compared to 60 corrective measures in 2022);
- › **211 notices** and **181 data breach notifications** received (as compared to 198 notices and 155 data breach notifications in 2022);
- › based on them, **341 investigations** were opened (as compared to 314 investigations in 2022), resulting in:
  - **31 fines** totally amounting to EUR 309.900 Euro (as compared to 44 fines in 2022 totally amounting to EUR 160,090);
  - **66 reprimands** (as compared to 44 reprimands in 2022);
  - **58 corrective measures** (as compared to 33 corrective measures in 2022);
- › in total: **4,772 complaints, notices and data breach notifications** received (as compared to 4,260 in 2022);
- › based on them, **548 investigations** were opened (as compared to 629 investigations in 2022), resulting in:
  - **73 fines** totally amounting to RON 2,348,265 – approx. EUR 472,041 (as compared to 69 fines in 2022, totally amounting to RON 1,058,863 – approx. EUR 213,122);
  - **186 reprimands** (as compared to 134 reprimands in 2022);

- **138 corrective measures** (as compared to 93 corrective measures in 2022).

## II. The most frequent cases of complaints

- Image processing through CCTV systems;
- Receipt of unsolicited commercial messages;
- Failure to respect the rights of data subjects;

## III. The most frequent cases of notified data breaches

- Privacy of personal data in the online environment due to misconfiguration of websites/software applications used by controllers;
- Disclosure of data on the internet;
- Unlawful access to video monitoring systems (CCTV);
- Disclosure of data in the healthcare system;
- Processing of personal data through the use of mobile video surveillance (body-cam).

## IV. The most frequent cases of notices

- Confidentiality/availability/integrity of data affected as a result of the unauthorized disclosure;
- Privacy of personal data in the online environment due to misconfiguration of websites/software applications used by controllers;
- Unlawful access to personal data of clients from the banking system;
- Processing of personal data through the video monitoring systems;
- Disclosure of personal data in the healthcare system.

## Other statistics

- › **970 requests** received for points of view on matters related to the protection of personal data *(as compared to 948 requests in 2022)*;
- › **103 legislative drafts** on which the Romanian DPA issued its notice *(as compared to 107 legislative drafts in 2022)*;
- › **21 cases pending before the Court of Justice of the European Union** in which the Romanian DPA has issued its opinion *(as compared to 30 cases in 2022)*;
- › **155 files pending in court dealt by the Romanian DPA** *(as compared to 108 files in 2022)*, out of which:
  - **47 new claims** *(as compared to 40 new claims in 2022)*;
  - **28 claims** against acknowledging/sanctioning minutes of the Romanian DPA *(in 2022, from 40 new claims, 22 were against such minutes)*;
- › **28 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; 5 of such preliminary complaints were accepted *(in 2022, 26 preliminary complaints were received and 6 were accepted)*;
- › **14 multinational companies** made requests analyzed by the Romanian DPA for the approval of binding corporate rules - BCRs *(as compared to 34 companies in 2022)*.

The press release is available [here](#) and the 2023 Annual Report is available [here](#) (both available only in Romanian).

*Note: This document should not be copied, disclosed, distributed or reproduced, in whole or in part, without the prior written consent of Nestor Nestor Diculescu Kingston Petersen. The contents of this document are for information purposes only and should not be relied upon or construed as legal or other kind of advice.*