25.05.2022

May 25, 2022 - ANSPDCP activity

On May 25, 2022, it will be four years since the application of the General Data Protection Regulation (EU Regulation no. 679/2016 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of of these data and of the repeal of Directive 95/46/CE - RGPD), which marked a turning point in ensuring uniform rules in the community space.

On this occasion, we emphasize the fact that, during the four years of application of the RGPD, operators in the public and private environment continued to put into practice the rules for the processing of personal data, especially those regarding the information of natural persons, to the effective compliance of the rights of natural persons (the right of access, the right to rectification, the right to deletion - "the right to be forgotten", the right to restrict processing, the right to data portability, the right to opposition, the right not to be the subject of a decision based solely on automatic processing, the right to file a complaint with a supervisory authority), to ensure the confidentiality and security of personal data processing.

The National Supervisory Authority continued the activity of monitoring and control regarding the legality of personal data processing.

The significant number of complaints, referrals and requests for views received during the four years demonstrates an increase in the level of awareness of the general public regarding the rights they benefit from, as well as the interest of operators in complying with European rules.

In the context of the celebration of four years since the application of the GDPR, we present a summary of the most significant aspects of the activity of the National Supervisory Authority carried out during the first four months of 2022.

Thus, in the first four months of 2022, the National Supervisory Authority received 1345 complaints, notifications and notifications regarding security incidents, based on which 129 investigations were opened.

As a result of the investigations carried out during this period, 17 fines were imposed in the total amount of 169,158 lei (the equivalent of 35,100 euros).

Also, in the control activity, 34 warnings were applied and 23 corrective measures were ordered.

As for the complaint resolution activity, the National Supervisory Authority received in the first four months of the current year 1235 complaints, based on which 80 investigations were started.

In the same period, data operators submitted 48 notifications regarding data security breaches and 62 notifications regarding possible non-compliance with the provisions of the GDPR. As a result of these, 49 ex officio investigations were started.

The complaints, reports and notifications regarding security incidents received by the National Supervisory Authority during this period mainly concerned the following aspects:

- image processing through video surveillance systems,
- violation of the rights of the persons concerned,
- violation of the principles provided for by RGPD,
- receiving unsolicited commercial messages,
- disclosure of data without the consent of the data subjects,
- breach of security and privacy measures,
- data processing without a legal basis.

At the same time, in the first four months of 2022, a number of 338 requests were addressed to our institution to issue points of view on various aspects related to the way of interpretation and application of the RGPD and the other incidental regulations.

During this period, the National Supervisory Authority issued opinions on 40 draft normative acts submitted by institutions and public authorities, which involved the analysis of complex aspects regarding the processing of personal data.

In the same period, requests for approval of BCRs submitted by 8 multinational companies were analyzed. Also, the National Supervisory Authority acted as a co-auditor on the requests for approval of BCRs submitted by 2 companies during this period.

The National Supervisory Authority carried out in the first four months of 2022, a series of information actions aimed at popularizing the rules for the protection of personal data.

Thus, several events dedicated to the celebration of the European Day of Data Protection were organized, including a Conference, at the same time the "Guide on data processing carried out by owners' associations" was launched, which includes clarifications regarding the appropriate application of regulations in the field of data protection of a personal nature by the owners' associations, posted on the website of the National Supervisory Authority www.dataprotection.ro. Also, a brochure containing relevant elements from the activity of the National Supervisory Authority in 2021, in Romanian and English, was posted.

At the same time, in 2022, the National Supervisory Authority continued to inform the general public by publishing 21 press

releases, by participating in online conferences and events, by attending inter-ministerial and institutional meetings and meetings.

Regarding the activity of representation in court, in the first four months of 2022, a number of 12 new requests for summons were registered.

Of these, 5 subpoena requests were received, the object of which is to contest the processes - minutes of findings/sanctions concluded by the representatives of the National Supervisory Authority.

Regarding the appeal of fine sanctions ordered by the National Supervisory Authority after the implementation of the GDPR, it is worth noting that, out of the total of 110 fines applied to operators from 2019 until May 2022, based on the GDPR, only 25 fines were challenged in the courts.

Of these, 12 files have been finalized so far, and in 9 of these cases, final solutions were pronounced in favor of the National Supervisory Authority.

Thus, the courts fully confirmed the fines applied by our institution to the following operators:

Banca Transilvania SA (100,000 euros)

I want Credit SRL (20,000 euros)

Proleasing Motors SRL (15,000 euros)

Hora Credit IFN SA (14,000 euros)

Dante International (3,000 euros)

Royal President SRL (2,500 euros)

At the same time, they were resolved in favor of the National Supervisory Authority, by maintaining the minutes of ascertainment/sanctioning in the sense of retaining the contraventional nature of the facts, with the reduction of the amount of the fine or its replacement with a warning, as regards the operators: SC Entirely Shipping & Trading SRL (decrease), World Trade Center Bucharest SA and Legal Company & Tax Hub SRL.

Contravention complaints filed by 3 operators were admitted: ING Bank N.V. AMSTERDAM, CN Tarom and Tip Top Food Industry SRL.

In order to ensure full information to the general public and to support operators concerned with the correct application of data protection rules, we present below, for example, some extracts from relevant cases in which the courts have retained the

legality and validity minutes drawn up by the National Supervisory Authority, confirming our institution's approach in evaluating the respective situations.

♦ By Decision no. 23/11.11.2021, the Bucharest Court of Appeal confirmed, as well as the trial court (TMB), the sanction of the fine in the amount of 20,000 euros, ordered against the operator Vreau Credit SRL, noting, in relation to the criticisms regarding the legality of the minutes, "that when applying the sanction, the authority took into account all the elements indicated by art. 83 [of the RGPD], as well as other additional elements, all of which are likely to ensure the possibility of subsequent legality checks by the court."

Regarding the amount of the fine applied to the operator, for the violation of art. 32 para. (1), (2) and (4) of Regulation 2016/679, the Bucharest Court of Appeal found that:

"The aspects invoked by the appellant-complainant in the sense that appropriate measures were taken, in order to implement the provisions of the Regulation in a correct way, were removed by the substantive court, being contradicted by the established facts, which attest to the unauthorized disclosure of personal data personally for an extremely large number of clients - 1177 natural persons/clients - by sending photocopies of their identity documents to unauthorized persons (employees of another data operator — Raiffeisen Bank) who in turn disclosed these data to a third party (Biroul de Credit SA).

The large number of affected people attests to the fact that this way of working was, in reality, a common practice of the operator, who, although he had work procedures in writing, did not ensure their effective implementation."

The Bucharest Court of Appeal also noted that:

"In the case, there was no evidence of those "adequate technical and organizational measures" in order to ensure an appropriate level of security, nor was there evidence of employee training in order to prevent the type of violation found. The respondent correctly observed that the appellant had the obligation not only to draw up written procedures, but also to establish mandatory rules for all employees regarding the security of processing and data confidentiality, in the absence of these, as well as evidence regarding the training of the own staff in an effective and sufficient manner, the simple drafting of some procedures remaining ineffective and, as it was found, with serious consequences on the private life and privacy of its customers."

Regarding the sanction related to the fact that the same operator did not notify the National Supervisory Authority of the security incident, the Bucharest Court of Appeal correctly noted that:

"Given that the appellant did not provide proof of this notification to the authority within the term provided for by the Regulation, it was rightly held that the violation of legal obligations and the need to apply sanctions were in her charge.

The court will remove the claims of the appellant-plaintiff [Vreau Credit SRL] regarding the existence of the clients' agreement regarding data processing, which led her to the conclusion that notification would not be necessary.

The Court will find that from the Appendices presented by the appellant [Vreau Credit SRL] to the substantive file (...) there is no unequivocal consent of its clients for the transmission of personal data/their processing by a third party, even less their use for queries in the database of the Credit Bureau carried out by a third party against the contractual report.

It was correctly observed from the study of the documents submitted by the appellant that its clients were not correctly informed about the processing operations and they were not asked for their express consent, unequivocally they did not have the opportunity to act in any way to - manifests his free will, specific and informed, as provided in art. 7 para. (1) in conjunction with art. 4 point 11 of the GDPR."

♦ Regarding the sanction of the fine in the total amount of 14,000 euros, by Decision no. 25 of 25.11.2022, final, the Bucharest Court of Appeal confirmed the measure ordered by the National Supervisory Authority to the operator Hora Credit IFN SA, rejecting its request to replace the three fines applied with the warning sanction.

Thus, the appellate court noted that:

"As the appellant ANSPDCP correctly observed, the criteria for individualizing the sanction are those provided for in art. 83 para. (2) of the RGPD", as well as the fact that "The provisions of art. 83 para. (4), according to which: "if an operator or a person authorized by the operator violates intentionally or through negligence, for the same processing operation or for related processing operations, several provisions of this regulation, the total amount of administrative fines cannot exceed the amount provided for the most serious violation.(...)

Therefore, in case of violation of several provisions of the Regulation, as in the present case, in order to be able to apply the "warning" sanction, it is necessary that the extremely low degree of social danger be ascertained in relation to each of the detected deviations, this cannot be evaluated "as a whole", depending on the conduct adopted by the verified person after the communication of the minutes. (...)

Analyzing each of the detected violations, the Court will note that the first of these was sanctioned with a fine of 3000 Euros", and "will note that the sanctioned deed, consisting in the communication of personal data to third parties without proving the

application of effective mechanisms verifying and validating the accuracy of the data, respectively preserving their confidentiality represents an act of high social danger, being the violation of some of the general principles of the Regulation, regulated by the provisions of art. 5 para. (1) lit. d) and f) and art. 5 para. (2) of the GDPR.

Moreover, as previously shown, the plaintiff appellant [Hora Credit IFN SA] had at her disposal a reasonable period of time from the entry into force of the Regulation and until the commission of the facts, in order to adapt her conduct according to European norms, in the purpose of ensuring the protection guaranteed by the Regulation, but it did not proceed in this sense, the verification mechanisms implemented by it - verification by phone call of the data - being devoid of any efficiency from the perspective of confirming the reality of this data and ensuring the identity between the credit applicant and the owner of the data of a personal nature communicated.

However, the Court will observe that the fine applied to the appellant, of 3000 Euros, is far from the maximum limit of the fine provided by the regulation, so that in relation to the seriousness of the ascertained fact, it had to be maintained by the trial court.

Also, (...) it will be noted that the criterion from art. 83 para. (2) lit. a), the appellant-plaintiff [Hora Credit IFN SA] being a professional specialized in granting loans to consumers, with obligations regarding the guarantee of the security of their personal data, who illegally processed these data not only once, but repeatedly, including after being warned about the illegality of the processing.

Also, by reference to art. 83 para. (2) lit. c) from the regulation, it is found that the appellant-complainant, although she was warned about the stop of the processing as early as July 2019, only ordered measures to protect the consumer in September of the same year, during which she repeatedly the rights of the natural person were violated (...).

At the same time, the Court will consider the provisions of art. 83 para. (2) letter d), regarding "the degree of responsibility of the operator or the person authorized by the operator, taking into account the technical and organizational measures implemented by them pursuant to articles 25 and 32", noting that he [the operator Hora Credit IFN SA] did not implemented technical and organizational measures based on the mentioned texts, to guarantee the security of personal data.

Considering these criteria for individualizing the sanction, the Court will observe that the fine of 3,000 Euros applied by the authority for committing the first offense is fully justified, there being no need to replace it with the "warning".

Regarding the second violation, the Court noted that "for its commission, a fine of 10,000 Euros was applied, referring to the

provisions of art. 83 para. (4) lit. a) from the Regulation, according to which:

"(1) For violations of the following provisions, in accordance with paragraph (2), administrative fines of up to EUR 10,000,000 or, in the case of an enterprise, up to 2% of the total annual worldwide turnover corresponding to the financial year shall be applied previously, taking into account the highest value".

The authority considered the violation of art. 25 and 32 of the Regulation, as previously shown, finding that the appellant-complainant did not comply with these legal provisions, given that she was aware of them and did not ensure an appropriate level of security to prevent the illegal processing of data, by implementing appropriate technical and organizational measures, among those referred to in the texts indicated in the European act.

The Court will also note that not only did the plaintiff not comply with these legal obligations, but when she was notified by the said (...) she did not adopt any corrective measures, but continued the illegal processing of personal data personally, being thus applicable the criteria for individualizing the sanction from art. 83 lit. a), c) and d), which lead to the conclusion that the application of a fine was required, and not the penalty of a warning, the deed having a high degree of social danger, and the amount of the applied fine is fully justified, under the conditions that it is much lower than the maximum level provided by law."

Regarding the third sanction, applied for the violation of the obligation to notify the National Supervisory Authority of the security incident, "The Court will note that, also, being a matter of knowingly not complying with a legal obligation, followed by for the continuation of the illegal processing of personal data, the amount of the applied fine of 1000 Euros is justified. However, the non-compliance with a legal obligation to notify, which led to the continuation of the illegal behavior of the appellant-complainant, justifies the amount of the applied fine, of only 1000 Euros, the sanctioned act having a high degree of social danger, by affecting the rights of private individuals (...), taking into account the provisions of art. 83 lit. h) from Regulation 2016/679.

As the appellant-defendant rightly observed, social danger is an essential feature, common to all acts that undermine the rule of law. At the same time, it indicates the extent to which the contravention affects one of the values or social relations protected by a normative act (in this case, the right to a private life protected both by art. 26 of the Romanian Constitution and by Regulation (EU) 2016/ 679).

Given that the plaintiff appellant did not adopt sufficient personal data security measures, according to art. 25 and 32 of the RGPD, so as to prevent the unauthorized and accessible disclosure of his client's personal data (...), persisted in

non-compliant conduct even after being informed of the violation and did not fulfill his legal obligation to notify the authority on security risk, the Court will appreciate that the facts held in charge of it present a high degree of social danger, so that the final fine applied must be maintained."

♦ By Decision no. 1148/17.11.2020, final by non-appeal, the Prahova Court confirmed the fine granted by the National Supervisory Authority SC PROLEASING MOTORS SRL, in the amount of 15,000 euros.

Thus, under the aspect of the committed act, the court found that:

"arguments regarding the non-existence of a violation cannot be retained, since it [the plaintiff SC PROLEASING MOTORS SRL] admitted that a security incident took place which it notified the Authority, its systems were vulnerable and possible to access, reported this to Cert-RO, called on an IT consultant and took a series of technical and organizational measures after the incident, all these aspects contradicting the non-existence of a violation.

In the same sense, the court opines that the plaintiff's obligation was all the more necessary since she showed that she is part of the network of an international corporation and implemented "all the Corporate Rules" of the group (...) whose authorized dealer she is.

However, in relation to the above, the court is of the opinion that the report is thorough and legally drawn up, there being no doubt that would lead to its annulment.»

At the same time, regarding the request made by the plaintiff SC PROLEASING MOTORS SRL regarding the replacement of the fine with a warning, the court established that:

"in relation to the seriousness of the act in the application of the measure, the principle of the proportionality of the sanction was respected, all the more so since it was evident from the evidence administered that the applicant did not submit all the diligence to take and comply with the appropriate technical and organizational measures to ensure a security level corresponding to the risks (...).

Moreover, when it comes to the nature or seriousness of the act, the legislator understood to individualize it by the amount of the fine, and compared to this amount, other considerations besides the plaintiff's lack of diligence are already redundant."

♦ By Decision no. 3161/2020 06.11.2020, which remained final due to non-appeal, the Bucharest Municipal Court confirmed the sanction of the fine in the amount of 2,500 euros, imposed on the operator Royal President SRL by the National Supervisory Authority.

Thus, as regards the commission of the act consisting in non-compliance with the provisions of art. 15 and art. 12 para. (3) and (4) of EU Regulation 679/2016, the court noted the following:

"Contrary to the claims of the plaintiff [Royal President SRL], the court finds that she did not provide proof of communication within the term provided by law (...) of the answer (...). Thus, although in the content of the summons request, as well as in the addresses sent to the defendant, the plaintiff claims that she made the communication within one month of receiving the request, no document to this effect was submitted, from the content of the confirmation of receipt attached in copy to the file (...) not showing the date on which the communication took place."

Also, regarding the commission of the deed consisting in non-compliance with art. 5 para. (1) lit. f) related to art. 32 para. (1) lit. b) from EU Regulation 679/2016, the court correctly noted the fact that through the contested minutes it was held that the applicant did not implement adequate technical and organizational measures in order to ensure the confidentiality of the personal data of the person concerned, as well as in order to ensure a level of security corresponding to the processing risk for the rights and freedoms of the data subject.

As such, the court concluded that:

"the consequence of not taking these measures determined the compromise of the confidentiality of personal data (...), generating the unauthorized disclosure of personal data (...) (name, first name, identity card series and number, CNP, information related to accommodation in Hotel Royal President) to an erroneous addressee."

In this context, the court noted the following:

"Although the plaintiff [Royal President SRL], claims that the person who requested the communication of the tax invoice in which the personal data were entered (...), was identified by telephone in compliance with the provisions of the RGPD, the court notes that the said invoice was sent to an email address that is not found in the accommodation sheet. Thus, verifying the content of the accommodation sheet, the court finds that the columns for the phone number and email address were left blank, the address to which the invoice was sent (...) not having been previously used in the correspondence between the parties, nor obtained directly from to [the person concerned].

Compared to the above and considering the provisions of art. 12 para. (6) RGPD, according to which, if it has reasonable doubts about the identity of the natural person submitting the request referred to in articles 15-21, the operator may request the provision of additional information necessary to confirm the identity of the person concerned, the court considers that no a

telephone confirmation of the accuracy of an e-mail address is sufficient, the operator having the obligation to take all reasonable steps to verify the identity of a data subject requesting access to data, especially in the context of online services and online identifications.

Consequently, the court considers that the plaintiff did not prove a factual situation distinct from the one established by the contravention report, respectively she did not prove that she adopted sufficient personal data security measures, according to art. 25 and 32 of the GDPR, so as to prevent the unauthorized disclosure of the personal data of the [data subject].

Also, with regard to the document entitled Procedure regarding the protection of personal data accompanied by the table with the persons who took cognizance and their signatures, it is noted that its contents do not show the date on which it was drawn up, nor the date on which was communicated to the plaintiff's employees. In addition, even if the document had been drawn up before the incident of 28.08.2019, the court considers that the steps taken by the applicant were neither sufficient nor effective in ensuring an appropriate level of security, the consequence being the impairment of the right of [the person concerned] to the protection of personal data."

♦ By Decision no. 3 of 27.01.2022, the Bucharest Court of Appeal definitively confirmed the sanction with a fine of 3,000 euros applied by the National Supervisory Authority in 2020 to the Dante International operator, noting that:

"In the case, the sanction applied by the authority fully corresponds to these requirements of proportionality in the conditions in which, as already noted, the act was committed in the conditions in which the person who formulated the notification had expressly requested that the appellant-complainant [Dante International] to stop sending him commercial messages.

At the same time, it does not appear from the content of the summons and the appeal that the appellant-plaintiff [Dante International] understood the fact that he had carried out illegal processing, his arguments being centered on the fact that he acted fully in accordance with the legal provisions , by trying to disguise under the guise of a transactional message a direct marketing message.

The Court also notes that the appellant-plaintiff was also sanctioned for violations of the legal provisions regarding the processing of personal data (...).

On the other hand, the amount of the fine established by the appellant-defendant through the infringement report (the equivalent of 3000 euros) is oriented towards the minimum specially established by law and has a much lower value than sanctions applied to other economic operators for similar acts."

♦ By Civil Decision no. 9 of 13.04.2022, definitive, the Cluj Court of Appeal confirmed the fine of 100,000 euros applied by the National Supervisory Authority to Bănci Transilvania, for the violation of art. 32 para. (1) and (2) in conjunction with art. 5 para. (1) lit. f) from the General Regulation on Data Protection.

Also, the same solution favorable to the National Supervisory Authority was also pronounced on the merits, by Civil Judgment no. 1309 of May 6, 2021 of the Cluj Court, fully upheld by the appeal court.

In order to decide in this way, "the Court emphasizes that the Regulation has introduced a much higher level of responsibility of the data operator compared to Directive 95/46/EC on data protection, and articles 24 and 32 of the Regulation provide that the operators "have in mind the current state of technology, the costs of implementation and the nature, scope, context, purposes of the processing, as well as the risks with varying degrees of probability and severity for the rights and freedoms of natural persons that the processing presents"».

Also, the court correctly noted the following aspects:

"In the case, in order to prove her diligent conduct in terms of staff training in the field of personal data protection, the plaintiff submitted a series of internal regulations as well as proof of the organization of courses on this topic, but it is important to emphasize that participation was not proven effective attendance of staff at these courses, nor the effective application of any way of verifying the acquisition of this knowledge and information.

In addition, the aspects invoked by the plaintiff in the sense in which appropriate measures were taken, in order to implement the provisions of the Regulation, are contradicted by the facts ascertained by the contravention report and undisputed, which attest to the intentional disclosure, in an unauthorized manner, by the persons under the authority of the Bank, of a significant [set] of personal data (some in the category of extremely sensitive data) to a very large number of people.

The casualness with which the plaintiff's employees acted, transmitting from one to another the personal data of the bank's client and later to third parties, through the Whatsapp application, attests not only to the lack of knowledge of the working procedures regarding the processing of personal data, but especially (and worse) their inability to identify and qualify the data they have access to as personal data, which indicates an acute lack of effective training.

Therefore, although the plaintiff submitted to the file, in copy, extracts from various internal procedures, this did not prove, on the one hand, the effective training of the three employees who caused the security incident, and on the other hand, that she applied the mechanisms of control and evaluation developed to ensure that its employees have mastered the mentioned

internal regulations.

That being the case, the documents presented by the applicant, in proof of the implementation of the appropriate technical and organizational measures, are not likely to prove the provision of an appropriate level of security regarding the ability to ensure confidentiality and the periodic testing, evaluation and assessment of the effectiveness of the technical and organizational measures in order to guarantee the security of processing."

Regarding the consequences of the violation, the Cluj Court held that "they were correctly qualified by the defendant as serious by reference to the amount of personal data disseminated by the Bank's employees, their sensitive nature, the method of dissemination (via the Internet, the email including the Bank's customer data circulating intensively in the public space, synthetic information being taken up including by blogs, TV channels and news sites), the extremely large number of people who gained access to the Bank's customer data for a period of time impossible to determine, following the transmission of information through the most diverse means, all these aspects being able to give a correct picture regarding the extent and seriousness of the consequences of the security incident.

The plaintiff admitted, moreover, in relation to the method of transmission of personal data, that the measures taken to limit the consequences of the security breach were not "feasible", the extent of their dissemination in the public space being obviously out of control."

Finally, the trial court correctly concluded that:

"For all the factual and legal considerations set out above, the court will conclude that the fine in the amount of 100,000 euros is legal, "effective, proportionate and dissuasive" and was established taking into account the nature, gravity and consequences of the violation, as well as all the other criteria provided by the Regulation, criteria that were analyzed by the defendant in a coherent and objective manner.»

Legal and communication department

ANSPDCP