data protection - legal changes published in July 2020

I. ROMANIA

1. ANSPDCP. THE NATIONAL COMPANY ROMANIAN POST WAS SANCTIONED WITH A FINE IN THE AMOUNT OF RON 9,686.60, THE EQUIVALENT OF EUR 2,000

On 15 July 2020, the National Supervisory Authority completed an investigation at the controller the National Company Romanian Post and found that it violated the provisions of art. 32 of the General Data Protection Regulation regarding the security of processing, sanctioning it with a fine of RON 9,686.60, the equivalent of EUR 2,000.

The fine was issued because the controller **did not implement adequate technical and organizational measures (e.g. pseudonymization),** both upon establishing the means of processing and during the processing itself, so as to efficiently implement the principles of data protection and to include the safeguards necessary for the processing, so as to fulfill the requirements of the GDPR and to protect the rights of data subjects.

In particular, the controller has not taken the appropriate technical and organizational measures to prevent **unauthorized access to personal data** (e-mail addresses and telephone numbers) at the website https://awb.posta-romana.ro belonging to the National Post Company, which led to the compromise of the confidentiality of the personal data of **eighty one** (**81) data subjects**.

The National Supervisory Authority carried out the investigation as a result of receiving from the controller a notification of a data security breach, according to the provisions of art. 33 of the GDPR.

2. ANSPDCP. THE CONTROLLER VIVA CREDIT IFN S.A WAS SANCTIONED WITH A FINE IN THE AMOUNT OF RON 9,680, THE EQUIVALENT OF EUR 2,000

The National Supervisory Authority completed an investigation at the controller Viva Credit IFN S.A., finding the violation of art. 12 par. (3) and (4) of the General Data Protection Regulation, by reference to art. 17 of the same Regulation, applying a fine in the amount of RON 9.680 lei, the equivalent of EUR 2,000.

The investigation took place as a result of a complaint claiming that the controller did not solve the petitioner's request by which they exercised their right to erasure, according to art. 17 of the General Data Protection Regulation.

Also, the controller did not provide the applicant with information on the actions taken following their request within one month (or a maximum of 3 months, stating the reasons for the delay) at their home address or contact address (e-mail) available in its records.

Thus, the controller Viva Credit IFN S.A. violated the provisions of art. 12 par. (3) and (4), by reference to art. 17 of the General Data Protection Regulation.

The controller has the obligation, according to art. 12 par. (3), to respond to the requests of the data subjects without undue delay and at the latest within one month from the receipt of the request, and according to par. (4) of the same article "If the controller does not take action on the request of the data subject, the controller shall inform the data

subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy".

At the same time, the controller S.C. Viva Credit IFN S.A. was ordered a corrective measure based on the provisions of art. 58 par. (2) let. d) of the GDPR, whereby it must send a reply to the petitioner to the submitted request, within 5 working days from the communication of the citation.

3. ANSPDCP. THE CONTROLLER CNTAR TAROM WAS SANCTIONED WITH AN ADMINISTRATIVE FINE IN THE AMOUNT OF RON 24,182.50, THE EQUIVALENT OF EUR 5,000

The National Supervisory Authority completed on 06.07.2020 an investigation at the controller **SC CNTAR TAROM SA**, as a result of the transmission by the controller of a notification regarding a personal data security breach, finding the violation of the provisions of art. 32 par. (4), art. 32 par. (1) let. b) and par. (2) of the GDPR, which led to the application of a fine in the amount of **RON 24,182.50**, the equivalent of **EUR 5,000**.

The personal data security breach consisted in the fact that the controller **did not implement adequate technical and organizational measures** to ensure that any natural person acting under the authority of the controller and having access to personal data only processes said data at the request of the controller, **which led to the loss of the confidentiality of personal data through unauthorized access to data belonging to five (5) TAROM passengers, as well as to the unauthorized disclosure of their data.**

The controller was also ordered the corrective measure **to review and update the technical and organizational measures implemented** as a result of the risk assessment for the rights and freedoms of individuals, including working procedures on personal data protection, and the implementation of certain measures **on the regular training of persons acting under its authority (employees)**.

4. ANSPDCP. THE CONTROLLER PROLEASING MOTORS ARL WAS SANCTIONED WITH A FINE IN THE AMOUNT OF RON 72,642, THE EQUIVALENT OF EUR 15,000

The National Supervisory Authority completed on 23.06.2020 an investigation at the controller **Proleasing Motors SRL and found the violation of the provisions of art. 32 par. (1) and (2) of the General Data Protection Regulation, sanctioning the controller with a fine in the amount of RON 72,642, the equivalent of EUR 15,000.**

The investigation was initiated following the submission by the controller of a notification of personal data breach, by filling in the specific form established under the General Data Protection Regulation.

The security breach consisted in the fact that, on the Facebook page where the controller conducted an online contest to attract participating customers to the repair shop, **a document was posted with a screenshot of the website source code which included the access password to the forms filled in by the contest participants.**

This situation led to the unauthorized viewing and access to the personal data of 436 customers of the controller, on the website of Proleasing Motors SRL, and to the unauthorized disclosure of this data, contrary to the obligations provided by art. 32 of the General Data Protection Regulation.

As such, the sanction was applied to the controller due to the fact that it did not implement adequate technical and organizational measures in order to ensure an appropriate level of security of the processing regarding the rights and freedoms of individuals, in relation to the risk generated in this case accidentally or illegally, of destruction, loss, modification, unauthorized disclosure of personal data transmitted, stored or otherwise processed, or unauthorized access thereto.

A corrective measure was also applied to the controller, namely to review and update the technical and organizational measures implemented as a result of the risk assessment for the rights and freedoms of individuals, including electronic communications procedures, so as to avoid similar incidents of unauthorized disclosure of the personal data processed, in relation to art. 58 par. (2) let. d) of the General Data Protection Regulation.

II. EUROPEAN UNION

1. GERMANY. A HEALTH INSURANCE COMPANY HAS BEEN FINED EUR 1,240,000 FOR GDPR VIOLATION

According to a statement dated 29 July 2020, the German Personal Data Protection Supervisor imposed a fine on AOK Baden-Wuerttember.

Due to a breach of secure data processing obligations (Article 32 of the General Data Protection Regulation, GDPR), the State Commissioner for Data Protection and Freedom of Information imposed a fine of € 1,240,000 against AOK Baden-Wuerttemberg.

From 2015 to 2019, AOK Baden-Württemberg organized competitions on various occasions and collected personal data of the participants, including their contact details and health insurance affiliation. The AOK also wanted to use this data for advertising purposes, provided the participants had given their consent. With the help of technical and organizational measures, including internal guidelines and data protection training, the AOK wanted to ensure that only data of those contest participants who had previously given their effective consent would be used for advertising purposes. However, the measures defined by the AOK did not meet the legal requirements. As a result, the personal data of more than 500 lottery participants were used for advertising purposes without their consent. No insurance data was concerned.

2. ITALY. A PHONE COMPANY HAS BEEN FINED EUR 17 MILLION FOR GDPR VIOLATION

On 27 July 2020, the Italian Authority for the Protection of Personal Data announced a fine of € 17 million to Wind Tre SpA for several cases of illegal data processing which were largely related to marketing.

The fine was imposed following complex investigations and inspections. Complaints have been received from users in connection with unsolicited marketing communications, made without their consent by sending automated messages, e-mails, faxes and telephone calls. In several cases, the data subjects were not able to exercise their right to withdraw their consent and object to processing for direct marketing purposes because the information contained in the Data Protection Policy was incomplete in relation to the contact details. In other cases, users' personal data were included in public telephone lists, despite objections (sometimes reiterated) made by these users.

The Authority fined Wind Tre EUR 16,729,600 and banned any further processing of the data it had acquired without consent.

3. POLAND. A NURSERY AND A KINDERGARTEN WERE FINED PLN 5,000 FOR GDPR VIOLATION

The Polish data protection authority imposed a fine of PLN 5000 on an entrepreneur operating a nursery and a kindergarten.

The company did not allow the Authority access to personal data and other information necessary for the performance of its tasks - in this case, to assess whether the controller had notified a security breach.

The controller notified the Authority of a personal data breach, which consisted of losing access to personal data stored by the company.

In view of the lack of information necessary to carry out an assessment of the notification, the supervisory authority sent three requests to the company to provide relevant explanations.

4. POLAND. INSPECTOR GENERAL WAS FINED PLN 100,000 FOR GDPR VIOLATION

The Polish Data Protection Authority, following an ex officio administrative procedure, imposed a fine of PLN 100,000 on the Inspector General of Poland.

The Authority established that the Inspector General of Poland had violated the provisions of the General Data Protection Regulation where the breach consisted in failing to provide the Authority, during the inspection, access to the data processing facilities and equipment and information necessary to perform its tasks. In addition, the Inspectorate did not cooperate with the President of the Authority during this inspection.

5. BELGIUM. GOOGLE BELGIUM HAS BEEN FINED EUR 600,000 FOR GDPR VIOLATION

The Belgian data protection authority has fined Google Belgium 600,000 euros. for the rejection of an application by a data subject under the right to be forgotten, and lack of transparency in Google's form for dereferencing applications.

A Belgian citizen has requested the dereferencing of links containing negative information about him. The request was denied by Google.

The Authority found that some of these referenced links were necessary for the public interest and should not be removed: the citizen does indeed play a role in public life, and the links concerned an alleged relationship with a political party. The other links contained old, unfounded information and could seriously damage the citizen's reputation. The Belgian authority considered that these links should therefore have been dereferenced by Google.

6. POLAND. A RECRUITMENT COMPANY WAS FINED PLN 15,000 FOR GDPR VIOLATION

The Data Protection Authority imposed a fine of PLN 15,000 to East Power from Jelenia Góra for failing to provide the Authority with access to personal data and other information necessary for the performance of its tasks.

The fined company provides employment services in Poland and Germany, and a German citizen filed a complaint against its actions because it processed his personal data for marketing purposes. The complaint was lodged with the competent German Data Protection Authority but was taken up for examination by the Polish Authority, which was the so-called main authority in this case, as the company is established in Poland.

In this proceeding, the President of the Authority sent three subpoenas to the company for an explanation. Two of them went unanswered. The company responded to one of the requests, but its explanations were incomplete and contradictory. In the opinion of the President of the Authority, these were clearly insufficient to establish the facts of the case. Due to such conduct of the company, the President of the Authority considered that the company had deliberately obstructed the course of the procedure or at least failed to comply with its obligations to cooperate with the supervisory authority.

III. NEW LEGISLATIVE AND REGULATORY DEVELOPMENTS

1. INVALIDATION OF EUROPEAN COMMISSION DECISION (EU) 2016/1250 ON THE EU-US PRIVACY SHIELD

In its judgment from 16 July 2020 in Case C-113/18 Schrems II, the Court of Justice of the European Union invalidates Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 under Directive 95/46/EC of the European Parliament and Council on the adequacy of the protection afforded by the **EU-US Privacy Shield.**

Thus, the CJEU examined the validity of European Commission Decision (EU) 2016/1250 in the light of the requirements derived from Regulation (EU) 2016/679, taking into account the provisions of the Charter guaranteeing respect for private and family life, protection of personal data and the right to effective judicial protection.

In the opinion of the CJEU, the limits on the protection of personal data arising from US domestic law on access to and use by US public authorities of such data transferred from the European Union to the third country are not circumscribed in a way that satisfies requirements which are essentially equivalent to those imposed by European Union law, by the principle of proportionality, in so far as surveillance programs based on these provisions are not limited to what is strictly necessary.

At the same time, the CJEU emphasized that, although these provisions set out the requirements that the US authorities must comply with when implementing the surveillance programs in question, the provisions do not grant the data subjects rights of legal action against the US authorities.

With regard to the requirement of judicial protection, in the opinion of the CJEU, the Ombudsperson's mechanism for the Privacy Shield does not offer guarantees equivalent to those imposed by EU law, so as to ensure both the Ombudsperson's independence and the rules that allow it to make decisions that are binding on the US intelligence services. In this regard, the CJEU notes that although Recital (120) of European Commission Decision (EU) 2016/1250 mentions a commitment by the US government that the intelligence component should be obliged to remedy any breach of the applicable rules detected by the Privacy Shield Ombudsperson, that decision does not contain any indication that said Ombudsperson was empowered to take binding decisions in respect of those services, nor does it mention the legal guarantees which would accompany that undertaking and which could be invoked by the data subjects. Thus, the Ombudsperson mechanism provided in European Commission Decision (EU) 2016/1250 does not offer a legal remedy to a body that grants persons whose data are transferred to the United States guarantees essentially equivalent to those provided in Article 47 of the Charter of Fundamental Rights of the European Union.

For all these reasons, the Court of Justice of the European Union has invalidated Decision (EU) 2016/1250 of 12 July 2016 under Directive 95/46/EC of the European Parliament and Council on the adequacy of protection offered by the EU-US Privacy Shield. The CJEU decision is available at the following link:

http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=10304093

At the same time, during the Plenary Session of the European Data Protection Board, held online on 17 July 2020, **the Statement on the invalidation by the Court of Justice of the European Union of Decision (EU) 2016/1250 was adopted under Directive 95/46/EC of the European Parliament and Council on the adequacy of the protection afforded by the EU-US Privacy Shield.**

In such a situation, in the absence of an adequacy decision under art. 45 par. (3) of Regulation (EU) 2016/679, the transfer of personal data to the United States may be carried out in accordance with one of the following instruments provided by art. 46 of Regulation (EU) 2016/679:

- standard data protection clauses,
- binding corporate rules,
- codes of conduct and certification mechanisms.

Also, the transfer of personal data to the United States may be made under the derogations provided in art. 49 of Regulation (EU) 2016/679.

The English version of the **EDPB Statement** can be found at the following link:

https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en

Following the judgment of the CJEU in Case C-113/18, the European Data Protection Board adopted the document "Frequently Asked Questions" to provide initial clarifications and preliminary guidance to interested parties on the use of legal instruments for the transfer of personal data to third countries, including to the USA. It should be noted that this document will be supplemented by additional guidance, as the Board will continue to examine and evaluate the judgment of the CJEU.

The FAQ issued by the European Data Protection Board is available in **Romanian** and in **English**.