

14.04.2022

Final decision regarding the fine of 100,000 euros

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 Transilvania Bank Supervisory Authority, for the violation of art. 32 para. (1) and (2) in conjunction with art. 5 para. (1) lit. f) of the General Data Protection Regulation.

Also, the same solution favorable to the Supervisory Authority was also pronounced on the merits, by Civil Judgment no. 1309 of 06 May 2021 of the Cluj Court, upheld in its entirety by the court of appeal, noting that "the summons filed by the defendant Banca Transilvania SA in opposition to the defendant the National Authority for the Supervision of Personal Data Processing, is clearly unfounded and will be rejected, the contravention report no. 23409 concluded by the defendant on 26.11.2020 to be maintained as fully legal and well-founded."

In order to decide in this way, "the Court emphasizes that the Regulation introduced a much higher level of responsibility of the data operator compared to Directive 95/46/EC on data protection, and articles 25 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"».

The court also 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 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 organizational technical 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 to guarantee processing security."

Regarding the consequences of the violation, the Cluj Court held that "they were correctly qualified by the defendant as being serious by referring 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 over by blogs, TV channels and news sites), the extremely large number of people who have 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.

The defendant also properly capitalized on the criteria provided for in art. 83 paragraph (2) letters c)-k), the proof of the thorough examination of these criteria is precisely the establishment of a fine in an amount much lower than the maximum allowed for the deed committed by the applicant. Moreover, the report includes in detail the analysis carried out by the defendant regarding each of the criteria established by art. 83 para. (2) for the individualization of the sanction."

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.»

In this context, we specify that, through the press release that can be consulted at

[https://www.dataprotection.ro/?page=Comunicat\\_17\\_12\\_2020&lang=ro](https://www.dataprotection.ro/?page=Comunicat_17_12_2020&lang=ro), the National Supervisory Authority has published relevant information regarding the investigation completed at the operator Banca Transilvania SA, as a result of which the violation of the provisions of art. 32 para. (1) and (2) in conjunction with art. 5 para. (1) lit. f) of the General Data Protection Regulation.

At the same time, we underline the fact that in other similar cases of violation, by operators in the sphere of financial institutions, of the RGPD provisions regarding the principles of data processing and the measures to ensure their security, through final court decisions, the courts have maintained the processes - verbal by which fine sanctions were granted, as follows:

The Bucharest Court of Appeal confirmed the fines applied to the Vreau Credit operator in the total amount of 95,024 lei (the equivalent of 20,000 euros) for violating art. 32 and 33 of the GDPR;

The Bucharest Court of Appeal confirmed the fines imposed on the Hora Credit operator in the total amount of 66,901.8 lei (the equivalent of 14,000 EUR), for violating art. 5 para. (1) lit. d) and f), art. 5 para. (2), art. 25, art. 32 and art. 33 para. (1) of the GDPR.

Legal direction and communication

A.N.S.P.D.C.P.