data protection - legislative changes published in April 2022

I. ROMANIA

1 SANCTIONS APPLIED BY THE NATIONAL SUPERVISORY AUTHORITY (ANSPDCP)

1.1 IKEA ROMANIA S.R.L was sanctioned for violating the provisions of Article 12 para. (3) of the GDPR with a fine amounting to LEI 4,949.00 (the equivalent of EUR 1,000)

Following the investigation, the National Supervisory Authority found that the controller failed to submit in due course a response to the repeated requests from the data subject, by which he/she exercised the right to delete his/her personal data from an Ikea user account, created based on an email address.

As a corrective measure, the controller was required to take the necessary measures to ensure that the rights of data subjects are observed in all cases.

1.2 An Association of Owners was sanctioned for violating the provisions of Article 83 para. (5) point e) in conjunction with Article 58 para. (1) point a) and e) of the GDPR with a fine amounting to LEI 2,747.50 (the equivalent of EUR 500)

Following the investigation, it was found that the controller (The Association of Owners from 17 Soporului Street, Cluj-Napoca) failed to respond to the request for information from the National Supervisory Authority, although it had previously confirmed its receipt.

In addition, the controller was requested to provide all the information requested within 5 working days from the notification of the penalty notice.

The investigation was initiated following a complaint by the data subject that the controller had disclosed, on the Facebook group of the building where the data subject lives, images of himself/ herself from the surveillance system managed by the association.

1.3 Cluj Court of Appeal confirmed the fine in the amount of LEI 487,380.00 (the equivalent of EUR 100,000) applied by the National Supervisory Authority to Banca Transilvania S.A., for violating the provisions of Article 32 para. (1) and (2) in conjunction with Art. 5 para. (1) lit. f) of the GDPR

Following the investigation performed and finalised on 26.11.2020, the National Supervisory Authority found that the controller failed to take sufficient measures to ensure that individuals acting under its authority and having access to personal data, only process them at the controller's request.

In particular, 3 employees of Banca Transilvania S.A. disclosed, on the Facebook social media platform, a statement requested by the controller from one of its clients on how he intended to use an amount of money that he wanted to withdraw from his personal account. This led to the disclosure and unauthorized access to the data subject's personal data, such as name and surname, e-mail addresses, personal preferences, the value of financial transactions, liable to cause moral damage, as well as other economic or social disadvantages to the data subject.

Subsequently, the controller challenged the fine in court, and the Cluj Court of Appeal has finally confirmed the decision delivered by the first level court in this case, in relation to the lawfulness and grounds of the related fine notice and the „effective, proportionate and dissuasive" nature of the fine imposed.

In delivering its judgment, the Court of Appeal considered that the controller failed to prove the effective training of the three employees causing the security incident and the implementation of control and evaluation mechanisms developed to ensure that its employees have mastered its internal data protection policies.

The Court also held that the excerpts from various internal procedures submitted by the controller in order to prove the implementation of appropriate technical and organisation measures were not able to prove that an adequate level of security was ensured.

II. RELEVANT ISSUES AT THE EUROPEAN DATA PROTECTION BOARD (EDPB) LEVEL

2.1 EDPB adopts Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework

The EDPB notes that this announcement does not constitute a legal framework on the basis of which EEA data exporters can transfer data to the U.S.

Data exporters shall continue taking the necessary actions to comply with the case law of the Court of Justice of the European Union, in particular with Schrems II decision of July 16, 2020.

The EDPB will pay special attention to how this political agreement is translated into concrete legal proposals.

2.2 EDPB amends the Rules of Procedure on notification and translation of binding decisions in compliance with Article 65 of the GDPR

During its Plenary held on April 6, 2022, the EDPB adopts version VIII of Rules of Procedure on the notification and translation of binding decisions. The amendments relate to the powers and procedure to be followed in dispute resolutions assessed by the EDPB, in compliance with Article 65 GDPR.

More details can be found at the following link: edpb_rules_of_procedure_version_8_adopted_20220406_en.pdf (europa.eu).

III. EUROPEAN UNION

1 SANCTIONS APPLIED IN THE EU

1.1 The Danish Data Protection Authority ("Datatilsynet") imposed to Danske Bank a fine of EUR 1,3 million for breaches of the GDPR provisions

Following the investigation, Datatilsynet found that the controller failed to implement adequate procedures for the storage and deletion of personal data in more than 400 banking systems, where data belonging to millions of individuals were being managed.

Hence, Datatilsynet has sanctioned the controller for violating the provisions of art. 5 para. (2) of the GDPR, which provides for its obligation to comply with the general principles of personal data processing.

The investigation was initiated in November 2020, following the controller's statement pointing out that it had found problems with the deletion of personal data whose storage was no the longer necessary or justified for the business purposes pursued.

3.2 The Irish Data Protection Authority ("DPC") imposed to Bank of Ireland a fine of EUR 463,000 for breaches of the GDPR provisions.

Following the investigation, the DPC found that due to flawed personal data processing processes, there has been a breach of security of personal data of more than 47,000 data subjects, in violation of Article 32 of the GDPR.

In particular, the Bank of Ireland submitted incorrect information to the Central Credit Register, an entity under the authority of the Central Bank, and unauthorisedly disclosed personal data belonging to its clients, errors which were likely to alter their credit performance score. In addition, the controller unjustifiably delayed in fulfilling its obligation to inform data subjects on the incidents occurred.

The investigation was initiated following 19 notifications received from the controller with resepct to personal data security breaches.

In addition to the fine, the controller was required to implement appropriate technical and organizational measures to ensure a level of security that is proportionate to the business risks.

3.3 The Dutch Data Protection Authority ("AP") imposed to Tax and Customs Administration a fine of EUR 3,7 million for breaches of the GDPR provisions

Following the investigation, the AP found that the controller violated several provisions of the GDPR, including processing personal data without a legal basis, storing outdated or inaccurate personal data and retaining it for unreasonably long time-periods.

In particular, the irregularities extended over a period of 6 years and were detected through the use of the Fraud Reporting System, a database of personal data of over 250,000 data subjects, including minors. A number of them suffered financial consequences as a result of the wrong information being attributed to them.

In determining the amount of the fine, the AP considered the severity of the offences, their duration and the damage caused to the data subjects.