Read this post online

The French Data Protection Authority imposes a 250,000 euros fine on Spartoo

The *Commission Nationale de l'Informatique et des Libertés* (French Data Protection authority or "CNIL") has just imposed a penalty of 250,000 euros on Spartoo, a company specializing in the online sale of shoes. The CNIL noted several breaches of the GDPR, the general regulation on data protection which came into force on May 25, 2018.

This is the first penalty imposed by the CNIL as "lead supervisory authority" in cooperation with other EU supervisory authorities as the consumers (and their personal data) of Spartoo which is based in Grenoble extend beyond French borders.

In May 2018, the CNIL carried out an on-the-spot inspection in Spartoo's premises to determine whether the company was complying with all the provisions of the GDPR. The CNIL's investigation focused in particular on Spartoo's customer and prospective customer files, and on the recording of phone conversations between customers and Spartoo's employees working in the customer service department.

In July 2018, as Spartoo's customers and prospects concerned by the investigation were located in several European countries, the CNIL informed all European supervisory authorities that it was competent to act as lead supervisory authority for the cross-border processing carried out by the company and opened the procedure for the declaration of the relevant authorities concerned by this case.

In 2019, the President of the CNIL decided to initiate sanction proceedings against the company.

On July 28, 2020, on the basis of the investigation carried out, the CNIL considered in deliberation n°SAN-2020-003 that the company had failed to comply with several obligations under the GDPR.

Breach of the data minimization principle (Article 5(1)(c) of the GDPR)

It should be recalled that Article 5(1)(c) of the GDPR provides that personal data must be *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)."*

Full and permanent recording of phone calls received by Spartoo's customer service department

The CNIL found that the full and permanent recording of phone calls received by the customer service department was excessive: it held that recording all the calls was not justified, especially as the person in charge of employee training only listened to one call recording per week and per employee.

Recording of bank data during phone calls with the company

The CNIL further found that the recording and storage of customers' bank details when orders were made by phone was not necessary for the intended purpose, i.e. employee training.

Data collection in the context of the fight against fraud

In view of the purpose of the processing and the residual nature of the number of copies of identity cards processed by the company, the CNIL considered that the copy of the identity card may constitute relevant proof.

However, the collection in Italy of the copy of customers' "health card" was considered excessive. For the CNIL, the communication of this document, which contains more information than the identity card, while a copy of the identity card was also requested, was excessive and irrelevant.

Failure to comply with the obligation to limit the data retention period (Article 5(1)(e) of the DGPR

It should be recalled that Article 5(1)(e) of the GDPR provided that personal data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')*."

During the inspection, the CNIL noted that the company did not set a retention period for customers' and prospective consumers' data, did not regularly erase personal data and did not archive them.

Data retention period

Although the company had planned to keep the data for five years after the CNIL inspection, the CNIL nevertheless found a breach as the company kept for several years a very large number of former customers' data (more than 3 million customers had not logged on to their account for more than 5 years).

With regard to prospective consumers' data in particular, the CNIL noted that the company did not send commercial prospection to these people if they did not show interest in its products or services for two years. It therefore considered that it was not necessary to keep prospective consumers' data beyond this two-year period.

Starting point of the retention period

In its deliberation, the CNIL noted that "*prospective consumers' data allow a data controller to send messages, for example by e-mail, to people who show an interest in its products or services*".

It considered in this respect that "*when the starting point of the data retention period is the last contact from the prospective consumer, there must be an event that demonstrates the person's interest in the message received, such as a click on a hypertext link in an e-mail*".

However, it specified that "*the mere opening of an e-mail cannot be considered as a contact from the prospective consumer, since it may be opened unintentionally due to the operating methods of the e-mail software being used or by mistak*e".

Anonymization

The company explained that at the expiry of the five-year retention period applied to customers' data it deleted some data (surname, first name and date of birth) but retained others (e-mail address and password) which were hashed by an algorithm and transferred to another table.

The CNIL noted that while the algorithm in question, SHA-256, is considered by the French National Agency for the Security of Information Systems (*Agence Nationale de Sécurité des Systèmes d'Information* or "ANSSI") and the CNIL as guaranteeing a sufficient level of data security, its hash function did not make it possible to anonymize data and thus to justify their retention indefinitely by a data controller.

The CNIL noted in passing that the company indicated that the purpose of implementing such a measure was to enable its customers to reconnect to their accounts, even though the data were supposed to have been deleted. It held that the personal data of former customers should be definitively deleted at the end of the period for which they had been kept in an active or archive database, once the legal obligations had expired, and could not be kept for a hypothetical future use.

Failure to inform individuals (Article 13 of the GDPR)

Articles 12, 13 and 14 of the GDPR set out the procedures for informing data subjects. While Article 12 concerns the conditions for such information, Articles 13 and 14 list the aspects to be covered by this information.

Information to customers

For the CNIL, the information provided in the website's data privacy policy was not compliant. Indeed, the

company indicated that consent was the legal basis for all data processing activities, whereas several of such activities were in fact based on other legal bases (such as the contract or the legitimate interests pursued by the company).

Information to employees working in the customer service department

The CNIL considered that information about the recording of phone calls with clients was insufficient. In particular, employees were not informed of the purpose of the processing activity, the legal basis of the processing, the recipients of the data, the data retention period and their rights.

Failure to comply with the obligation to ensure data security (Article 32 of the GDPR)

Article 32 of the GDPR that deals with security of processing provides that "*taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate (…)*."

Access passwords to customer accounts

During the inspection, the CNIL noted that people wishing to create a user account on the company's website could create a password consisting of six characters with a single type of characters. After the inspection, the company implemented a one-minute blocking measure for the account (after 19 unsuccessful attempts to access an account from the same IP address in less than a minute) and then required passwords with at least eight characters. For the company, the length and complexity of a password were not basic criteria for assessing the strength of such password.

The CNIL did not share this opinion: "*To ensure a sufficient level of security and meet the requirements of password strength, when authentication is based solely on a login and a password, the password must be at least twelve characters long – containing at least one upper case letter and one lower case letter, a number and a special character – or the password must have at least eight characters – containing three of these four types of characters – and be accompanied by an additional measure such as, for example, the timeout of access to the account after several failed attempts (temporary suspension of access, the duration of which increases as attempts are made), the introduction of a mechanism to guard against automated and intensive attempts (e.g. captcha) and/or the blocking of the account after several unsuccessful authentication attempts.*

It thereby agrees with ANSSI for which "*a good password is above all a strong password, i.e. difficult to retrieve even with the help of automated tools. The strength of a password depends on its length and the number of possibilities that exist for each character in it. Indeed, a password made up of lower case letters, capital letters, special characters and numbers is technically more difficult to discover than a password made up of lower case letters only*".

Customers' banking data

As part of the fight against fraud, the company had set up a system enabling customers to send photographs or scans of their bank card containing the full bank card number by unencrypted email from their email inbox. These data were kept in the database for six months in clear text format, together with the supporting documents requested in the context of the fight against fraud.

The CNIL considered that the retention for six months and in clear text of the bank card scans used for an order did not guarantee the security of the data.

Sanction

Given the number of infringements, the CNIL decided to impose on Spartoo a fine of 250,000 euros and to publish its decision.

In particular, it took into account:

- the seriousness of the infringements (related to the recording of phone conversations and the retention of bank data);
- the number of people concerned, as the data of several thousand people had been kept beyond the necessary periods (more than 3 million former customers and more than 25 million prospective consumers);
- the fact that many of the infringements related, for the most part, to obligations that already existed before the entry into force of the GDPR.

The company was ordered to bring its data processing activities into compliance with the GDPR and to demonstrate compliance within three months following the CNIL's deliberation, subject to a penalty payment of 250 euros for each day of delay.