GDPR news - cross-border data breach

Cross-border data breach - to be notified once, however information about a breach to be given in all countries

In the event of cross-border processing of personal data, a personal data breach may entail a risk for persons in more than one EU member state.

Hence, a French company may process data not only on data subjects in France, however also on data subjects domiciled in other EU member states.

The rules on notifying a personal data breach are basically the same regardless in which EU member state, the notification is made.

Meanwhile, the provisions of the GDPR on which EU supervisory authority shall be competent to process a notification entail that the competent authority, which is to receive and process the notification, is not necessarily located in the same country in which the data controlling company responsible for the breach is located.

The competent authority is the supervisory authority of the country in which the main establishment is situated, or the country in which the establishment making all decisions about the company's processing of personal data is located.

The competent supervisory authority is referred to as the lead supervisory authority.

This means that when a breach pertains to the protection of personal data of data subjects in more than one EU member state, the data controller must notify the lead supervisory authority.

Data controlling companies handling cross-border processing should therefore consider which supervisory authority among EU's member states should be their lead supervisory authority. This should be stated in the company's contingency plan in order for the company to be prepared in the event of a breach.

If the data controller has not yet considered such, the company should notify the supervisory authority of the country in which the breach has occurred.

When the data controller notifies a personal data breach to the lead supervisory authority, it should also notify that the breach comprises establishments in other EU member states and in which EU member states there are data subjects affected by the breach.

Once the lead supervisory authority - e.g. CNIL in France - has received the notification, including information that data subjects in other EU member states are affected by the personal data breach, it is the authority's responsibility to notify the relevant supervisory authorities in the particular member states.

Example:

Through its website, a company with its main establishment in France, offers online sales of clothes.

In connection with an update of the website, the company by mistake discloses a list stating the company's customer database. The list contains the customers' full names, and information on payment, contact and addresses also appears.

The company has customers in France, but some of the customers are also located in other EU member states, and from the disclosed list the company can establish that customers domiciled in Germany, Belgium and the Netherlands, respectively, are affected by the breach.

The company assesses that the breach should be notified and therefore it notifies CNIL.

It is stated in the notification that data subjects in the above said EU member states have been affected.

Accordingly, CNIL shall notify the supervisory authorities of Germany, Belgium and the Netherlands.


Henrik Christian Strand


Pernille Kristensen


Michael Gravesen


Bianca Britt Nielsen

Do you require our assistance?

In the event of personal data breach, our experts are ready to assist you in notifying the breach to the relevant supervisory authority.