Romania - Data Breach Notification

In case of a cross-border data breach affecting Romanian residents, is there any legal obligation to notify either (i) the Romanian Data Protection Authority ("DPA"); or (ii) the affected individuals? Can an organization located outside the EU appoint a Lead Supervisory Authority?

The General Data Protection Regulation of European Union no. 679 of 2016 (the "**GDPR**") now makes data breach notification mandatory for all the data controllers *unless* a personal data breach is unlikely to result in a risk to the rights and freedoms of individuals. The GDPR applies to any organisation in the world that deals with the personal data of European Union (EU) residents. Thus, GDPR also applies to the US companies whose websites are made available to individuals in the EU and which process such data in EU, or which collect personal data from EU-based job applicants, employees, or independent contractors.

The GDPR introduced the requirement for a personal data breach to be notified to the data protection authority, i.e. the competent national supervisory authority or in the case of a cross-border breach, to a Lead Supervisory Authority ("**LSA**"). What this means in practice for a multinational organisation that processes EU data subjects' personal data, is that instead of filing data breach notifications with national regulatory authorities in each location where it processes data or where its data subjects are based, it may appoint a LSA that will deal with all relevant matters. LSA will further notify the data breach notification, and liaise with the relevant EU national regulatory authorities.

An organisation located outside EU which processes personal data of EU-based data subjects, and it does not have a registered presence in the EU, e.g. branch or subsidiary, cannot appoint a LSA. Therefore, it has to file data breach notifications with the supervisory authority at each location where it operates and/or where its data processing affects its data subjects, and notify the affected individuals. Thus, in case the personal data incident affected the personal data of a Romanian resident, such organization located outside EU must file the data breach notification with the DPA.

Is there: (i) any required or suggested content of the data breach notification to be filed with the DPA; (ii) a deadline in which notice must be filed; or (iii) a method of filing the notification, such as regular mail, email, web-posting or publication?

<u>Content of the notification</u>

Even if no specific derogations are provided by the Law no. 190 of 2018 on the Measures for the Application of the GDPR in Romania with regard to the Notification of a Personal Data Breach, the DPA issued the Decision no. 128 of 2018 on the Approval of the Template for the Personal Data Breach Notification under the GDPR. Thus, the data controller must fill in the information requested by the notification template approved by the DPA.

<u>Deadline for filing the notification</u>

The data controller must notify the data security breach which is likely to result in a risk to the rights and freedoms of individuals to the DPA without undue delay and, if possibly, within no more than 72 hours from the date on which it became aware of it.

Filing Method

The notification must be electronically signed and thereafter sent to the email address brese@dataprotection.ro.

The breach notification which are not electronically signed are not taken into consideration by the DPA.

This article provides general information and should not be considered as legal advice. For more information about the issues discussed above, you can contact us at office@buzescu.com.

Buzescu Ca