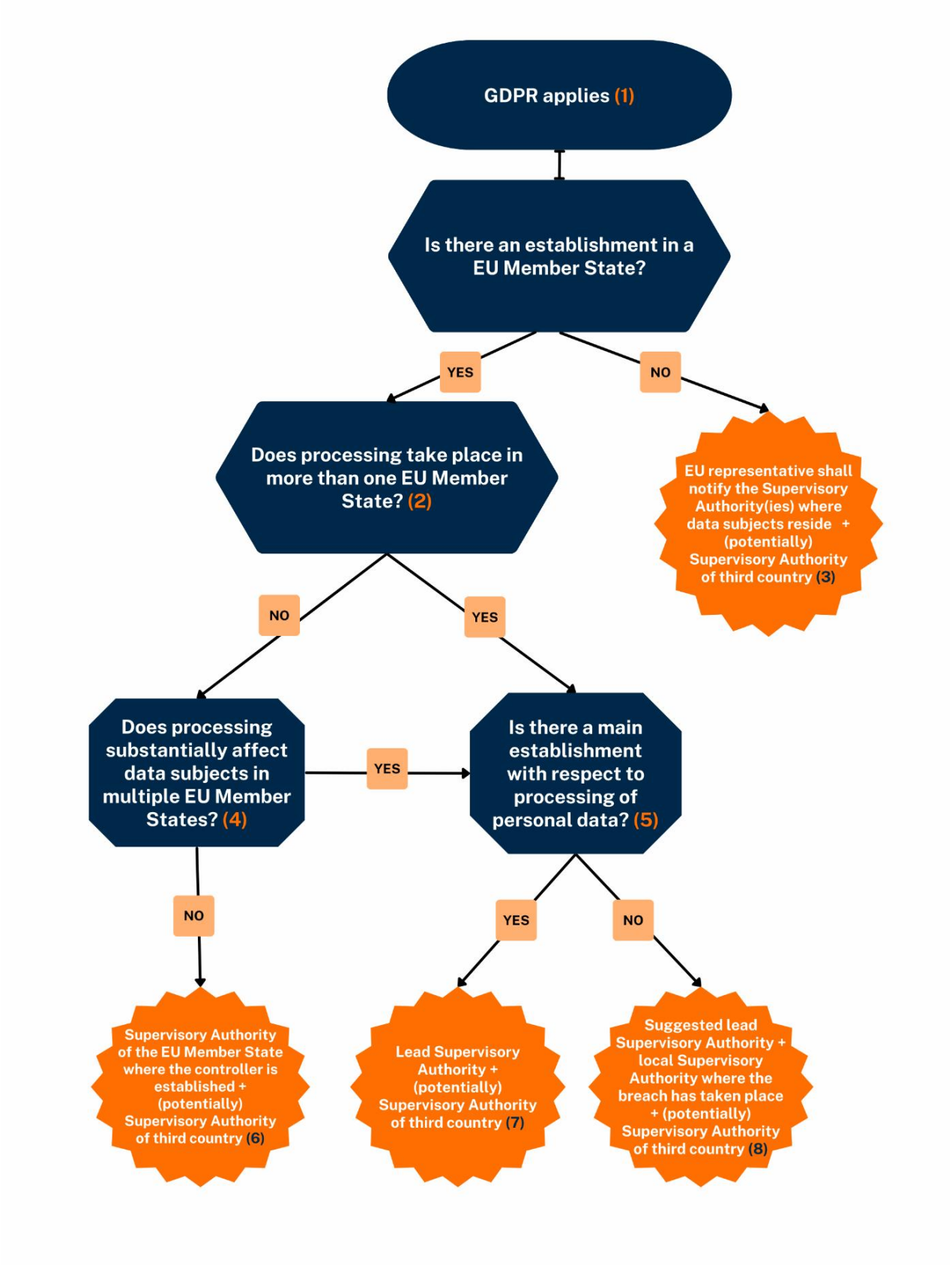
LYDIAN

Where to notify a personal data breach?

September 2023

Ransomware, malware, hacking and phishing … all phenomena that organisations are facing on a large scale. Data breaches are here to stay in our highly digitised world, and both large and small organisations have to deal with them. Even organisations that have far-reaching security policies in place can be affected, whether it comes from a crafty cybercriminal or a small mistake by an employee. The question is not whether an organisation will be affected, but rather when.

Data breaches under the GDPR should be reported to the Supervisory Authority. When it comes to complex corporate structures that cross national borders, it is not always easy to ascertain to which Supervisory Authority exactly a data breach should be notified. Lydian's *Information Governance & Data Protection (Privacy)* team therefore put together the below practical flow chart to help you answer this question.


GDPR applies (1)
Is there an establishment in a EU Member State?
YES
NO
Does processing take place in more than one EU Member State? (2)
EU representative shall notify the Supervisory Authority(ies) where data subjects reside + (potentially) Supervisory Authority of third country (3)
NO
YES
Does processing substantially affect data subjects in multiple EU Member States? (4)
YES
Is there a main establishment with respect to processing of personal data? (5)
NO
YES
NO
Supervisory Authority of the EU Member State where the controller is established + (potentially) Supervisory Authority of third country (6)
Lead Supervisory Authority + (potentially) Supervisory Authority of third country (7)
Suggested lead Supervisory Authority + local Supervisory Authority where the breach has taken place + (potentially) Supervisory Authority of third country (8)

1) Please note that this flow chart only applies to data breaches suffered by organisations that are subject to the GDPR. Organisations must consider the material and territorial scope of the GDPR.

   Pursuant to Art. 2 GDPR, processing of personal data falls under the **material scope of application** in case it done wholly or partly by automated means or forms part, or is intended to form part, of a filing system. Excluded from the material scope is processing of personal data (a) in the course of an activity which falls outside the scope of EU law; (b) by the EU Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on the European Union (TEU); (c) by a natural person in the course of a purely personal or household activity; and (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

   Pursuant to Art. 3 GDPR, processing of personal data falls under the **territorial scope of application** in case it takes place in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not. Moreover, the GDPR also applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or (b) the monitoring of their behaviour as far as their behaviour takes place within the EU. Excluded from the territorial scope of the GDPR is processing of personal data by a controller not established in the EU, but in a place where EU Member State Law applies by virtue of public international law.

2) This is the first criterion of cross-border data processing as defined in Art. 4 (23) (a) GDPR.

3) Controllers not having an establishment in a EU Member state but subject to the GDPR pursuant Art. 3 (2) GDPR cannot benefit from the one-stop-shop system, even if they have appointed a EU representative pursuant Art. 27 GDPR. As a result, the data breach will need to be notified to the Supervisory Authorities of all EU Member States where affected data subjects reside. In addition, the data breach may need to be notified to Supervisory Authorities in third countries (i.e. outside the EU).

4) This is the second criterion of cross-border data processing as defined in Art. 4 (23) (b) GDPR.

5) As it concerns a cross-border data processing, the organisation must identify the Lead Supervisory Authority, which depends on the location of the ‘main establishment’ or ‘single establishment’ in the EU.

   - For controllers, this means the place of its central administration in the EU, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the EU and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment.
   - For processors, this means the place of its central administration in the EU, or, if the processor has no central administration in the Union, the establishment of the processor in the EU where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under the GDPR.

6) In this case, there is no cross-border data processing as defined in Art. 4 (23) (b) GDPR. It concerns a purely local processing. The data breach will need to be notified to the Supervisory Authority of the EU Member State where the

controller is established. In addition, the data breach may need to be notified to Supervisory Authorities in third countries (i.e., outside of the EU).

7) In this case, the processing is a cross-border data processing as defined in Art. 4 (23) (b) GDPR and a Lead Supervisory Authority can been identified. The data breach will need to be notified to the Lead Supervisory Authority. Given the one-stop-shop principle, no other notifications within the EU are needed. Organisations are strongly advised to analyse and document (in accordance with the accountability principle) well on beforehand and in respect of each cross-border processing the identification of the Lead Supervisory Authority. Indeed, in the event of a data breach, the 72-hour deadline usually does not allow enough time for this analysis to take place. The data breach may however also need to be notified to Supervisory Authorities in third countries (i.e., outside of the EU).

8) In this case, the processing is a cross-border data processing as defined in Art. 4 (23) (b) GDPR. However, no Lead Supervisory Authority could be identified as there is no central administration in the EU. This could be the case for multinational companies for which decisions about processing are exclusively taken outside the EU. In these circumstances, the EU establishment that has the authority to implement decisions about and take liability for processing, shall be designated. The Supervisory Authority of such EU Member State shall thereby function as the lead Supervisory Authority. However, as forum shopping is not permitted under the GDPR, this decision to designate the establishment can be challenged by other relevant Supervisory Authorities or the EDPB. If there is any doubt as to the identity of the Lead Supervisory Authority then at a minimum the local Supervisory Authority where the breach has taken place shall be notified. The data breach may however also need to be notified to Supervisory Authorities in third countries (i.e., outside of the EU).

Bastiaan Bruyndonckx
Partner
+32 (0)2 787 90 93
bastiaan.bruyndonckx@lydian.be

Olivia Santantonio
Counsel
+32 (0)2 787 90 07
olivia.santantonio@lydian.be

Liese Kuyken
Associate
+32 (0)2 787 91 34
liese.kuyken@lydian.be