THE
NATIONAL LAW REVIEW

GDPR Enforcement: Portugal

Tuesday, February 19, 2019

A hospital became one of the first organisations to face GDPR enforcement in Portugal in July 2018. The hospital received a €400,000 fine from the Portuguese regulator, Comissão Nacional de Protecção de Dados ("CNPD") for various breaches of the GDPR.

The hospital was fined for the following three violations of the GDPR:

1. Breach of the data minimisation principle;
2. Breach of the integrity and confidentiality principle; and
3. The failure to ensure the ongoing security of processing under Article 32 of the GDPR.

For breaches of the data protection principles, a maximum fine of €20,000,000 or 4% of global turnover, whichever is higher, may be imposed. However, the maximum fine for the third violation is €10,000,000 or 2% of global turnover, whichever is higher.

Article By Emma Yaltaghian
Rosa Barcelo
Squire Patton Boggs (US) LLP
SECURITY & PRIVACY // BYTES

Communications, Media & Internet
Health Law & Managed Care
Global
Portugal

Breach of the data minimisation principle

The data minimisation principle requires that only relevant personal data is retained.

In this scenario, doctors at the hospital, regardless of speciality, could access all patients' clinical information. Further, nine members of technical staff benefitted from medical status and therefore were able to access patient data beyond what was required by their roles. The CNPD found this to be a breach of the data minimisation principle because personal data could be accessed for wider purposes than was necessary.

This specific breach constituted €150,000 of the €400,000 fine.

Breach of the integrity and confidentiality principle

The GDPR further mandates that personal data must be kept confidential and that appropriate technical and organisational measures must be used to prevent unlawful processing.

The CNPD found that by granting access to all patients' clinical information, regardless of a doctor's speciality, breached the confidentiality and integrity principle. Personal data was accessible by a wider group of people than was appropriate in the circumstances. Therefore, there was a risk that it could have been unlawfully processed.

This specific breach also constituted €150,000 of the €400,000 fine.

Failure to ensure ongoing data security

The third violation relates to ongoing and prolonged data security failures including the "*ongoing confidentiality, integrity, availability and resilience of processing systems and services*", as well as failing to have "*a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures*" (Article 32).

The hospital did not actively update user credentials in order to prevent unauthorised access to personal data. It also failed to implement technical and organisational measures that were appropriate to the risks involved. Greater risks were present because of the access to special categories of personal data (i.e. health-related data) and the large number of data subjects.

This third violation incurred a €100,000 portion of the fine.

Defence

The hospital, by way of defence or mitigation, asserted that it simply used the software provided by the Portuguese healthcare authority. This, however, was not accepted by the CNPD. The CNPD insisted it should have carried out its own due diligence checks and been aware that the software was not GDPR compliant.

Media influence

Interestingly, the CNPD investigated this breach because of a newspaper report that detailed the hospital's activities, not because of a formal complaint or breach notification to the CNPD. In the EU investigations tend to arise from complaints to the regulator, but Supervisory authorities have the power to start ex officio investigations, which may result from newspaper/media reports. Such type of investigations are seen more commonly with HIPAA investigations in the United States of America.

Lessons

This enforcement action demonstrates how seriously the regulators are taking the data protection principles, as breaches of the principles make up the bulk of this fine. The implementation of appropriate technical and organisational measures is an excellent method of demonstrating commitment to the principles. Generally, in terms of implementing technical measures it would be prudent to work with the organisation's IT team. Examples of organisational measures may include the following:

- Information notices;
- Policies; and
- Contracts with third parties.

A further organisational measure might include assigning responsibility for the implementation of policies and determining how data security measures will be escalated throughout the organisation. Such measures must be appropriate to the risks presented by the processing and will be fact-specific. Where special categories of personal data are present or large numbers of data subjects are being monitored, more extensive measures will need be included and recorded.

Additionally, organisations need to carry out their own due diligence on items such as third party software and not just rely on the assurances of the third party, in line with the GDPR principle of accountability and privacy by design. Organisations should be able to show that they have vetted the third-party software they use and if they find a gap, they need to be able to close it, or show that they are working to close it and in the interim, detail how it is protecting that data.