Simmons & Simmons elexica

Data security and data breaches

In brief

The Regulation requires data controllers and data processors to take a risk based approach to the implementation of security measures to protect against loss or unauthorised disclosure of personal data. Data controllers will also need to revamp their security incident monitoring and reporting processes to comply with a mandatory requirement to notify data protection authorities of security breaches, whilst data processors are subject to a stand alone legal duty to notify relevant data controllers of security breaches. In a widely defined range of circumstances, data controllers will also be required to notify affected individuals.

Background

The current EU Data Protection Directive (95/46/EC) requires data controllers to implement appropriate technical and organisational measures to protect personal data against accidental loss, alteration, unauthorised disclosure or access. As part of this requirement, data controllers are required to enter into written agreements with data processors processing personal data on their behalf requiring the implementation of appropriate security measures.

Under the current EU Data Protection Directive, EU Member States are not required to implement rules obliging data controllers or data processors to make a notification (whether to data protection authorities or data subjects) if a security incident causes the loss of, or unauthorised disclosure or access to, personal data. As a result, at present it is rare for organisations to be legally required to report data security breaches. However there are some exceptions to this: for example, in Germany, data protection authority and data subjects must be notified without delay if an incident occurs in certain circumstances. Other exceptions derive from specific legal requirements in certain sectors, such as the telecoms sector, where more stringent obligations, including notification obligations, seek to protect consumers from network security or data security breaches.

Changes in detail

Technical and organisational security measures

Under Article 30(1) of the Regulation, both the data controller and the data processor will be required to implement appropriate technical and organisational security measures, such as pseudonymisation of the personal data, to ensure a level of security appropriate to the risk.

When implementing appropriate security measures, the data controller and the data processor will need to take account of:

(A) the available technology

(B) the costs of implementation

(C) the nature, scope, context and purposes of the processing

(D) the likelihood and severity of the risk for the rights and freedoms of individuals, and

(E) the risks represented by data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Adherence to approved codes of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the above mentioned security measures requirement (Article 30(2a)).

Moreover the data controller and the data processor are required to take steps to ensure that no person acting under their authority shall process personal data protection without instructions from the controller, unless otherwise required by applicable law (Article 30(2b)).

Resilience and availability

The Regulation goes beyond merely covering data security. The listed “security” measures to be considered by data controllers include:

- the ability to ensure the ongoing integrity and availability and resilience of the systems processing data, and
- the ability to restore availability and access to data in a timely manner in the event of an incident.

Notification of authorities and data subjects

Articles 31 and 32 of the Regulation relate to the notification of security breaches. These Articles refer to the concept of “personal data breach”, defined in Article 4(9) as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.”

The tables below summarise the obligations that data controllers (and to a lesser extent data processors) will have to notify data protection authorities and data subjects in the event of a personal data breach.

Notification of data protection authorities	
Article	Obligation

Article 31(1)	If a personal data breach occurs, which is likely to result in a high risk for the rights and freedoms of individuals, the data controller will be required to notify its national data protection authority “without undue delay” and where feasible not later than 72 hours after having become aware of it. The notification to its national data protection authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.
Article 31(2)	A data processor will need to notify the data controller “without undue delay” after becoming aware of a personal data breach.
Article 31(3)	The notification served on the data protection authority will need to: (A) describe the nature of the personal data breach including, where possible and appropriate, the approximate categories and number of data subjects concerned and the categories and approximate number of data records concerned (B) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained (C) describe the likely consequences of the personal data breach, and (D) describe the measures taken or proposed to be taken by the controller to address the personal data breach and mitigate the possible adverse effects of the personal data breach.
Article 31(3a)	When the communication of information described above is not possible at the same time the data controller may provide the information when it is possible but without undue further delay.
Article 31(4)	The data controller will need to keep records of personal data breaches, including the facts of each breach, its effects and remedial action taken. The data controller’s records must be sufficient to enable the national data protection authority to verify compliance with the data controller’s obligations under Article 31.
Notification of data subjects	
Article	Obligation
Article 32(1)	The data controller will be required to notify data subjects “without undue delay” when a personal data security breach is likely to result in a high risk for the rights and freedoms of individuals, unless the exemption in Article 32(3) applies.
Article 32(2)	The data controller’s notification to data subjects must: (A) describe the nature of the breach (B) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained (C) describe the likely consequences of the breach, and (D) describe the measures taken or proposed to be taken by the controller to address the personal data breach and mitigate the possible adverse effects of the personal data breach.

Article 32(3)	The data controller will be excused from having to notify data subjects if: (A) the controller has implemented appropriate technological and organisational protection measures and those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption (B) the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects is no longer likely to materialise, or (C) it would involve disproportionate effort. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Analysis

The requirement to implement data security measures under the Regulation is one example of the extension in scope of data protection obligations under the Regulation to data processors. Whilst Article 30 imposes stand-alone obligations on data processors with regard to data security, data controllers will also need to ensure that contracts entered into with data processors require them to take “all appropriate measures” pursuant to Article 30.

The security measure requirements of the Regulation are broadly equivalent to the existing requirements of the Data Protection Directive. However, the focus on resilience and availability of systems processing data seems to stretch the requirements beyond pure data security.

The process of notification of security breaches set out in Articles 31 and 32 of the Regulation to a large extent reflects the breach notification system under Article 4(3) of E-Privacy Directive 2002/58/EC, which is binding on providers of publicly available electronic communications systems and there has been a debate for some time about whether there is any logic to companies in the communication sector having a security breach notification requirement whilst companies in other sectors (sectors that may commonly handle more sensitive data) do not.

Data controllers are required to notify the data protection authorities without delay and, where feasible, not later than 72 hours after becoming aware of a breach. This reflects a compromise position between two earlier drafts of the Regulation: (i) the EC’s proposal, which provided for a 24 hours’ notice and (ii) the water down version of the Civil Liberties, Justice and Home Affairs Committee of the European Parliament (LIBE), which did not provide for a specific timeline but solely required data controllers and data processors to act “without undue delay”.

It will be challenging for data controllers to make informed notifications within 72 hours and it may well be that, in most cases, holding notifications will have to be made with further detail being provided subsequently.

Conclusion

Matters of data security are already central to data controllers’ data protection compliance obligations under existing law, and data processors will usually find themselves bound by equivalent obligations under the contracts they enter into with data controllers. The implementation of further security measures reflecting the prescriptions of the Regulation and the greater enforcement threat may mean greater resource needs to be devoted to compliance in this area. The harmonised

security breach notification obligations under the Regulation will also, inevitably, place an increased administrative burden on organisations. A data breach incident management increasingly looks at the required corporate governance lead.

elexica Limited, CityPoint, One Ropemaker Street, London EC2Y 9SS