January 29, 2021

European Data Protection Board Issues Guidelines on Examples Regarding Data Breach Notification

Attorneys
Clare Sellars

On 14 January 2021 the European Data Protection Board (EDPB) adopted Guidelines 01/2021 on Examples Regarding Data Breach Notification, ("Guidelines"). The Guidelines are intended to complement the Guidelines on Personal Data Breach Notification under Regulation 2016/679, ("GDPR"), WP 250, ("Guidelines WP250"), which were produced by the Article 29 Working Party, ("WP29") in October 2017. The Guidelines are intended to be practice-orientated, case-based guidance giving worked examples and non-exhaustive lists of advisable organisational and technical measures that may assist with prevention and mitigation in each case. The examples provided draw on the experiences of European national supervisory authorities ("SAs") since the application of the GDPR and are intended to assist data controllers in deciding how to address personal data breaches and which issues to consider during risk assessment. Comments on the new Guidelines are invited and should be submitted by 2 March 2021.

The GDPR defines a personal data breach 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*." WP29 has previously classified personal data breaches into three main groups: confidentiality breaches, which involve unauthorised or accidental disclosure of, or access to, personal data; integrity breaches, which involve unauthorised or accidental alteration of personal data; and availability breaches, which involve accidental or unauthorised loss of access to, or destruction of, personal data.

Breaches can have a number of possible significant undesirable consequences for data subjects, which can lead to physical, material or non-material damage, including, among other things, loss of control over their personal data, fraud or identity theft, reputational damage, financial loss and other serious social or economic disadvantages. Data controllers must consider these risks to individuals' rights and freedoms and implement suitable technical and organisational measures to tackle them. Under the GDPR, controllers are required to document personal data breaches; notify the competent SAs of breaches, unless they are unlikely to result in risks to individuals' rights and freedoms; and inform individuals of breaches if they are likely to lead to high risks to the data subjects' rights and freedoms.

In some cases, controllers will be able to appreciate that an incident is likely to result in a risk and will need to be notified, while in others controllers do not need to wait until the risk and impact surrounding the breach have been fully considered, as the full risk assessment can take place in parallel with notification, and information obtained can be made available to SAs in stages without excessive further delay. It is also important to note that controllers should not wait for a detailed forensic examination and (early) mitigation steps before deciding whether breaches are likely to result in a risk and should therefore be notified – they should make this assessment on discovering the breach.

The Guidelines discuss the fact that all controllers should implement data breach policies and procedures and clear accountability structures. Appropriate personal data breach management training for relevant personnel is also emphasized, as is accountability and data protection by design. Personal data breach handbooks are also recommended as roadmaps for how to handle personal data breaches.

The various examples of different types of personal data breaches described in the new Guidelines are fictitious, but are founded on SAs' involvement in data breach notifications. The EDPB notes that, if the circumstances of actual incidents differ from the examples provided, they may result in different risks, which may require alternative steps to be taken. Various scenarios involving ransomware, data exfiltration attacks, internal human risk sources, lost or stolen devices or paper documents, mispostal issues and cases involving social engineering are considered. In each case, various examples are provided, together with an analysis of appropriate prior measures and risk assessment and mitigation and obligations. In most cases, organisational and technical measures for preventing/mitigating the impacts of the particular type of breach in question are also considered.

Ransomware

Ransomware attacks often lead to the need for data breach notification. Ransomware attacks involve malicious code encrypting personal data, with the bad actor requiring a ransom in exchange for a decryption code. Ransomware attacks usually constitute availability breaches, but confidentiality breaches may also be involved. The Guidelines consider examples of data breaches involving ransomware with proper backup and without exfiltration, ransomware without proper backup, ransomware with backup and without exfiltration in a hospital and ransomware without backup and with exfiltration.

The EDPB emphasises the importance of a comprehensive evaluation of the data security systems of controllers who suffer ransomware attacks, with special emphasis on IT security, and notes that any vulnerabilities that are identified should be documented and tackled without delay, as key elements of advisable organisational and technical measures for preventing/mitigating the impacts of ransomware attacks.

Suggested measures include, among other things, keeping relevant firmware, operating system and application software up to date and ensuring that all reasonable IT security measures are established, effective and regularly updated; ensuring that processing systems and infrastructure separate data systems and networks to avoid the proliferation of malware within the organisation and to external systems; establishing an up-to-date, secure and tested backup procedure; implementing appropriate, up-to-date, effective and integrated anti-malware software and firewall and intrusion detection and prevention systems; implementing appropriate employee training; putting in place robust encryption and authentication; and carrying out regular vulnerability and penetration testing.

Data Exfiltration Attacks

Data exfiltration attacks take advantage of weaknesses in services offered over the internet and are usually intended to copy, exfiltrate and abuse personal data for some malicious purpose. Data exfiltration attacks mainly comprise breaches of confidentiality and sometimes also data integrity. The Guidelines explore examples involving exfiltration involving job application data from a website, exfiltration of hashed passwords from a website and credential stuffing on a banking website.

To assist in preventing/mitigating the impacts of data exfiltration attacks, the Guidelines emphasise the importance of re-evaluating IT security systems and suggest measures that include use of sophisticated encryption and key management, (with cryptographic hashing and salting for secret information such as passwords being preferred over encryption and authentication methods that do not involve passwords being preferable); keeping systems (software and firmware) updated and ensuring that all IT security measures are in place, effective and regularly updated when circumstances or processing change; using strong authentication methods, such as two-factor authentication, together with an up-to-date password policy; secure development standards, such as the filtering of user input and brute force prevention measures, (e.g. limiting the number of re-tries); implementing strong user privileges and access control management policies; using suitable, current, effective and integrated firewall, intrusion detection and other perimeter defence systems; carrying out regular IT security audits and vulnerability assessments (penetration testing); and performing regular evaluations and analysis to ensure backups can be used to restore any data whose integrity or availability has been affected.

Internal Human Risk Source

Human error leading to personal data breaches is a frequent occurrence and can be both deliberate and accidental, making it difficult for data controllers to identify weaknesses and take steps to avoid them. The EDPB considers various examples of data breaches of this nature, including exfiltration of business data by a former employee and accidental transmission of data to a trusted third party, noting that such breaches usually comprise breaches of confidentiality.

Human errors may by reduced or mitigated by, among other things, conducting regular employee training, education and awareness programs; establishing and maintaining effective data protection and privacy practices, procedures and systems; establishing robust access control policies and obliging users to adhere to them; putting in place practices to force user authentication when accessing sensitive personal data; de-activating users' company-related accounts

immediately when they leave the company; monitoring unusual dataflow between file servers and employee workstations; reviewing employees' access policies; de-activating open cloud services; prohibiting access to known open mail services; making clear desk policies compulsory and automatically locking computers after certain periods of inactivity; and using dedicated systems for managing personal data that apply appropriate access control mechanisms to prevent human error (e.g. sending communications to the wrong subject).

Lost or Stolen Devices and Paper Documents

Portable devices are often stolen or lost, meaning that controllers must consider the circumstances of the processing operation, such as the type of data stored on the device, the supporting assets and steps taken before the breach to ensure suitable security, which all impact upon the possible effects of the data breach. The Guidelines note that risk assessment may be difficult if devices are no longer available. These breaches constitute confidentiality breaches, but can also compromise availability and integrity if there is no backup for a stolen database. The Guidelines consider various examples involving stolen material storing encrypted personal data, stolen material storing non-encrypted personal data and stolen paper files with sensitive data.

To prevent or mitigate the impact of loss or theft of devices, organisations should consider activating encryption on devices; using passcodes/passwords on all devices; using multi-factor authentication; activating functionalities to allow mobile devices to be located in case of loss; using secure VPNs to connect mobile devices to back-end servers; properly regulating device usage; and using mobile device management software/apps, enabling remote wipe functions and installing physical access controls.

Mispostal

Breaches involving mispostal also involve internal human error, but not malicious action. As few mitigating steps by controllers are possible in cases of mispostal, avoidance is even more important than with other types of breaches. The Guidelines explore various examples involving snail mail mistake, sensitive personal data sent by mail by mistake and personal data sent by mail by mistake.

Although mispostal may seem less of a risk, steps suggested for preventing/mitigating the impacts of mispostal include, among other things, setting rigorous standards for sending letters and emails; listing multiple email recipients in the Bcc field as standard; using automatic, rather than manual, addressing using data from a current database; applying message delay when sending emails; and de-activating auto-complete when typing in email addresses.

Social Engineering

The Guidelines also consider certain other types of personal data breaches linked to social engineering, including examples involving identity theft and email exfiltration. The EDPB focuses on a number of measures that could help to prevent such attacks, such as the importance of appropriate authentication mechanisms and robust prior client validation processes, (recommending out-of-band multi-factor authentication methods).

Comment

The Guidelines will provide welcome guidance to data controllers in respect of various different types of personal data breaches, and the practical real-life examples should assist controllers who experience similar breaches. The scenarios set out should help controllers to determine whether any personal data breaches that they suffer are sufficiently serious to merit notification to the relevant SAs and also any data subjects impacted by such breaches. The clarity of the Guidelines may be helpful both to organisations and the resource-constrained SAs in preventing over-reporting of personal data breaches. It will be interesting to see what comments are received regarding the draft Guidelines and whether further details and examples will be included in the final version.