TRANSCENDENT GROUP INSIGHT

In case of an emergency: Personal data breaches– what they are, what to do, and why it is important to act swiftly on them

Data, especially personal data, are the crown jewels of many organizations. These assets need protection against destruction, loss, modification or from falling into the wrong hands, whether by mistake or by malicious intent.

The General Data Protection Regulation (GDPR) provides the regulatory framework for how to manage and protect personal data. Under its requirements, companies have put into place organizational and technical measures to help avoid wrongful disclosure. However, sometimes these measures are not enough, and a breach of personal data occurs. With this article, we want to raise awareness about what to do when you suspect a personal data breach. If nothing else, perhaps this article can serve as a just-in-case-safety card, similar to aircraft safety instructions in seat pockets in front of you, only without the cryptic pictographs.

What is personal data?

Personal data include any information related to a person or "data subject", which would allow to identify them by for example name or through other attributes, such as social security number, images, or IP address. Personal data are everywhere: in clients or potential clients files, including information on representatives within corporate companies, staff or third parties.

What is a personal data breach?

As technical and digital as the world has become, and as much as cyber threats are relevant, breaches are often caused by the person in front of the screen: During 2020, almost 60% of all personal data breaches reported to the Swedish Data Protection Authorities were due to human error, and 40% of breaches stemmed from information sent to wrong recipients[1].

This is what is called a confidentiality breach, i.e. personal data is disclosed to someone who should not have access to that information. Other types of breaches include integrity breaches, where data is accidentally or unlawfully changed (e.g., external threats to personal data including hacked accounts), as well as availability breaches when personal data is not accessible or even destroyed when files are lost or deleted or systems are down for a certain period.

What to do when suspecting a personal data breach?

Personal data breaches should be flagged as soon as possible. Companies have the obligation to protect people's personal data and should therefore have clear internal instructions on how to handle a data breach. It is important to detect and react, assess, mitigate and escalate incidents, especially as certain severe incidents require reporting to the Data Protection Authorities within 72 hours of detecting the incident. That means three calendar days, and unfortunately incidents have a tendency not to appear on Monday mornings 9am, so it is important to report in line with existing processes. This should at least include escalating to the manager as soon as possible and registering the incident in the internal incident handling platform, documenting as much details as available.

If the 72 hours timeline cannot be kept or has already passed, incidents should of course be raised anyway. In the event the incident turns out not to be a personal data breach, or it is a minor breach that does not require reporting to the Authorities or the affected data subjects, it is still important to make that assessment, as swiftly as possible.

This process is about protecting personal data and the trust in the organization - it is not about spot-lighting mistakes or placing individual blame. Moreover, it may help the company to improve internal processes as what went wrong is investigated, in order to evaluate how to avoid something similar in future.

Steps to take in a personal data breach

1. Escalate the data breach immediately, register the data breach and involve the responsible privacy unit in your organization
2. Mitigate privacy risks where possible – any measures that help to stop or "heal" the incident
3. Identify what kind of breach it is:
    1. Who and how many people have been affected?
    2. What personal data categories can be involved in the data breach?
4. Assess the severity of the personal data breach, take relevant action and follow up

[1] IMY: Anmälda personuppgiftsincidenter 2020 (in Swedish language)

How do I know if it is a confidentiality, availability or integrity breach, and how severe it is?

To avoid subjectivity as much as possible, deciding the nature of the data breach and its severity should be based on an acknowledged model applied to make objective assessments. The most recognized is the EDBP and data protection authority-endorsed ENISA methodology. This rather self-explanatory framework serves as a guide through the various elements of assessment, and helps to address the relevant details about the incident as are available on the when, what, how and why of it.

More information

Don't recognize the above in your organization and want to know more? Contact our team of experienced privacy consultants if you want to strengthen the awareness in your organization or enhance your processes for managing incidents. Visit transcendentgroup.com or contact the authors below.

Åsa Nilsson
Gothenburg
Phone: +46 72 196 36 66
asa.nilsson@transcendentgroup.com

Cécile Marcotte
Oslo
Phone: +47 455 00 957
cecile.marcotte@transcendentgroup.com

Andreas Liese
Malmö
Phone: +46 70 143 50 49
andreas.liese@transcendentgroup.com