IMY. Integritetsskydds myndigheten

Reported personal data breaches 2022

A national overview with an examination of malicious attacks and a Nordic comparison 2019–2022

IMY Report 2023:2

Summary

A personal data breach is when data under the control of an organisation is exposed in a security incident that leads to a breach of confidentiality, unauthorised access or breach of privacy. If this occurs and it is likely that the personal data breach threatens the rights and freedoms of an individual, the organisation must report the incident to IMY without unnecessary delay and no later than within 72 hours after having become aware of the incident.

In 2022, IMY received about 5,330 reports of personal data breaches, of which 70 per cent came from the public sector and about 25 per cent from the private sector. Within the public sector, every fourth incident was reported by a government agency and every fifth incident was reported by medical and health services.

Sixty-three per cent of reports can be categorised as some form of unauthorised access, either through information sent by mistake or by other incorrect handling of personal data (25 per cent).

Fifty-nine per cent of all reports of personal data breaches in 2022 were attributed to human error. Often this involved a person making a mistake when handling personal data in their work. More than half of the personal data breaches caused by human error were letters, emails and SMS messages sent in error. Compared with the previous year, the percentage of reports from the health and medical care system attributed to human error increased.

The changed security situation with the war in Ukraine and Sweden's application for membership in NATO caused many to be concerned that Sweden would face more cyber attacks in 2022. Despite this concern, IMY's study shows that malicious attacks as defined by GDPR fell compared with the previous year. The most malicious attacks, 140 cases, were reported by the private sector (excluding the financial sector or insurance sector). Other relatively exposed organisations included municipal organisations and schools and education, which submitted about 40 reports of malicious attacks involving personal data.

IMY's recommendations for preventing personal data breaches

This year's compilation of reports on personal data breaches 2019–2022 shows that not quite 60 per cent of reports each year are attributed to human error. Since these can be of a serious nature and place the freedoms and rights of individuals at high risk, IMY publishes recommendations that can help prevent incidents and mitigate the consequences when breaches do occur.

A detailed description of IMY's recommendations is available in Appendix 3.

Systematic information security is crucial

With so many personal data breaches being attributed to human error and that these can lead to serious incidents means this is an important factor to consider in your organisation's systematic information security. Organisational and technical security measures need to be integrated into the organisation's routines and enable the ability to easily act correctly and difficult to make mistakes.

The organisation's security level in relation to the risks to the freedoms and rights of individuals

The security level must be understood in relation to the processed personal data and the specific risks to the freedoms and rights of individuals that are inherent in your operations. This means that it is not possible for an organisation to simply copy the security measures of other organisations and there must be a continual focus and assessment on security as the organisation, technology and, thereby, the risks continually change.

Reduce the risk of mistakes

Organisational and technical measures can help you reduce the risk of staff making mistakes. Examples of this are technical solutions that prevent staff from saving information on removable media and preventing them from installing software and apps that are not approved centrally. Solutions that facilitate staff having password protected and encrypted email and attached files can also improve security.

Active authorisation control

Another important and fundamental security measure is having active authorisation control. Each authorisation is to be granted based on each staff member only gaining access to the personal data needed to be able to perform their job.

Processes that strengthen systematic information security

All organisations that manage personal data need to have documented and implemented risk management and personal data breach processes to be able to prevent, detect and manage personal data breaches. These processes must also enable continual learning from breaches that do occur.

Security culture

Achieving a good security culture requires the involvement of management in security questions, including the protection of personal data. A good security culture also communicates lessons learned from breaches and how these lessons can then be used to create an even better security culture and thereby contribute to systematic security.