Don't open the





to your personal

information

FACTS & FIGURES

Cybersecurity and personal data breaches

What is a personal data breach?

A personal data breach is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to transmitted, stored or processed personal data of individuals. The personal data unlawfully disclosed can be email addresses, passwords, health data or financial information.



Between January and July 2024, the EDPS received 68 data breach notifications, 12 of which were due to external attacks.

What are common cyber threats leading to personal data breaches?



When cyber-criminals try to obtain personal data from a person, by addressing them via email, phone call or direct message, and pretending to be someone they know in the hopes of convincing the recipient to provide personal information and/or their credentials to an online service.



When cyber-criminals impersonate a legitimate source, e.g. the website of an organisation or the email address of a colleague, to gain their victims' trust to convince them to click on or download a malicious link or software, or even to fill out a form with their personal data.



A malicious software created to infect devices, gather data, and send it to cyber-criminals without a person's consent. Users download this type of software on devices via vicious emails, text messages, websites, or infected USB-keys, without realising.

What are common consequences of personal data breaches?

For an individual, this may include identity theft, financial loss, psychological or reputational consequences. For an institution or organisation, this may cause reputational, financial (including a possible fine).

What can you do as an institution or employee to takle personal data breaches?

As an EU institution employee

- Stay informed and follow your institution's policies and procedures on cybersecurity and personal data breaches, by following training sessions for example.
- Regularly change your passwords with complex combinations.
- Update your anti-malware and software.
- Double-check emails that seem "too good to be true", such as emails offering discounts or money, or emails requesting access to personal data or sensitive files.
- Alert your institution's Data Protection Officer (DPO) and your Local Incident Security Officer (LISO) as soon as an incident occurs.

As an EU institution

- Put in place or regularly check and update your personal data breach procedure and cybersecurity awareness plan.
- Raise awareness and offer training to employees on procedures and policies to follow to prevent or respond to personal data breaches and cyber-attacks.
- Protect the personal data you handle by collaborating with your IT department to deploy privacy-friendly tools and encrypting data, for example.
- Work closely with your incident response team and CERT-EU to detect or address cyber threats and attacks; set up alerting tools and systems.
- Remember to notify the EDPS within 72 hours of detecting a personal data breach, it is mandatory under EU data protection law, Regulation (EU) 2018/1725.

What are common consequences of personal data breaches?



The Cybersecurity Regulation for EU institutions aims to establish common rules and minimum-security requirements to enhance individuals' safety and personal data. It emphasises the importance of establishing an internal cybersecurity risk management, governance and control framework, tailored to each EU institution's needs and the evolving nature of cyber threats and the interconnection of digital systems.







