CYBERSECURITY 101 · eBuilder Security

GDPR

The EU data protection law that turns weak security into a legal liability. Here is what it requires and how to stay on the right side of it.

WHAT IT IS

The General Data Protection Regulation governs how organisations collect, use and protect personal data. In force since 2018, it applies to anyone handling the data of people in the EU. Article 32 makes appropriate security a legal duty, which is why so many large fines follow a breach.

WHY IT MATTERS

1.2 billion euros

The largest GDPR fine so far, against Meta for unlawful US data transfers

Irish DPC, 2023

6 million kronor

IMY's fine on SportAdmin after a breach exposed 2.1 million people

IMY, 2025

20 million euros or 4%

The maximum fine for a serious breach, of global annual turnover

GDPR Article 83

WHAT HAPPENED

In 2018 attackers slipped into British Airways systems and redirected the payment details of around 500,000 customers to a fake site. The UK Information Commissioner's Office found BA had failed to secure the data under Article 32 and issued a 20 million pound fine in 2020. The way in was a supplier's compromised credentials.

RED FLAGS TO WATCH FOR

Common gaps that turn a GDPR duty into a fine.

- Personal data you cannot fully account for or locate
- Suppliers and cloud vendors with no signed Article 28 contract
- No tested plan to report a breach within 72 hours
- Access without multi-factor authentication, especially for third parties
- US-controlled services holding EU personal data with no transfer safeguard

THE ONE RULE THAT STOPS IT

Protect personal data as if a regulator will inspect it, because under GDPR one can.

THEN BUILD THE HABIT AROUND IT

- Map what personal data you hold and delete what you do not need
- Encrypt data and require multi-factor authentication on access

- Sign an Article 28 contract with every processor
- Rehearse the 72-hour breach report so it is ready in advance
- Run a konsekvensbedömning before any high-risk processing

MYTHS AND FACTS

MYTH

GDPR is only a legal or paperwork problem.

FACT

Most of the largest fines followed a security failure. Article 32 makes security a legal duty.

MYTH

Only big companies get fined.

FACT

IMY fined SportAdmin, a mid-sized supplier, 6 million kronor. Smaller organisations are in scope.

MYTH

EU servers mean the transfer rules do not apply.

FACT

A US-controlled provider can be compelled to hand over EU-stored data, so control matters as much as location.

THE LEGAL DUTY

Under GDPR a personal data breach must be reported to IMY within 72 hours. For essential and important entities the same attack is also a cyber incident under Cybersäkerhetslagen, reported since 1 July 2026 to the national cyber security centre at FRA.

GET HELP

See how each GDPR duty maps to practical security controls in the full guide.

Read the Full Article →