WHITE PAPER

General Data Protection Regulation (GDPR) & Cyber Security

HOLM SECURITY

GDPR & the Right to Protect Our Personal Data

Integrity & Confidentiality

Our right to integrity is a human right, according to the UN. Just as we have the right to lock our front door to protect ourselves from burglars, we have the right to privacy online. We decide who we want to welcome into our house. The EU Charter of Fundamental Rights stipulates that everyone in the EU has the right to protect their personal data and get access to data collected and the right to have it rectified. But new technology has eroded this human right, and companies continuously collect data for their own purposes.

Consistency & Increased Security

General Data Protection Regulation or GDPR came into force on May 25th, 2018. GDPR aims to create coherence around the management of personal data within the EU. Because data protection is an essential part of GDPR, it has had a significant impact on the importance of protecting personal data, especially from a cyber security perspective.

Continuous Evaluation of Cyber Security

Higher security demands and structured security management are necessary to assure proper personal data protection. Each organization must continuously ensure systems that handle or store personal data. Since most IT environments are a network of computers, servers, etc., interconnected in different ways, organizations must ensure security throughout their entire IT environment.

Incident Reporting within 72 Hours

Compliance with GDPR demands significantly higher requirements on liability and accountability in the operations where breaches occur. Except for more strict regulations within cyber security management, organizations must also report a data breach within 72 hours from when the processor became aware of the breach.

Framework for Increased Security Audits

GDPR requires a combination of technology, processes, procedures, and people working together to guarantee personal data privacy. IT departments need to establish security strategies and use them as a framework to prevent, monitor, and manage any data breaches. This includes developing policies and procedures to train employees to handle data correctly.

- Establish processes and systems to identify possible signs of intrusions or security irregularities and notify and report these instances.
- Implement preventive security systems such as firewalls and IDS (Intrusion Detection System).
- Monitor users with administrator privileges to detect discrepancies or deviant behaviors.
- Establish security policies that facilitate continuous monitoring of activities to detect irregularities or unauthorized access to personal data.
- Otherwise, ensure that your organization has sufficient protection for the organization's network against threats such as unauthorized intrusion, removal, and sharing, as well as copying and attempting to copy information.

Example

A hacker gains access to a database with sensitive data by hacking a web application. The hacker proceeds to extract personal data, such as names and email addresses. This personal data breach must be reported by the breached organization within 72 hours and could result in them receiving a hefty fine. Violations like this can lead to financial damage and damaged reputation and trust.

Facts about GDPR

- GDPR (General Data Protection Regulation) is an EU-homogeneous regulation.
- It has been implemented as a local law in each EU member state and replaced any previous local laws.
- It was launched across the EU on May 25th, 2018.
- The legislation aims to create coherence around the management of personal data within the EU and increase security.
- In the case of a personal data breach, the controller shall, without delay no later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority.
- Penalties for non-compliance are either up to €10 million, or 2% annual global turnover – whichever is higher or up to €20 million, or 4% annual global turnover – whichever is higher. The fines are based on the specific articles of the regulation that has been breached.

Financial Fines

British Airways

€22,4^{m}

Lack of security led to hackers stealing information from about 400,000 customers.

Mariotte

€20,4^{m}

Lack of security led hackers to steal 339 million customers' data. Thirty-one million were EU residents.

Capio St. Göran

€3,2^{m}

The hospital's information system was not adequately secured and ignored the principle of minimum access, which gave users full access to all patient data, including sensitive information.

The Seven Principles of GDPR

Lawfulness, Fairness, and Transparency

You may only process personal data if you meet the requirements of the law.

Integrity and Confidentiality

Personal information must be stored securely, not altered or stolen.

Data Minimisation

You may only collect the information that is necessary to fulfill the purpose.

Accuracy

If you have personal information, you must keep it correct and up to date.

Storage Limitation

Data should not be kept longer than needed and should be deleted.

Purpose Limitation

You may only collect personal data for a specified purpose.

Accountability

You must be able to prove that you meet all these requirements.

Why Holm Security?

Leading Attack Vector Coverage

The broadest coverage of attack vectors in the industry which includes both technical and human attack vectors.

More Than Just Another Vendor

Your most important partner within cyber security heping you stay one step ahead of cybercriminals.

Data Privacy

Any vulnerability data we collect is stored and encrypted in data-neutral locations so you can be assured that only you will have access to your data.

How can we help?

Want to get in touch? We'd love you hear from you. Here's how you can reach us.

☎ +46 8-550 05 581

✉ info@holmsecurity.com

www.holmsecurity.com

HOLM SECURITY