nuvias

Guide to Cyber Security Compliance with GDPR

Security

V1.3

General Data Protection Regulation – GDPR Overview

What is GDPR?

- An EU regulation coming into force in May 2018
- Which means it applies to all EU member states at a National Level without modification

What is the aim of GDPR?

- The aim is to increase the privacy for EU citizens in regards to their personal data.
- To give regulators broader powers over data protection of EU individuals

Who does it apply to?

- EU companies and entities that deal with personal data of EU residents
- Non-EU companies that deal with the EU resident's personal data irrespective of where the equipment is hosted.
- Businesses with any information that can be used to directly or indirectly identify a natural person - Including customer and staff data.

What are the costs?

- Data breach must be disclosed 72 hours after the company becomes aware
- Breach penalties include fines of up to 4% of the company's annual revenue or;
- 20 million euros depending on which of the two is greater

What are the rare possible reliefs?

- In the event of a data breach leniency may be possible in situations where
  - Data that is hashed or obscured or encrypted so that it cannot be used to identify the individual – pseudonymous data where loss may cause harm to the individual
  - Appropriate and necessary steps (including security systems) were place to protect data

Policy - Prevent - Respond & Report

As a minimum, it is a good idea to consider a strategy for GDPR compliance in the following three broad Security Technology Areas:

A. Incident Policy Guidelines

B. Incident Prevention

C. Incident Response & Reporting

A. Incident Policy Guidelines

Security and Compliance Policy Document

If you currently do not have a policy in place that can quickly be put into effect in the event of a security breach, it is strongly recommended that you implement one. If you already have a policy, you will likely need to review it to comply with GDPR.

So what should be included in your policy:

- Procedures for incident handling
- Who to contact and when to comply with GDPR
- A Risk Impact Matrix to get quick visibility on a breach

Data Protection Officer (in-house or outsourced)

GDPR requires you to assign a Data Protection Officer (DPO) under certain circumstances if you are a particular type of organisation. The officer will be responsible for the structure of data protection and the governance of how it's used as well as being the foremost point of contact. Even though not every type of organisation is obliged to appoint a DPO under GDPR, they may consider it as a worthwhile appointment none the less.

B. Incident Prevention

Perimeter Protection with Threat Prevention and Advanced Sandboxing

Your perimeter is like the castle walls that surround the all-important keep. It should have the very best defences you can deploy. This is where your security software and hardware should be actively judging everything coming in for signs of malicious intent. Techniques such as sandboxing to ask questions of a potentially malicious file should be deployed to minimise the threat to your network.

IdAM – Identity and Access Management

Identity and access management enables the right individuals to access the right resources at the right times and for the right reasons. Identifying what goes on in your network is a key factor in protecting data and GDPR compliance.

Encryption for Data at Rest

Encryption is a very effective way of securing your sensitive data from attackers. Full disk encryption ensures that even if a breach occurred, anything they stole would be unreadable and would therefore protect you from any GDPR backlash.

Vulnerability Management

The software and firmware you use could have vulnerabilities that can be exploited to give an attacker access to sensitive areas of your network. Protect vulnerabilities beyond your control with Vulnerability scanning and management solutions.

Encryption of Data in Motion

The process of obtaining personal data should also be highly secure. Secure web pages and spaces where a customer is expected to give personal data should be secure with HTTP with data transfer protected by Transport Layer Security (HTTPS). This ensure that data on the move from the web page to your secure network is encrypted and secure.

Patch Management

Latest patch updates, and can push patches from console. Missing updates. Alerts, emails. – Main ways to get breached avoid with vulnerability management to avoid data lose.

Password Management / 2-Factor Authentication

The traditional username and password method of accessing an endpoint is out of date. Implementing multi factor authentication will go a long way to securing one of the most vulnerable parts of your network, the end points.

Endpoint Security

Endpoint security is a main stay in any basic network security portfolio. It's an effective line of defence on an endpoint and has been used for years as an essential tool for blocking any malicious attacks.

Data Loss Prevention

Prevent your sensitive data being passed into unwanted hands, either with malicious intent, or by accident. Data loss software can help you keep track of your GDPR compliance by monitoring where data is going within your network and potentially stepping in to stop it from going somewhere unauthorised.

Staff Cyber Security Awareness Training

If you were to suffer a breach, it's very likely to come as a result of a phishing attack at an endpoint controlled by employees. Regular awareness training will minimise the risk of a successful phishing attack thanks to a more alert and responsive employee.

C. Incident Response & Reporting

What do you do if you suffer a breach incident?

Threat Hunting

Threat Hunting

Is the process of analysing a network to provide actionable information on potential and actual advanced threats. Threats can come from external malicious players or an insider.

It combines manual methods combined with automated systems involving the use of User and Entity Behaviour Analytics (UEBA), Anomaly Detection, Forensics, Threat Emulation and Machine Learning.

Incident Response security specialists, Security Intelligence / SIEM systems, Threat Detection and UEBA systems all contribute to this effort.

Threat Remediation

Attacks that have been identified should be remediated.
This involves removing the current threat such as malware and putting measures in place like patching software, restricting account privileges and updating security configurations to stop similar or new attacks.

GDPR notification compliance

When and who do you notify in the event of a data breach?

The ICO classifies a personal data breach as: a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

If you suspect that a breach has occurred within your network. You will need to do the following:

You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If this is confirmed, you will need to notify the relevant supervisory authority within 72 hours of finding out that your data has been compromised.

The notification should include: The nature of the personal data breach including the categories and approximate number of individuals concerned; and the categories and approximate number of personal data records concerned. A description of the likely consequences of the personal data breach; and A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects. You will also need to give the contact details of your appointed data protection officer.

Data Backup

It is important to keep damage to your day to day business environment to a minimum. If a breach occurs that leaves you with corrupted or deleted data, being able to revert to a back-up is essential to your business being able to immediately run as normal.

Not having effective back-ups could cripple a business which would mean losing vital information on their customers, processes, passwords, financial information, marketing databases and much more needed to successfully run a business.

Wick Hill / Nuvias can provide Technological recommendations in the following areas:

B. Incident Prevention

Barracuda provide Next Gen Firewall and Web Security solutions that protect the perimeter of your network.

Next Generation Threat Prevention, Firewalls and security management. Check Point have a comprehensive portfolio of products designed to protect networks prior to attack.

HID are a leading access management brand. Specialising in authenticating end points, devices and the cloud to ensure that only authorised people can access sensitive data.

Kaspersky are a leading Endpoint Security provider. Solutions built from decades of experience include advanced features such as System Watcher and Data Encryption.

Leaders in Security Awareness Training and anti-phishing awareness. KnowBe4 work with world renowned hacker Kevin Mitnick to create effective corporate training programmes.

Malwarebytes take a multi layered approach security with their comprehensive Anti-Malware, Endpoint Security and Breach remediation solutions.

Tenable transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context with their advanced monitoring solutions.

VASCO is a global leader in trusted security with two-factor authentication, transaction data signing, document e-signature and identity management solutions designed for all businesses.

WatchGuard specialise in Unified Threat Management Next Gen Firewall and Secure wireless solutions for businesses of all sizes. Consitently recognised as a Leader by Gartner.

C. Incident Response & Reporting

Barracuda provide leading back up security solutions that enable you to return your network to its normal secure state if an incident occurs.

The Check Point Incident Response Service is a dedicated service that will help you mitigate a network breach through careful planning and response execution from a team of highly trained experts.

The Dtex Advanced User Behavior Intelligence Platform combines technology, intelligence and services to provide cutting-edge protection from user threats.

FileFacets specialise in online privacy compliance and enterprise analytics. Enabling organisations to perform sophisticated data discovery and advanced content searches of networks, servers, desktops and laptops.

Malwarebytes Endpoint Protection protects against exploits, malware, fileless attacks, and ransomware with seven unique technology layers.

According to the Information Commissioner's Office (ICO), these are the 12 initial steps you should be taking now in order to be ready for GDPR compliancy.

1. Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely

2. Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit. to have.

3. Communicating Privacy Information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation

4. Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5. Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6. Legal basis for processing personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

7. Consent

You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

8. Children

You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

9. Data Breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10. Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11. Data Protection Officers

You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

12. International

If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

Learn More...

Visit www.nuvias.com/GDPR

For plenty more resources on GDPR from our vendors.
Or to get in touch to dicuss how we can help you.

Data protection and cyber security has never been more important.
GDPR is arriving shortly – don't get caught out.

01483 227 600 | www.nuvias.com/cybersecurity | cybersecurity@nuvias.com

Nuvias Cyber Security, River Court, Albert Drive,

Woking, Surrey, GU21 5RP

nuvias | CYBER SECURITY
formerly Wick Hill