GDPR

General Data Protection Regulations

THE ROAD TO **GDPR** COMPLIANCE

This whitepaper introduces the **General Data Protection Regulations (GDPR)** which come into force on **May 25, 2018**, including key concepts such as Privacy by Design and Individuals' Rights. It also provides a roadmap of what organisations need to do to become compliant with the legislation and avoid data breaches, including how **Netsparker** can help organisations achieve compliance.

February 2018

Dawn Baird and **Robert Abela**

netsparker

What is GDPR?

The European Union (EU) General Data Protection Regulations come into force on May 25, 2018. After this, there will be one EU supervisory authority, rather than a separate one for each member state.

This whitepaper introduces the General Data Protection Regulations (GDPR) and outlines what organisations need to do in order to become compliant.

Table of Content

What is Personal Data?

GDPR focuses on privacy, which means it is all about how businesses (Data Controllers) should ask for, retain, manage and use personal data. So before we dig into how to be GDPR compliance we need to understand what is Personal Data.

Personal Data (PD) refers to any information relating to an identified or identifiable natural person (the 'data subject'). It includes anything which might enable the identification of an individual, beyond the usual and obvious identifiers, such as name, date of birth and address. This new definition is broader than before, and includes genetic and biometric data for example.

Who Needs to Comply with the GDPR Regulations?

There are two ways to answer the question: by thinking of Organisation Type or Organization Location.

Organization Types

GDPR applies to any organization (all public and some private sector) that collects, processes, stores, analyzes, or shares the Personal Data of EU residents and customers.

Organization Locations

GDPR applies to everyone who does business in or with the EU, even if they are not located there, including the UK (regardless of Brexit). EU organisation will be forced to consider the risk of transferring data to non-EU countries and international processors who might not be compliant.

Key Concepts in GDPR

These are the key data protection principles that set out the main responsibilities for organizations.

Privacy by Design (PbD)

PbD means that all processes must be designed with privacy and data protection built in from the start ('data protection by default'), rather than as an afterthought.

Organizations must take measures to protect their own data. For example, they can conduct data protection impact assessments (DPIAs), ensuring technical safeguards, and make staff aware of their legal obligations.

Organizations also have an obligation to design their process for external privacy. For example, they should publish Privacy Notices (PNs), practice data minimisation and deletion, and provide users with privacy options.

Consent

The GDPR insists that consent for the collection and use of all Personal Data must be clearly given by the customer. Consent may not be assumed and must be easy to withdraw.

Organizations should only collect the information they require and have specific customer authorization for, and must discard it when it is no longer needed.

Individuals' Rights

The GDPR collates and strengthens the rights for all those whose Personal Data is collected, as explained below:

Right to Data Portability

Individuals have the right to request and receive a copy of all data they have previously provided to an organization.

Right to Erasure ('Right to be Forgotten')

Organizations must ensure that they can delete data when requested.

Right to Rectification

Organizations must ensure that they can update, correct and complete data when requested.

Right to Restrict Processing

And organizations must ensure that they can stop processing Personal Data when requested, if they believe it is inaccurate or objectionable for example.

GDPR Fines and Liabilities in the Event of Non-Compliance

If an organization or business is not compliant, the EU has the right to penalize them with fines of up to €20 million or 4% of a company's annual, global turnover, depending on whichever sum is greater. An organization's Data Protection Officer (DPO) will bear legal and professional responsibility for data protection compliance.

The Road to GDPR Compliance

This section sets out what organisations must do in order to become GDPR compliant.

Determine Where Personal Data is Stored

Once organizations are clear about the scope of Personal Data, they need to document the nature and use of all the data they possess.

Conduct an Information Audit

As well as the date and description of each piece of data, an audit addresses the following:

- Where do we store this data?
- What is the source of this data?
- How do we protect this data?
- How long do we keep this data?
- What is our reason for holding this data?
- Who has access to this data?
- Who has rights over this data?
- How often is the data used?

An audit also includes an organization's current procedures and policies on data.

Who Do You Share Personal Data With?

Organisations also need clarity on with whom they share Personal Data – where does Personal Data go after it leaves the organisation?

Map Out Data Flows

Organisations need to map their data and information flows in order to assess their privacy risks and find unintended data uses. A data flow is any transfer of information from one location to another; for example, from inside to outside the EU, or from suppliers to customers.

A data flow must identify and map out all data items, storage formats, transfer methods, and storage locations as part of the information lifecycle, and identify who is accountable.

Finally, an organization needs to draw up a plan on how they will implement the right technical and procedural safeguards, as well as determining their legal and regulatory obligations.

Raise GDPR Awareness and Train Staff

All decision makers and key staff need to be made aware of changes in the law, impact on their organization, potential compliance problems, timescales to compliance, new processes and resource implications.

Add GDPR to Policy Documentation

Organizations can either add GDPR principles to their existing policies, or create a new standalone policy to deal with it.

With GDPR, organizations will also have to tell people the lawful basis for processing their data, data retention periods, and that individuals have a right to complain to the Information Commissioner's Office (ICO) if they think there is a problem with the way their data is handled.

Write a Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is required in situations where data processing is likely to result in high risk to the rights and freedoms of individuals.

A DPIA could contain information on information flows throughout and around an organization. The ICO has a Code of Practice for conducting such assessments.

Assign a Data Protection Officer

Public authorities and organizations that monitor individuals on a large scale, organizations that process data on criminal convictions, and companies that process Personal Data as one of their core activities have a further requirement, to assign a Data Protection Officer (DPO).

For further information on the DPO, see Controller and processor (Section 4).

Outside the EU? Appoint a Representative Within the EU

The GDPR requires that those organizations outside the EU designate, in writing, a representative within the EU.

Avoid Data Breaches

A data breach is any accidental or deliberate negative impact on Personal Data resulting in: unlawful destruction, loss or corruption, alteration, unauthorized access, unauthorized disclosure or unauthorized transfer.

In addition to a negative outcome for the person to which the data belongs, organisations can be fined or taken to court. Here are two ways to avoid data breaches.

Process Data Securely

Due to the GDPR's principle of Privacy by Design, organizations have an obligation to be proactive in their security measures (technical and organizational). This includes 'a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of data' (see Security of Processing 1d).

Take Necessary Steps to Prevent Security Breaches

The year of mega data breaches was 2016, when year a huge number of world-renowned businesses, such as LinkedIn and Yahoo, suffered data breaches. We analyzed the most notorious data breaches of 2016 and found out that:

- Nearly three billion records were leaked during 2016
- The major cause of data leaks were web application hacks

To avoid getting hacked, and experiencing a data breach similar to the cases mentioned above, you need to ensure that all the software you use is up to date, implement and use proper protective technical measures (such as firewalls, IDS and IPS) and most importantly of all, ensure that your web applications are not vulnerable to malicious hack attacks.

How Netsparker Can Help You Ensure Your Systems Are Secure by Default

Many organisations are keen to get ahead of the GDPR legislation by writing and implementing policies now, making changes to how they collect and process data, training staff and informing customers.

Here is how Netsparker can help IT departments, security researchers and development teams to actually implement the practical requirements of the legislation:

- Privacy by Design can be achieved in your web applications that process the majority of your data, by adopting our approach to web security. We recommend that web application creators and vendors set up scheduled, automated vulnerability testing using Netsparker, ensuring it is integrated into their Software Development Life Cycle and DevOps processes. This helps you Prevent Security Breaches.
- Don't stop at the finished product! Once you've build a secure system or web application, schedule automated vulnerability testing against web applications using the web security industry benchmarks such as OWASP Top 10.
- Scan your web applications and APIs each time your developers add features and other changes.
- Many organisations focus, rightly, on the spectre of a catastrophic loss of data (Data Breaches and Notification). But they forget the other side: customers have the right to be able to access their data too (Individuals' Rights). Denial of Service attacks will breach almost every individual part of the legislation on Individuals' Rights. Vendors must eliminate these types of vulnerabilities.
- Save time on all this extra effort by: integrating Netsparker with an Issue Tracking System to enable vulnerabilities that are identified during a web application security scan to be automatically created as issues; integrate Netsparker with other useful tools, such as Jenkins which enables you to automate scans and export reports; and finally, remember that Netsparker's unique Proof-Based Vulnerability Scanning Technology means zero reported false positives, further saving you time on working toward data protection compliance!

Request an Audit

Once you reach the end of the tunnel on the road to GDPR compliance, request an audit. The data protection supervisory authority in your country can help you to understand and meet the regulations. And some even carry out their own audits, which can save you a lot of money.

In Case of a Data Breach

Organisations that neglect to put in place the recommendations we summarised above, and who consequently suffer data breaches, have further responsibilities. If the worst happens, you must:

- First, quickly establish whether, in fact, a Personal Data breach has occurred
- Promptly take steps to address it
- Notify your country's enforcement authorities
- Notify the subject(s) of the data breach, who have the right to be informed by Data Controllers within 72 hours of discovering any higher breach which presents a risk to consumer privacy

Local authorities may enforce fines for such breaches. Further, individuals have the right to claim for compensation for material damages arising from such data breaches and other non-adherence to the legislation. They can also assign not-for-profit bodies to claim on their behalf, which could lead to class actions.

The consequences of a Data Breach are both serious and severe. We have explained above how integrating the Netsparker web application security solution into your SDLC can help you get ahead of the GDPR legislation. Let us help you to build secure web applications and web APIs to ensure that risks of Data Breaches are minimal and security is maximal.

How can Netsparker Help You?

Learn how Netsparker web application security scanner can help your business become and remain GDPR compliant.

Resources & Further Reading

GDPR Regulation (EU)
https://gdpr-info.eu/

GDPR Portal
https://www.eugdpr.org/

ICO Guide to the General Data Protection Regulation (GDPR)
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/