GDPR Guide

All the details you need to know in one concise Guide
What Is GDPR?

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive (DPD) 95/46/EC and was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organisations across the region approach data privacy.

Retrieved from http://www.eugdpr.org/

**GDPR will come into effect 25th May 2018**

**GDPR addresses many of the DPD weaknesses including:**
- Updating requirements for documenting IT procedures
- Performing risk assessments
- Notifying the consumer and authorities of a breach
- Reinforcing the rules for data minimization

**GDPR covers all personal identifiable information (PII):**
- Name
- Address
- Phone Number
- Email Address
- Date of Birth
- IP Address
- Credit Card Numbers
- Medical Records
- Personal History Data
- Government ID Data

Secure GDPR Data in 5 Steps

1. Establish project scope
2. Scan for all sensitive data
3. Secure all data found
4. Systematic Monitoring
5. Regular Reporting
GDPR KEY CHANGES

INCREASED TERRITORIAL SCOPE
The most significant change to data privacy is the extended jurisdiction of GDPR. Previously territorial scope of the directive was unclear. GDPR makes it very clear, the legislation will apply to all organisations holding data belonging to EU citizens regardless of where the organisation is located.

DATA PROTECTION OFFICERS
Under the new regulations, any business that markets goods or services to customers within the EU and collects personal data for any purposes, must appoint a Data Protection Officer (DPO). The role of the DPO is to ensure the organisation is compliant under the legislation including implementing the specific retention periods for personal data and monitoring all departments to protect private customer data.

PRIVACY BY DESIGN
Privacy by design is not a new concept, but was not specifically outlined. Under GDPR, it will become a legal requirement. Privacy by design requires the inclusion of data protection resources from the initial design stage of a system. This requires controllers to hold and process only data crucial to the completion of its duties.
GDPR KEY CHANGES

THE RIGHT TO BE FORGOTTEN
The Right to be Forgotten entitles any private consumer to request the erasure of their personal data at any stage. This piece of legislation has been in effect under current ruling, however it currently does not cover data published on the web. GDPR rectifies this, and has been expanded to cover all data types.

RIGHT TO ACCESS
Under GDPR, the owner of the data has the right to obtain record of their personal information, including where it is being stored, and for what purpose. A copy of the record should be provided to the individual in electronic format and free of charge. Transparency, accessibility and empowerment are key elements under the new legislation.

BREACH NOTIFICATION
The new regulations provide explicit instructions in the eventuality of a data breach. Companies will have 72 hours to notify authorities where personal data has been compromised. Companies will also be required to notify customers at the first discovery of the breach. Failure to do either will result in hefty fines, and potential legal action.
GDPR NON-COMPLIANCE – WHAT ARE THE RISKS?

The most significant fine imposed under GDPR will be 4% of global revenue or €20 million (whichever is greater). This is reserved for companies found to have failed to implement basic security measures.

The second largest fine is 2% of global revenue or €10 million (whichever is greater), to be handed down to any organisation who fails to notify the relevant authorities as well as the individuals affected after a breach has been detected. An undefined strategy for breach notification could be a very expensive mistake for an organisation under the new legislation.

A harder cost to quantify but still substantial and potentially detrimental for an organisation is the irreparable damage a breach can cause to a brand.
GDPR responsibility needs to be companywide. Sensitive data can span across all departments within an organisation including Marketing, HR, Sales etc. It is the responsibility of the organisation to build a team in order to manage and ensure GDPR regulations are enforced from the top down in all departments.

Employees often present the highest risk to an organisation concerning data breach: 30% of all security failings come from within, often unintentionally. For this reason, GDPR requires companies appoint a Data Protection Officer (DPO). The DPO in most cases can be a current member of staff, but depending on the size of an organisation, a new hire or consultant may be required.
GDPR states that any company regardless of whether they have a physical presence within the EU, who collect data about EU citizens through a website or any other means must adhere to all requirements of GDPR.

For example if a company headquartered in the US, has EU customers or collects data from EU citizens, GDPR legislation and fines associated with non-compliance apply. The location of the server is not applicable. If the server is located outside the EU but the data belongs to an EU citizen, fines under GDPR will apply.

In summary the new regulations will extend beyond the boundaries of the EU including the US and a post Brexit UK. If you are doing business within the EU zone or hold data belonging to EU Citizens, GDPR must be adhered to.
5 NEXT STEPS –
HOW DO I BECOME GDPR READY?

**DETECTION**
Find and Secure all sensitive data within your organisation. Every server, workstation, file, document, email inbox, and cloud software must be included in this audit.

**AWARENESS**
Make sure the entire organisation knows about GDPR, what it covers, and the fines associated for non-compliance.

**EXECUTION**
Designate a team within the organisation to execute the GDPR strategy. Appoint a DPO to lead the team, and ensure all elements of the ruling are adhered to. This is not a once off implementation, GDPR must become part of the daily business process.

**IN SUMMARY**
It is vital that your organisation is aware of where the sensitive data is stored, who in the organisation is accessing it and how to secure it. Including these elements in your business practise now will ensure your organisation is GDPR ready.
The assessment will provide your organisation with a snap shot of all sensitive data being held within the environment we scan. The assessment will help you identify and understand the potential GDPR risks to your organisation.

Upon completion of the assessment we will provide you with a detailed risk report including practical solutions for your organisation to become GDPR compliant.
ABOUT GROUND LABS

Ground Labs is a data security software company dedicated to making data discovery and remediation tools to help organisations prevent sensitive data loss.

Our flagship product, Enterprise Recon, has helped thousands of organisations globally to discover sensitive data hidden in servers, workstations, documents, databases, emails, log files, cloud platforms and many other locations.

Enterprise Recon is a complete solution designed for the Identification, Remediation, and Monitoring of Sensitive Data. It is designed to be compliant with international data protection laws GDPR, PCI & PII.