

# GDPR

## The EU General Data Protection Regulation

Internal Report

by Michael Barber

February 2018

# Overview

---

The General Data Protection Regulation (GDPR) is the European Union's new legislation to protect the personal data of its citizens.

Organisations have been given a two-year lead-in period to become compliant, and **this ends on 25<sup>th</sup> May 2018**. The directive was approved by the EU Parliament on 14 April 2016. After the enforcement date, organizations in non-compliance may face heavy fines.

The GDPR supersedes the UK Data Protection Act 1998. This legislation is significant and wide-reaching in scope; the new laws expand the rights of individuals to control how their personal information is collected and processed. It places a range of **new obligations on organisations to make them more accountable** for data protection.

The new regulation demands that organisations **demonstrate compliance** with the data protection principles. This involves taking a risk-based approach to data protection, ensuring appropriate policies and procedures are in place to deal with the transparency, accountability, and the provision of individuals' rights, as well as building a workplace culture of data privacy and security.

Whether this new legislation is repealed after Brexit, or a UK document takes its place, this nevertheless must be acted upon before the compliance date of 25<sup>th</sup> May 2018. Additionally, even if the legislation is repealed for UK citizens, compliance will still be necessary when dealing with data belonging to EU citizens.

As IBM's [web site](#) puts it: GDPR "seeks to create a harmonised data protection law framework across the EU and aims to give citizens back the control of their personal data, whilst imposing strict rules on those hosting and 'processing' this data."

TermSet ([www.termset.com](http://www.termset.com)) have produced software, called ScanR, which can check files on a network and report on the level of compliance with the principles.

The following page provides a screen example:

Name	GDPRMatch	GDPRData	GDPRScore
Banking	True	[PERSON:John Smith][SORT CODE: 54-81-15][BANK ACCOUNT: 412341234][BANK ACCOUNT: 012345678][CREDIT CARD: 4234123412341234]	80
Car	True	[PERSON:Terry Turnbull][PERSON:Worcester Council][ORGANIZATION:Worcester Council][LOCATION:UK]	70
Clean	False		0
Credit Card	True	[CREDIT CARD: 5111222233334444]	10
Eg ser etter Ingrid Johansson	True	[PERSON:Ingrid Johansson]	50
HR Doc Word 97	True	[PERSON:Bill Gates][HR: Employee written warning]	51
InvoiceTIFF	True	[PERSON:John][CREDIT CARD: 1123456783456782]	60
IT Data	True	[IPADDRESS: 127.0.0.1][IPADDRESS: 192.168.1.1]	2
Jeg heter Vegard Johansen	True	[PERSON:Jeg][PERSON:Vegar][PERSON:Johansen]	50
Norway ID Sample	True	[PERSON:Jane Smith][NORWAYIDNUMBER: 15027112390]	85
PII	True	[PERSON:John Smith][ETHNICITY: asian][SEXUAL ORIENTATION: heterosexual][UKNATIONALINUSRANCENUMBER: jg103759a]	65
Postcodes	True	[PERSON:Lisa Clarke][PERSON:Peter Simpson][UKPOSTCODE: wr14 1na][UKPOSTCODE: cv32 1pq]	60
sampledoc	True	[PERSON:John Clarke][LOCATION:Malvern][LOCATION:Worcester][SORT CODE: 54-22-11][SORT CODE: 22-11-33][BANK ACCOUNT: 123456789][UK GOVERNMENT SECURITY TERM: Top Secret][UKNATIONALINUSRANCENUMBER: rk715021b][UKDRIVINGLICENCE: clark715021ba9yc]	94

## TERMS ET

This screen shows example output where the GDPR score gives the amount in percentage terms of each file that contains data that is GDPR-sensitive, and therefore must comply with the rules! The higher the score, the more alert the organisation must be to the need to check for compliance.

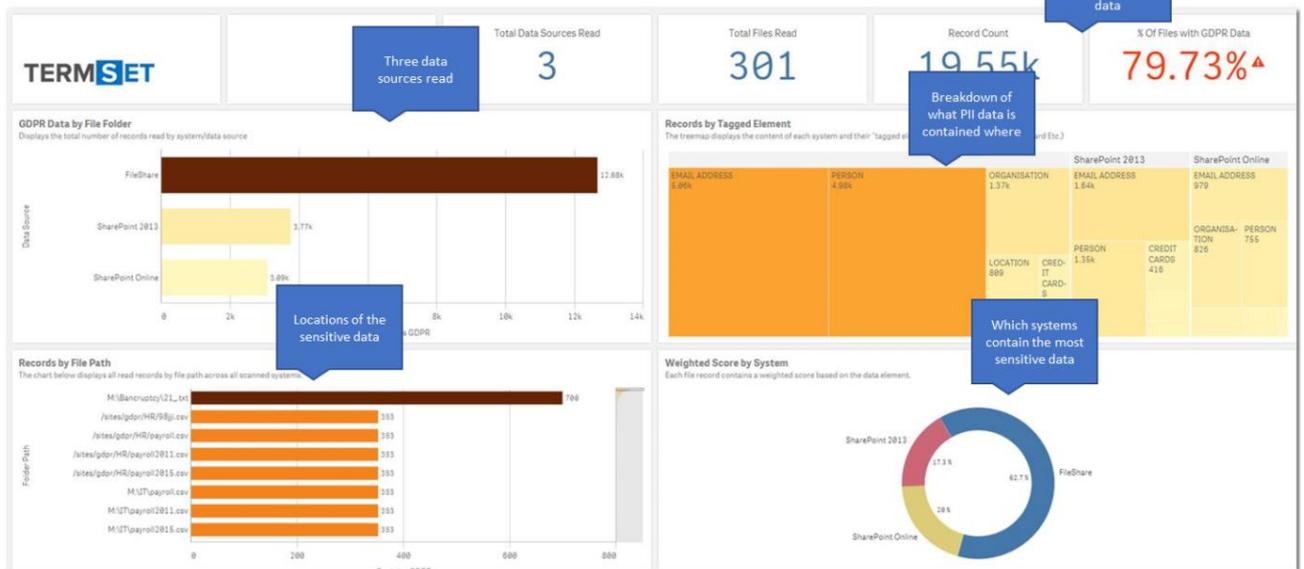
If this software is too pricey (costs for (1) small companies = £2,999, (2) medium companies = £7,999, (3) large companies = £14,999), then a *manual* search would need to be made of any possible GDPR data that would force checks on whether changes to the handling of that data are required.

## Scanning Files for Compliance

All databases, proprietary customer systems, SharePoint data, standard CRMs, and so on, need to comply with the security recommendations of the GDPR.

Using TermSet's ScanR, a comprehensive 'dashboard' is shown giving information that helps in isolating GDPR data:

## Overview Dashboard



Whatever method is used in planning for GDPR compliance, organisations need to be able to answer the following questions confidently:

- Are you aware of all the locations where your data is stored?
- Are you currently using data encryption for your files, especially when emailing or copying files to other people or to other locations?
- Do you have procedures in place when employees print, copy, or move GDPR data?
- Are you currently protected against Ransomware?
- Has your business trained employees on cyber-attacks and cyber-threats?
- Do you currently have mobile device management (e.g. how is data managed when employees with laptops are using them outside of the office)?
- Do you have solutions in place for Data Loss Prevention?
- Do you currently have a Disaster Recovery solution in place?
- Do you have intelligent reporting tools in place (see notes later on 'Qlik')?
- Does your business currently have any workflow automation solutions in place?
- Is your data categorised and appropriately secured based on content?
- Do you use cloud-based file sharing applications, e.g. OneDrive or Dropbox?
- Do you have solutions in place to allow email encryption as appropriate?

The GDPR covers the scope of the former Data Protection Act; however, note these additional areas that are covered:

- Economic information.
- Cultural details.
- Mental health information.
- 'Pseudonymised' data (for example, social media usernames or other online personas) - providing it can be easily identified.

Generally, if a person can be identified from the information about them stored in retrieval systems (name, telephone number, address, IP address, etc), then it can be classed as GDPR-sensitive data.

*"The GDPR requires you to show how you comply with the principles – for example by documenting the decisions you take about a processing activity."*  
(GDPR Principles, Information Commissioner's Office)

Article 30 of the regulation declares that organisations with fewer than 250 employees will not be bound by GDPR; however, if the processing carried out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as defined in GDPR Article 9, or personal data relating to criminal convictions and offences referred to in Article 10, then companies could still be liable to prosecution.

Article 9 states that "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited." There follows a long list of exceptions to this rule, including the explicit consent of the person, "reasons of substantial public interest," and "professional secrecy under Union or Member State law."

Article 10 states: "Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority."

Also, note the following general points in particular:

- Fines of £17.5m or 4% of global turnover, whichever is higher can be imposed.
- Organisations are required to notify a data breach within 72 hours.

- Organisations must understand key principles such as a person's right to be forgotten/removed and the handling of any information requests.
- Access Request response time has decreased from 40 days to 30 days. Therefore, action needs to be taken promptly on receipt of such requests.
- Organisations need to establish a clear legal basis for holding and processing personal data.

## Methodology for Compliance Assurance

---

---

A P Systems provides full services in connection with GDPR to support their customers in their compliance endeavours.

Here is a summary of the services provided:

- File encryption can be imposed for any data that is GDPR flagged, and reduces the risk of a Data Breach.
- Anti-virus must be in place.
- A Firewall (software or hardware) can be installed to reduce the risk of a Data Breach.
- Any device that is using this data, such as a workstation or laptop, can be configured to use data encryption and an active anti-virus system.
- Procedures for the handling of data off-site, for example with laptops, needs to be checked and enforced.
- A reporting tool such as Qlik (which can be tested for free: <https://www.qlik.com>) can be installed on request for data access monitoring. This tool is described as a "data visualisation and discovery tool."

## Web References

---

- <https://www.privacy-regulation.eu/en/index.htm>
- [https://www.hpe.com/uk/en/solutions/infrastructure-security.html?pp=false&jumpid=ps\\_hvdxg24ey7\\_aid-510379705&gclid=CK661frjtkCFUZGGwodw5wEgg&gclsrc=ds](https://www.hpe.com/uk/en/solutions/infrastructure-security.html?pp=false&jumpid=ps_hvdxg24ey7_aid-510379705&gclid=CK661frjtkCFUZGGwodw5wEgg&gclsrc=ds)
- [https://en.wikipedia.org/wiki/General\\_Data\\_Protection\\_Regulation](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation)
- <https://www.ibm.com/analytics/us/en/technology/general-data-protection-regulation/>