A P SYSTEMS
Complete IT Solutions

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 25th 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.

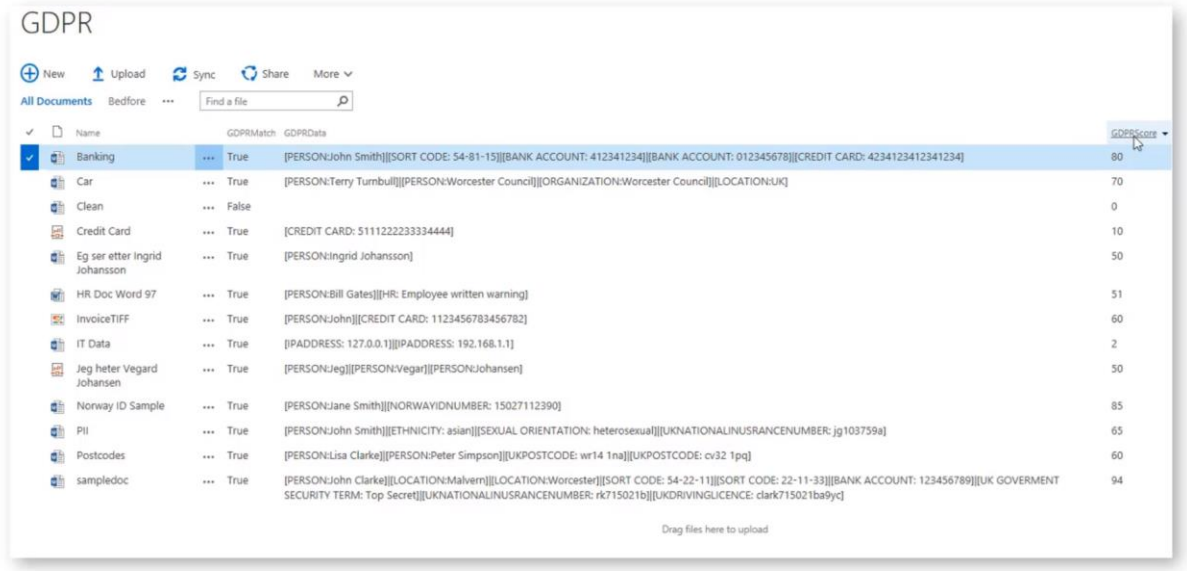
The new regulation demands that organisations demonstrate compliance with the data protection principles. This involves taking a risk-based approach to data protection, ensuring appropriate policies and procedures are in place to deal with the transparency, accountability, and the provision of individuals' 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Whether this new legislation is repealed after Brexit, or a UK document takes its place, this nevertheless must be acted upon before the compliance date of 25th May 2018.

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) 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:



TERMSET

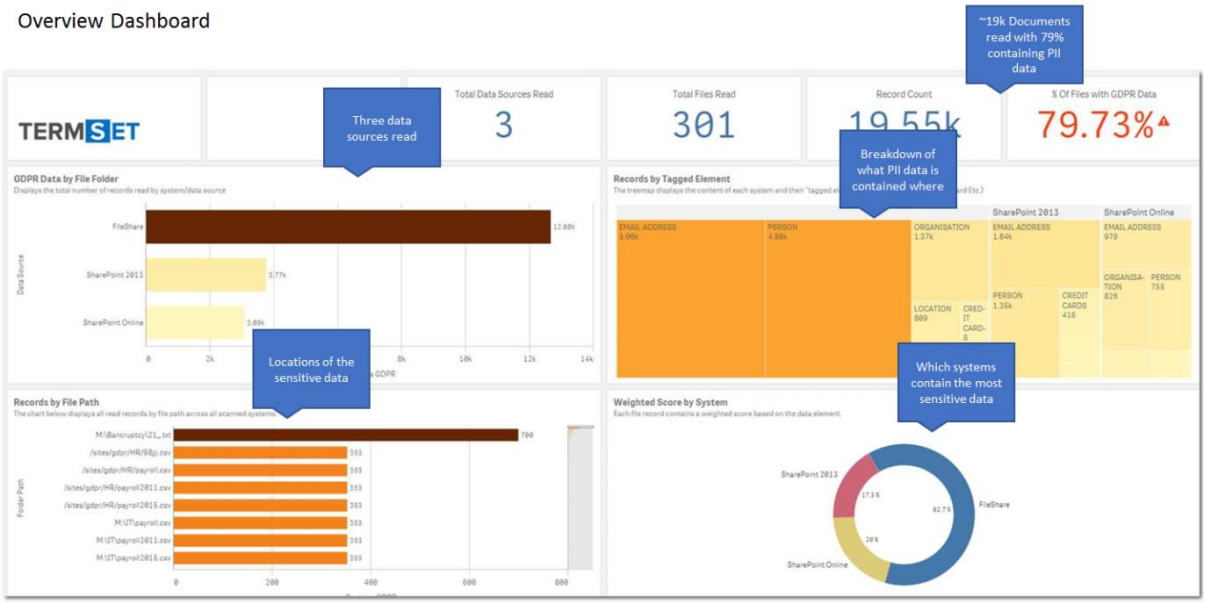
This screen shows example output where the GDPR score gives the amount in percentage terms of each file that contains data that is GDPR-sensitive, and therefore must comply with the rules! The higher the score, the more alert the organisation must be to the need to check for compliance.

If this software is too pricey (currently price is unknown), 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 and encryption recommendations of the GDPR.

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



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?
- Are you currently using device (not just data) encryption for laptops/tablets?
- 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?

Also, note the following 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 provide full services in connection with GDPR to support their customers in their compliance endeavours.

Here is a summary of the services provided:

- File encryption needs to be imposed for any data that is GDPR flagged.
- Anti-virus must be in place.
- Any device that is using this data, such as a workstation or laptop, must also use full encryption and have 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

- Main source: 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=CK661frfjtkCFUZGGwodw5wEgg&gclsrc=ds
- https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
- https://www.ibm.com/analytics/us/en/technology/general-data-protection-regulation/