Best practice

Preparing for the EU GDPR

The implications for your file sharing strategy and how to handle them.

Workshare®
Change matters

What's inside

If you need to know:

The GDPR timeline

On 25 January 2012, it was announced that new data protection legislation would be introduced across the European Union (EU), known as General Data Protection Regulation or GDPR. In April 2016, the details of the regulation were formally approved by the EU, paving the way for its implementation.

The legislation was shaped to replace woefully outdated law implemented in 1995, at the start of the digital era. It was said this harmonization of data protection regulation with all member states would make it easier to work across and with the EU, as there would only be one set of rules to understand and operate within. With implementation creeping closer, the idea of the GDPR being "easy" to handle feels debatable for many business services firms and their IT teams.

The regulation is now scheduled to become applicable from 25 May, 2018, and businesses are on a journey of discovery about what it means for them and, more importantly, how they will manage it. The crucial factor is that organizations that "control" and "process" the data of EU residents – whether the company itself is based in the EU or not – will have to be able to detect a data breach and report against it in a timely way.

Effectively, businesses will have to ensure they can detect breaches of data protection regulation and report on them within 24hrs. Practically speaking, most organizations are in no position to do this currently; however, it will soon become an absolute necessity to bridge this gap in defenses.

In this paper, we discuss:

- Who exactly is impacted by the GDPR?
- What the implications are for business services firms?
- The difference between detecting a breach of data vs. protecting data

Also included is a data protection / risk detection checklist to help with preparation and compliance with the GDPR.

Who is impacted by the GDPR?

The EU GDPR applies to any business or organization – no matter where it is located – that controls or processes personal data related to a resident of the European Union. Previous data protection laws placed the onus of responsibility on the controller of the data. One of the biggest changes with the GDPR is the expansion of scope to now include processors, as explained by Fieldfisher's international technology and internet lawyer, Mark Webber:

"The GDPR will expand the scope of application of EU data protection law...to include data "controllers" (i.e. persons who determine why and how personal data are processed), [and] certain requirements will apply for the first time directly to data "processors" (i.e. persons who process personal data on behalf of a data controller)."[1]

This brings into play a whole new world of vendors, providers and business services firms previously cushioned from responsibility, but who routinely handle personal and potentially sensitive information on behalf of their clients.

"It's important to note that the GDPR is a companywide issue for businesses, not just an IT project. It will affect contracts, procurement and many other departments, but it's something that will need to be facilitated by IT," says Tim Hyman, a GDPR specialist consultant.

To be compliant with the regulation, each business will need to appoint a named Data Protection Officer to assume responsibility for supporting those controlling and/or processing data. The DPO will be the one personally accountable for reporting any data breaches to the relevant authority. Wherever they actually reside within a firm, the DPO will obviously be heavily reliant on IT colleagues to help identify and detect a breach. Right now, however, the majority of firms would struggle to support this requirement, largely because the tools to monitor and audit activity relating to sensitive or personal data aren't present. This calls for a swift and necessary change in current procedures.

"A low percentage of business services organizations, including law firms, have fully understood the implications of the GDPR for a number of reasons. They have experts that understand the law, who have been monitoring progress of the GDPR for years, but few have actually taken steps to implement change, meaning there haven't been advanced preparations. Firms view all types of data as 'data' and they haven't yet started thinking about how to separate out what's personal and sensitive vs. the rest." Hyman adds.

> ***Firms view all types of data as 'data' and they haven't yet started thinking about how to separate out what's personal and sensitive vs. the rest.***

Implications of the GDPR for business services firms

Considering the GDPR is specifically designed to focus on protecting personally identifiable and therefore the potentially sensitive data of each individual resident in the EU, the implications of the new law are daunting to say the least. In terms of the serious personal data violations investigated by the UK's Information Commissioners Office (ICO), in the second quarter of 2016 alone they "Received 545 new cases – approximately a 22% increase on the number of cases received in the previous quarter (448).[2]" The global potential for data breaches related to EU residents is enormous.

Large percentages of employees in professional services firms "process" personal data every day as a matter of course. In many firms the handling of sensitive data is restricted to a few departments, e.g. HR and Finance, not so for the likes of law firms or public and private medical practices. Whether for consulting and advising clients, or dealing with different forms of transaction, matters naturally involve peoples' personally identifiable information. This makes detecting risks a large and difficult issue to target.

With the number of cases being investigated by official bodies in their hundreds each quarter in one country alone, when extrapolated, the consequences are obvious for businesses globally, and they are also potentially costly. Those dealing with personal and sensitive information as part of the currency of their work will have to find a means of strict control when exchanging or sharing data necessary for their job. For those who fail to do so, there will be a sliding scale of fines, with as much as 4% of annual global revenues at stake, not to mention valuable reputations.

Darren Saunders, Client Director at Trustmarque, says: "The impact of GDPR on the legal sector in particular is massive. Because of the sensitive and personal client data law firms manage on a daily basis, data security is more important than ever. Firms that fail to comply with GDPR could not only face huge financial penalties, but they could also suffer severe reputational damage if clients discovered their personal information was not managed in a compliant manner."

Technology can help, however Data Loss Prevention (DLP) solutions right now aren't sensitive enough to fully manage the dilemma. Many of the markers added to files by document management systems get confused about what is sensitive information and what's not. For example, credit card numbers can get confused for very normal unique identifying document IDs. This leads to too many false positives for a DPO to investigate in the course of their responsibilities. Many DLP tools can't be relied on to trigger the correct flags in a detection system in order to highlight risk and therefore properly handle it.

> *The impact of GDPR on the legal sector in particular is massive...*

Detecting a data breach vs. protecting data

There is a difference between data protection and being able to discover a data breach. This is one of the key elements of the regulation. For instance, could a law firm have as few data protection mechanisms in place as they wanted if they were always able to reliably detect a breach should one occur and then effectively report against it?

The obvious answer is no, however, the ideal solution lies somewhere in between.

Firms would be wise to complete a full analysis of where personal data is currently stored and processed within their organization and then introduce as many elements of data protection to those areas as feasible. Then, they can use flags on high-risk data or unusual activity with files, so they can be identified as possible breaches to be properly investigated and reported on.

While there are still many firms taking no measures to protect personal or proprietary information when sharing files, others are using software to prevent data loss, particularly via email. However, they are rarely doing the same for files shared via the browser and in the Cloud, therefore personally identifiable and sensitive information is still at risk in most firms, creating potential for data breaches, heavy fines and reputational damage.

Professional services firms also often ship large amounts of sensitive and personal content via removable media, such as USBs or CDs, for example post due diligence in an M&A transaction; in bibles or closing binders at the end of a deal; and in medical scans and images related to client matters. This creates huge scope for data loss that is completely undetectable once that media leaves the firm's front door.

Cyberattacks too are increasing each month and arguably pose a greater threat than physical security in a digital age. IT Governance reported the number of known leaked records at 289,526,590 in June 2016, accurate at the time of publication on 21 June 2016.[3] And, cyberattacks are just one way data loss can take place, there are also both accidental and malicious data protection breaches performed by employees across the world each day. A study by SC Magazine claimed "Internal employees account[ed] for 43% of data loss" events each year.[4]

Detecting unusual network activity can highlight where people are sharing content unusually, e.g. to other countries or domains outside their remit. It won't reveal what is inside a file being shared, e.g. a personal budgeting spreadsheet sent to a partner on holiday abroad, vs. a salary spreadsheet being sent to a competitor in the US.

13-point data protection and risk detection checklist

- ❑ Appoint a Data Protection Officer to take responsibility and control of data protection issues on behalf of your firm.
- ❑ Conduct further research on the exact responsibilities of your business and its partners as related to the regulation. Recommended is this video overview from Fieldfisher: https://www.youtube.com/watch?v=NxgZ57BTkFQ
- ❑ Complete a risk assessment on the systems used for processing and controlling data in your firm, and by any of your vendors or 3rd party providers.
- ❑ Identify the biggest areas of risk, for example there may be certain systems that don't have the same protection as others, but which hold sensitive personal information – these need to be tackled as a priority.
- ❑ Speak to experts and make use of advisory services, like those offered by Trustmarque in conjunction with Tim Hyman, to ensure you are fully meeting all GDPR requirements.
- ❑ Create an action plan, which lays out all the tasks that need to be completed prior to implementation of the GDPR in 2018.
- ❑ Investigate innovative and specialist technology in this space that can protect data, prevent data loss, or can support monitoring risk.
- ❑ Select a solution specifically designed to support business services firms, which can facilitate normal workflow, while preventing data loss and providing analytics to support detection of risk or unusual events.
- ❑ Use a data removal solution to strip files of sensitive metadata before they are uploaded to or shared in a browser, the cloud or via email.
- ❑ Implement a Secure File Transfer solution, rather than using USBs or CDs when sharing data, and give access to key parties, so there is no reason to use physical media. In many cases this will also save a huge amount of time and money.
- ❑ Perform an audit of all existing "at rest" data and ensure you know where potential risks are located, putting analytics in place against those you have identified.
- ❑ Identify a solution that can help assess the risk from content being shared and make sure files are only shared in correct and sanctioned locations, with flags on unsanctioned activity.
- ❑ Educate staff and end users on the risks of data sharing and particularly of embedded data objects within files being shared.

Summary

According to Tim Hyman, “Best practice would be to understand the systems currently in place and what type of data goes through them, i.e. firms should perform an impact assessment related to the GDPR. This will help identify exposure in terms of what data is on the systems, who has access to it, what the retention periods are and what risks would be associated with it.”

The 13-point checklist gives some practical steps towards preparation and compliance.

Those who get a head-start on preparation for the new regulations will inevitably gain a competitive advantage, as they will be seen as both more competent and trustworthy by clients looking for assurances.

Businesses entrusted with the most sensitive and confidential of information will need to demonstrate they are both aware of their responsibilities under the regulation and that they are making significant changes to their firm as a result.

> ***You have to assume that one day there will be a data breach in your firm, so you need to have prepared for it. One of the most important things at stake is a firm’s reputation, which makes any fines associated with the GDPR almost irrelevant.***
>
> Tim Hyman,
> Business Technology Consultant

Trustmarque & Workshare in Partnership

Workshare and Trustmarque have joined forces to offer secure, cloud-based document collaboration solutions to help UK organisations prepare for GDPR. Trustmarque's expertise, combined with the support from legal expert Tim Hyman, means that the partnership will allow Workshare's unique solutions to reach further than ever before.

With thanks to Tim Hyman

Tim Hyman is an independent Business Technology Consultant specializing in information security and GDPR technology compliance. He previously spent 20 years as an IT director at top 20 law firms, including Reed Smith, Olswang and Taylor Wessing, and has a broad base of management responsibilities. Delivering complex business solutions to improve service levels, while reducing cost and enhancing client experience through technology, Tim leads transformational change focused on strategic security planning, high caliber teams, improvement programs and best practices.

About Workshare

Workshare is dedicated to helping professionals compare, protect and share their high stakes documents. Since 1999, Workshare has developed and released intelligent technology for business services firms Now, more than two million professionals use Workshare around the world.

About Trustmarque

Trustmarque is a leading provider of end-to-end IT services to the UK public and private sectors; including cloud, professional and managed services, and software solutions. At Trustmarque we give honest, simple and independent advice that helps customers navigate an increasingly complex world of IT.

We simplify business, through a flexible and cost-effective approach that empowers organisations and their people. With over 27 years' experience at the heart of the rapidly evolving IT market, Trustmarque has established a position as a leading technology provider to high-profile clients from the private sector, UK government and healthcare organisations.

Trustmarque employs 600 people across six UK locations. Trustmarque is a CarbonNeutral® Company and is ISO certified in the disciplines of: Information Security, Service Management, Continuity and Data Recovery, Quality Management, Environmental Management, and Occupational Health and Safety. Technical and project management staff operate in line with ITIL, PRINCE2 and Agile industry standard.

For more information about Trustmarque visit www.trustmarque.com, call 0845 2101 500, or email info@trustmarque.com.

[1] http://privacylawblog.fieldfisher.com/2016/the-gdprs-impact-on-the-cloud-services-provider/
[2] https://ico.org.uk/action-weve-taken/data-security-incident-trends/
[3] https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-june-2016-135000000-records-leaked/
[4] http://www.scmagazine.com/external-hackers-and-internal-employees-pose-data-breach-threat/article/439510/