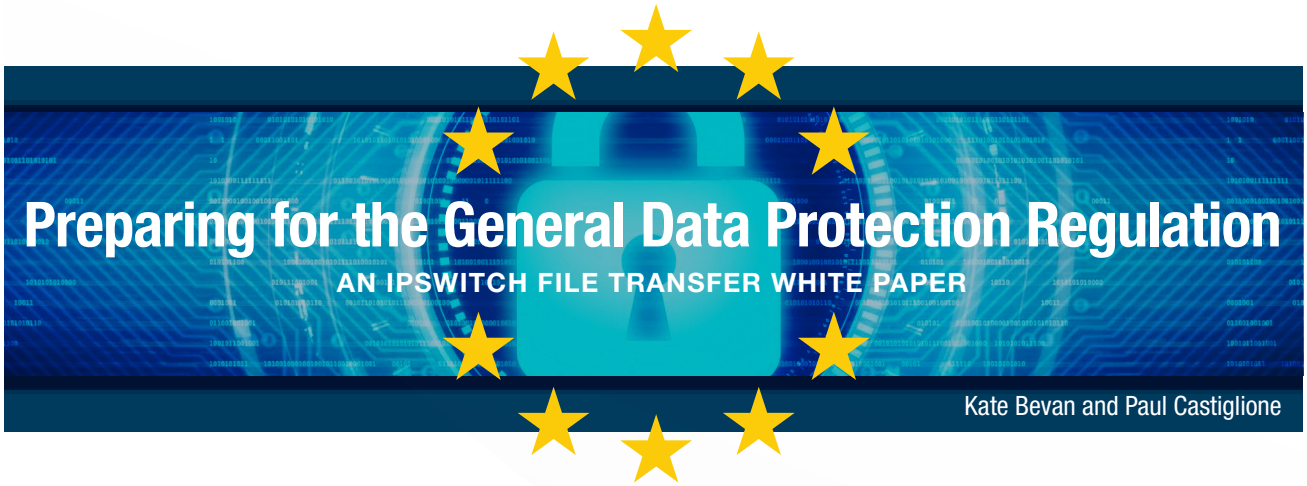
IPSWITCH
FILE TRANSFER



Preparing for the General Data Protection Regulation

AN IPSWITCH FILE TRANSFER WHITE PAPER

Kate Bevan and Paul Castiglione

Data protection laws across the EU are out of date and barely fit for purpose. Additionally, each member state has its own regime, creating a nightmare of compliance for businesses in the middle of the second decade of the 21st century

> Moving toward a risk based approach to identifying where sensitive data is must be your first activity."
>
> DAVID JUITT
> Chief Security Architect, Ipswitch

When existing data protection laws were drafted, security was a very different proposition. Data was held on in-house servers and rarely left the perimeter; security was therefore focused on protecting that perimeter.

Today's data landscape is very different: we collect more data than ever before, and rather than being kept within physical walls, it's held in the cloud, with documents, forms and databases distributed across servers and across borders. New technologies are constantly being introduced: a few years ago, the IT manager's concern was consumerisation, as users chose their own mobile phones and laptops, creating myriad security endpoints and risks. Now wearables are on the horizon, which further gather data that must be protected, and the Internet of Things provides a further host of devices communicating with back ends and generating yet more data.

"Moving toward a risk based approach to identifying where sensitive data is must be your first activity." comments David Juitt, Chief Security Architect at Ipswitch.

Keeping on top of rapidly changing technology is one challenge – keeping on top of regulation and compliance issues is a whole other challenge for IT professionals.

One key change is on the horizon: the creation of a new data protection framework for the whole of the European Union. This seeks to create a harmonised regulation that is fit for purpose in today's fast-moving IT, data and compliance landscape. Yet despite the fact that the proposed new rules are probably just over two years away from being implemented, IT professionals are worryingly unprepared for the change.

Keeping on top of data protection rules is a burden on business, say two thirds of the IT professionals, and nearly a fifth have no idea if the forthcoming changes will apply to them.

So what exactly is the GDPR? What are the key changes? What are the pain points? And what do businesses need to do to prepare for the new regulations?

What is the GDPR?

The EU's General Data Protection Regulation is designed to replace the patchwork of data protection regulatory authorities in the 28 member states with a regime that will apply across the Union.

Additionally, it will apply to any non-EU businesses that handle the data of EU citizens in Union. This means that the biggest cloud and social media companies such as Google, Facebook, Twitter, Microsoft, Apple, will be required to comply with the regulations.

The first draft of the regulation was published by the European Commission in 2012. Since then the proposals have been grinding through the legislative process and was finally adopted by the Council of Ministers in June.

This means that the next stage of negotiations can now begin to resolve some of the differences between the European Parliament and the Council of Ministers. It is hoped that a final agreement will be reached by the end of this year.

That will then usher in the two-year period before which the GDPR comes into force, meaning it should – in theory – be applicable across the 28 member states by the end of 2017.

What Are the Key Points of the GDPR?

Consent

One big change for any business that handles personal data is that it will have to seek clear consent from customers, staff and suppliers for use of their data.

That applies both to data gathered after the implementation of the regulation and – crucially – data that's already held.

PAIN POINT: All existing data will have to be audited to make sure it complies with the new standard. This could mean that every person your organisation holds data on will have to be contacted to upgrade their existing consent. And every consent will have to be available to the Information Commissioners Office for inspection on request. This will mean a huge auditing and compliance exercise.

Disclosure

The current draft of the regulation requires any organisation suffering a breach to notify it within 72 hours to the Data Protection Authority and anyone affected by a breach.

PAIN POINT: One sobering example of the potential impact of this requirement is the Ashley Madison breach: in July, hackers claimed to have stolen the customer database of the website that facilitates extra-marital hook-ups. In August, the hackers released that database online: it contained the details of some 30 million users.

Although Ashley Madison is an American business, many of their users are EU citizens, and as such Ashley Madison would, under the GDPR, have been required to notify the DPA and the users within 72 hours of the breach being discovered.

Penalties

There is some good news on this for businesses: the original proposal was for penalties for a breach to be up to 5 per cent of global turnover, or up to €100m. That has been watered down and the current proposal is for fines of up to €1m or 2 per cent of global turnover, depending on the seriousness of the breach.

PAIN POINT: Under the current regime in the UK, fines have been a maximum of £500,000, which might not seem much to a business turning over millions or even billions of pounds or euros. The UK's Carphone Warehouse, which in August had 90,000 credit card details stolen in a hack, might not feel a fine of that level, but the fine of £200,000 levied on British Pregnancy Advisory Service in 2014 after thousands of people's details were stolen by a hacker was a much bigger financial blow.
One key finding by the UK Deputy Commissioner and Director of Data Protection was that the BPAS was not aware of what information it was holding, nor that that data was not sufficiently secure.

Businesses affected by the GDPR will have to take steps ahead of its implementation to ensure that they know what information they're holding – a huge auditing and compliance exercise.

IPSWITCH
FILE TRANSFER

Right to be Forgotten

Businesses handling the data of EU citizens will have to erase data "without undue delay" if the individual asks them to do so, if the data was unlawfully processed or if they're required to do so by law. There are some caveats to that – freedom of expression and information and the public interest or scientific and historical archiving requirements may trump the right to be forgotten.

> "We've always taken the threat of data breach as a real possibility, but now with the new regulation we want to be able to measure how prepared we are."

PAIN POINT: With so much data held in the cloud and moving through enterprise, partner and customer networks, it is much harder for organisations to implement systems that will enable them to identify and erase personally identifiable information on request. Businesses will have to implement processes for responding to "right to be forgotten" requests in a timely fashion.

Are Businesses Ready for the GDPR?

The answer is – not really. Ipswitch's survey of more than 300 IT professionals from the UK, France and Germany found that 56 per cent could not accurately say what "GDPR" means, and 52 per cent said they were not ready. A further 64 per cent had no idea when the regulations are due to come into effect, while 35 per cent said they didn't know if their existing IT policies and processes were up to the job of complying with the new regulations. Just 12 per cent said they were ready for the change.

In the UK, that picture is even starker: just 5 per cent of IT professionals say they are ready for the GDPR.

The good news is that there is still some time to prepare: there will be a two-year period between the GDPR being ratified and it coming into force. The best guess for it taking effect is around the end of 2017.

"We've always taken the threat of data breach as a real possibility, but now with the new regulation we want to be able to measure how prepared we are."

What Needs to be done?

There are four different file transfer scenarios, and, when you consider managed file transfer, you should be looking for a single solution that can support all of them.There two areas that businesses need to focus on ahead of the implementation of the GDPR: technology and training, with 69 per cent of those surveyed saying they would need to invest in new technologies or services.

The key technologies businesses said they needed to invest in were encryption, analytics and reporting, perimeter security, file sharing and mobile device management, with encryption being mentioned by the most (62 per cent).

The other important area is training: here, businesses are more aware of the need to prepare, with around half saying they had allocated training budget and resource to help staff understand and comply with the GDPR. However, around a third had not yet allocated either budget or resource, and worryingly, nearly a fifth did not know if the money and resources were available for training.

Leadership from the Top

Getting ready for the GDPR is a priority for businesses all over the EU, and the wide impact of the changes mean that the drive for auditing, preparation, new processes and compliance must come from the top: this is a responsibility for the C-suite, and demands strong leadership so that new policies and processes can be implemented effectively.

The GDPR will impact many areas of every business that handles data, from data protection to file transfer.

What Should IT Professionals be Doing?

Even from a glance at some of the key points of the GDPR, it quickly becomes clear that the new rules are very wide-ranging, and that there is no one-size-fits-all roadmap for businesses preparing for GDPR.

"Every employee in my organization need to be aware of the GDPR. Instituting a security education process may be the critical element that keeps us off the front page."

However, there is one key strategy that should be the starting point for any business preparing for GDPR, and that is risk management. Mandated from the C-suite, a risk management process that identifies all the critical processes and assets and evaluates their vulnerabilities and potential threats to them sets the priorities for the next stage of the process towards compliance with the GDPR.

When the UK's existing Data Protection Act came in to force, the cloud and cross-border transfers of digital assets and data barely existed: security was predicated on creating a secure perimeter to protect the on-premises infrastructure.

Technology has moved on significantly since then, with a key challenge for CTOs and IT security professionals now being how to protect data held in the cloud, distributed among servers and across borders, and regularly moved between locations. Particularly sensitive assets that are routinely moved around via the internet include personal data, strategy documents, trade secrets, confidential bid documents and research assets and of course financial records.

A risk assessment should consider whether data is adequately encrypted and backed up, and if those back-ups are similarly properly protected and encrypted. Vulnerability to malware, the potential for human error or over-reliance on key staff are other areas to consider when looking at a business's risk profile.

Risk assessment covers all areas of the business, and should also consider technologies and strategies to mitigate the risks identified. One key technology for mitigating risk and ensuring compliance is managed file transfer, which will manage the entire process both within and outside the business.

Conclusion

Data breaches are common and damaging: the past year or so has seen high-profile incidents from eBay and Sony Pictures to Carphone Warehouse and Ashley Madison. Incidents like those, where personal data, sensitive company documents and other data have been stolen should be concentrating the minds not just of IT professionals, but of Chief Information Officers, Chief Technology Officers and indeed the entire C-suite. There are lessons to be learned from the mistakes of others.

"When I see businesses' names in the news because they've been hacked, I remember that we simply cannot be complacent. It wasn't us that was attacked this time, but it could be us another time. These big breaches encourage me to look again at our own processes and to keep on evaluating the risk we face." Comments David Juitt, Chief Security Architect at Ipswitch

Although the language and process of the European Union and its legislature might seem glacial and opaque, time is of the essence for businesses all over the EU. It's critical that organisations use the next two years to really get to know their own data landscape, to identify areas that need attention and to identify the technologies and service providers that can help them be ready for the day the new regime comes into force.

"Every employee in my organization need to be aware of the GDPR. Instituting a security education process may be the critical element that keeps us off the front page."

IPSWITCH
FILE TRANSFER

What Is Managed File Transfer?

Moving files and data is a key process in any business. Managed File Transfer is a middleware technology that streamlines those transfers and business processes, reinforces IT infrastructure, supports and improves compliance, improves agility and helps companies respond quickly to business challenges and opportunities.

Managed File Transfer is a key tool to mitigate risk. In environments from the informal, where there is no security policy, where file transfers are carried out manually and could be vulnerable to interception, failure or misdirection, to ones where policies and procedure are already in place, Managed File Transfer can reduce the burden on employees and enhance security and compliance across the business.

A comprehensive Managed File Transfer solution not only provides secure routes for assets, it also adds value with tools for the end users for tasks such as managing attachments and working in local folders. A Managed File Transfer solution also streamlines processes by automating workflows, managing performance and security, and providing reporting and analytics so that the business is always on top of data and documents as they move through, out of and back into the business.

Andrew Glencross, senior IT security specialist at NHS Wales Informatics Service, is responsible for providing operational security for all national applications and infrastructure covering every site across NHS Wales. He explained: “Using Ipswitch File Transfer’s MOVEit has given us a level of confidence that was perhaps missing in the past. We can now say with certainty that we have a secure solution in place which meets the needs of our internal teams and ensures compliance across the service and beyond.”

Ipswitch File Transfer provides solutions that move, govern and secure business information between employees, business partners and customers. The company’s proven solutions lead the industry in terms of ease of use, allowing companies of all sizes to take control of their sensitive and vital information and improve the speed of information flow. Ipswitch lets business and IT managers govern data transfers and file sharing with confidence and enable compliance by balancing the need for end user simplicity with the visibility and control required by IT. Ipswitch File Transfer solutions are trusted by thousands of organisations worldwide, including more than 90% of the Fortune 1000, government agencies, and millions of prosumers. For more information on Ipswitch File Transfer and its products, go to www.IpswitchFT.co.uk.