ipswitch

Secure. Control. Perform.

AN IPSWITCH EBOOK

Brexit and the GDPR: What IT Teams Need to Know

The EU's General Data Protection Regulation (or GDPR), which comes into effect in May of 2018, will force companies to change the way they handle personal data. The requirements to limit the use, limit the retention period and to provide copies and/or delete personal data on request far exceed the data protection requirements that most organisations are accustomed to. These requirements should be the topic of important discussions between departments like IT, marketing, finance, sales and senior management teams as they prepare for the advent of the GDPR.

According to a recent Dell survey, 80% of respondents knew 'little or nothing' about the GDPR, and that's not good to say the least. If your business collects, stores or processes the personal data of EU residents or citizens, you will need to comply with the GDPR. The potential consequences for breaches of GDPR requirements may well be material to your business and include fines and civil actions. This eBook discusses what GDPR means for businesses and how IT teams can prepare themselves for GDPR compliance in 2018. You will learn:

- If your business needs to comply with GDPR
- EU residents' rights under GDPR
- How US companies need to comply with GDPR
- How UK companies need to comply in wake of Brexit
- How every IT team need's to prepare for the GDPR

ipswitch

Does Your Business Need to Comply with GDPR?

If your company collects, stores or processes the personal data of EU residents or citizens, you will need to comply with GDPR. By the way, personal data is any data belonging to an individual through which they can be identified. This includes, but is not limited to, employee IDs, addresses and combinations of data which can be used to identify an individual. But what does that mean to IT teams? They need to think of all of the potential places that data is 'processed' and the security of those worklfows. By the way, processing includes the external transmission of data or data sharing between organisations. If your company transmits personal data to an outsourcer, you share the responsibility for the security and handling of those outsourced processes.

EU Residents Have Rights to Their Personal Data

GDPR mandates that EU residents and citizens have a right to ask that their data be deleted permanently from business databases. In addition, citizens have a right to receive a copy of every piece of data about themselves that an organisation may collect, process or store. To fulfill this requirement, it's critical to design your systems so that this data can be accessed, copied, corrected or deleted.

With GDPR, gone are the days of vague or misleading privacy policies hidden deep within websites. Under the GDPR it doesn't matter what type of privacy policy you have, consent in privacy policy agreements can never waive an EU resident's rights regarding their personal data. This is a huge step forward for data privacy advocates, but it causes a dilemma for businesses as, going forward, they will need to think long and hard about the implications of the GDPR.

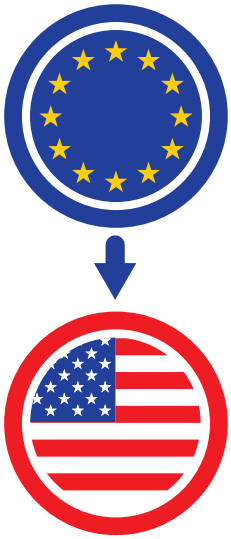
Opt in procedures and configuration settings will need to be re-designed in line with the requirement for explicit consent. The use of personal data for profiling, such as that used in targeted on-line advertising, may also need specific consent.

How US Companies are affected by the GDPR

There are still a lot of questions around how EU citizen complaints and requests for data copies or deletion will be handled by US companies. The concern with some is that an appointed US ombudsman doesn't go far enough. To say the least, the US government doesn't have the best record when it comes to data privacy.

In reality, efforts by the FBI and NSA to obtain EU citizen data via software back doors and forcing companies to hand over data is the biggest reason for the push by EU lawmakers for GDPR and the dissolution of the former Safe Harbour agreement.

For instance, if the NSA comes knocking on your door requesting data identifying EU citizens you will not be able to hand that data over due to GDPR. If you hand over data that is protected under GDPR, you are subject to fines of up to 4% of annual turnover. Further, affected residents and citizens of the EU will have adequate cause for civil action against your business. In the case of a security breach, the same risks apply.



The Implications of Brexit

Even with Brexit now a firm reality, there is no doubt that UK firms will have to comply with the GDPR. The date for withdrawal from the EU is later than the May 2018 date that the GDPR comes into effect. Thus, UK businesses will be under the jurisdiction of the EU and subject to the GDPR.

Ipswitch's survey into GDPR preparations revealed that more than three quarters of UK-based companies say that keeping up with data protection regulatory requirements will cost them financially. This would include investing in new tools and technologies, and also setting aside a training budget to help staff understand the new systems.

A ballpark percentage of UK exports to the EU is about 40%. In other words, businesses will have to find a way to continue to do business with the EU. And, even after Brexit is in effect, they will still need to collect, store and process data – personal and otherwise – concerning EU residents. UK businesses will need to make sure that data is adequately protected.

According to Emily Taylor, associate fellow in International Security at Chatham House, combining a new data transfer agreement like Safe Harbour with the Investigatory Powers Bill (Snoopers' Charter) could jeopardise data sharing between the EU and UK. It's worth noting that this view is not universal. A number of other pundits agree that a new deal would be required, but there are already precedents like those coming from Switzerland and Canada.

Any IT teams tempted to stall GDPR preparations until after Brexit should bear in mind that the GDPR is focused on protecting personal data belonging to EU residents, no matter where the company collecting, storing or processing that data resides. The compliance requirements will not go away and it is advisable to maintain momentum around preparations.

ipswitch

How can IT Teams Prepare for the GDPR?

1. Rethink Sign-Up Procedures

What should you do? Better question: What do you need to do? It's required that you get more explicit and clear consent. For instance, failing to un-tick a pre-ticked box wouldn't be considered explicit consent. This will influence how sign-up procedures and configuration settings are currently designed.

2. Profiling Users

Individuals can object against the use of personal data in the context of profiling, especially for the purposes of direct marketing. Tracking users on different systems requires you to get clear and unambiguous consent and describe every step: where, how and what data is stored.

3. The Right to Be Forgotten

If you have made personal data public, you need to inform others using this data in the case that its owner has requested the erasure of this data. For this reason, it's critical to design your system so that users can review data, request rectification or withdraw earlier given consent.

4. Data Portability

An individual who uses personal data with a service provider should have the ability to port this data to another service provider. The easiest way to do this? Probably to adapt commonly used standards (open standards) and have your services accessible via a well-designed API — one that may even allow downloads in a common format, like XML.

5. Redesign Systems with Privacy and Encryption by Design

The GDPR requires that data breaches be reported within 72 hours of discovery if the data has not been strongly encrypted. Keep in mind the reporting should include the nature of the breach, the contact point for the DPO (data protection officer) and measures to mitigate the effects of the breach itself.

Encryption (for storage and communication) of data and using privacy by design go hand in hand when (re)designing systems. Verifying whether everything has been properly implemented can be achieved with auditing processes. In the case you suffer from a breach, having the personal data encrypted or pseudonymised highly reduces the risk of harm for data subjects.

ipswitch

Compliance Means Having the Right Security Measures in Place

Whether private or public sector, when it comes to securing, storing and sharing confidential data, organisations must make sure they have the right policies and process in place. This includes using secure file transfer and data management technologies, security systems and most importantly, providing essential staff training across the board.

Stronger rights for individuals on how personal data is processed will require that many organisations consider the use of frameworks for data transfers outside the EU.

About Ipswitch

Ipswitch helps solve complex IT problems with simple solutions. The company's software is trusted by millions of people worldwide to transfer files between systems, business partners and customers; and to monitor networks, applications and servers. Ipswitch was founded in 1991 and is based in Lexington, Massachusetts with offices throughout the U.S., Europe and Asia.

For more information, visit **www.ipswitch.com.**

ipswitch

Download your 30-Day FREE TRIAL of Ipswitch MOVEit Transfer ›