VERDICT

How technology is being used to aid GDPR compliance

The General Data Protection Regulation (GDPR) comes into force today and is the biggest shakeup to data protection rules in decades, forcing companies to make significant changes to ensure GDPR compliance.

Organisations are faced with the daunting task of restructuring all of the personal data they possess in a way that can be easily erased, rectified and accessed—all while adhering to robust security standards. Failure to do so threatens maximum fines of €20m or 4% of global annual turnover, whichever is higher. For some of the world's largest companies, those fines could hypothetically run into the billions.

As well as providing extra data security to individuals, which been a subject of considerable attention in the wake of the Cambridge Analytica scandal, it is creating opportunities for technology companies to provide services that simplify and secure data management.

Technology may have created the need for GDPR, but many are seeing it as the solution.

Automated heavy lifting: AI-driven GDPR compliance

For larger companies, the volume of data involved with GDPR compliance is simply too large for human management, with many organisations spending "20-30% of their IT budget on compliance

audit reporting and preparation," according to Martyn Davies, director at Rocket Software.

One of the upshots of GDPR is that it is driving innovation in artificial intelligence to provide solutions that can tackle this problem. IBM, for example, has developed an automated system that uses a type of AI known as cognitive computing to scan data caches and index findings. It then automatically completes tasks such as user data requests, which is now permissible under the new legislation.

AI programmes can also save companies much of the heavy lifting by automating the discovery of sensitive data and risk analysis so that any gaps in compliance can be addressed.

Amit Walia, executive vice president and chief product officer at Informatica agrees, saying that "organisations must take a holistic and automated approach to governance and compliance to help maximise the potential opportunity."

GDPR makes direct reference to automation, stating that an individual has the right to know when and how it is being used to make decisions when processing their data.

However, according to Rainbird AI CEO Ben Taylor, there is quite a bit of misunderstanding around this "right to explanation".

"GDPR does not define how automated decisions should be made or what constitutes a satisfactory explanation," he said. "It simply compels companies to reveal how an algorithm works and the type of data it draws on to make determinations."

GDPR compliance through cybersecurity technology

Under GDPR organisations must ensure they have robust security in place and are required to report certain types of data breaches to the relevant supervisory authority within 72 hours. Article 32 calls for the encryption of personal data, which has created an opportunity for cybersecurity companies to capitalise on this legislation-driven demand.

"Encryption should be applied to all personal data within corporate systems and, even more so, to information stored and saved on media taken outside the business–such as USBs and portable hard drives," says Jon Fielding Managing Director EMEA of encrypted flash drive provider Apricorn.

To prevent organisations from holding onto data that they no longer need, Article 5 requires personal data to be stored for no longer than is necessary.

Companies are using technology tools such as Cloud B2B to stay ahead of this, which stores data in the cloud and gives them the ability to allocate dates for documents to be destroyed or reviewed.

Compliance with GDPR location and data sovereignty requirements

GDPR's data residency and sovereignty laws require data to remain in the country of record in order to protect their citizen's personal information. Cloud-based services—where data is stored in servers around the world and accessed via a network—has globalised what was once a very local process.

Under GDPR, problems can arise depending on where in the world it is stored and who is looking after it.

One way to meet data residency and compliance requirements is giving businesses the ability to assign a geographical storage zone for individual users' data. This is something that cloud content management platform Box recently launched with Multizone support, which allows customers to store data in a country of choice.

With regards to data sovereignty, it means that a file will always be sited in the country of record, regardless of the location an employee who is accessing it.

Speaking at the Box World Tour in London, Box CEO Aaron Levie said: "In the world of GDPR, in the world of cybersecurity, in the

world of increasing regulation, we have to not just keep information inside of our data centre of our company, but in fact we have to protect the flow of information. We have to know if the content leaving the enterprise has personally identifiable data inside of it."

While technology may provide a solution for managing data under the yoke of GDPR, for some it shouldn't be considered a silver bullet. Toby Bryans, Principal Consultant, Finance Practice at global technology consultancy DataArt says that company culture and business processes are more important for GDPR compliance.

"Get those right by understanding how you use data and ensuring your business and staff prioritise data privacy," he said. "Anyone who is selling a system that claims to solve all your GDPR woes is lying. In data protection generally, good IT only helps once you have a good culture and business processes. Without those you will always be in trouble."

Original article can be found here: https://www.verdict.co.uk/how-technology-is-being-used-to-aid-gdpr-compliance/