BIZCOMMUNITY

Implement GDPR or organisations risk losing business

For businesses around the world, including Africa, the implementation of the European Union's (EU) General Data Protection Regulation (GDPR) is particularly pertinent. This is because the GDPR applies not only to all states in the EU, but more especially to any companies that market goods or services to EU residents. Without GDPR-compliance, which was widely enforced on 25 May 2018, these organisations risk losing business opportunities.

© rawpixel via 123RF

According to David Warburton, senior systems engineer, F5 Networks, a cloud and security solutions provider represented locally by value-added distributor Networks Unlimited, the GDPR simply cannot be avoided.

Speaking during an EMEA webinar presentation, Addressing the Overlooked Aspects of GDPR, Warburton noted that F5 has certain ideas on how to start the compliance process and is also able to provide solutions that will assist.

“There is not only one thing for companies to do to become GDPR-compliant – it is very much a multi-disciplinary project involving functions across the business, from HR to legal to finance to IT, security and so on,” he said. “GDPR fundamentally tries to change the way that organisations think about personal data, and how it is treated. GDPR is as much about the people and processes as it is about the technology.”

Key considerations of the GDPR

Warburton noted that key considerations within the GDPR include the following:

- Reviewing/updating of consent options around data, both opt-in and opt-out.
  Data subject rights are key: this includes the ability to give users the option to be forgotten by any particular service.
- Breach notification should not necessarily be given to all customers or the public but must be given to the data protection authority as the first port of call.
- Any organisation with over 250 employees will need to maintain the records of processing. Records and processes are a very big part of GDPR. Your suppliers will need to be compliant and this should be contracted in.

Big data and IoT

Warburton pointed out that the increasing number of internet of things (IoT) connected devices may contain personal information such as an individual's name and address; GPS location history; health records including weight, height, pulse and heart rate; audio/video recordings; and access to the home and other networks.

"All this information is being collected and to make it useful, it's being made available on the web. And so we need to think about how this big data is used and processed, and how it impacts on GDPR compliance going forward."

Secure processing

The GDPR regulations observe that the controller and processor of data shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. "When it comes to security of processing, everything talks about risk," said Warburton, "and now 'state of the art' required by default refers to risk benefit analysis. So it's important here to keep an eye on costs, because as technology solutions costs go down, it may mean that a solution that had initially seemed prohibitive may become cost-justifiable compared to the risk involved in terms of data breaches in terms of some very personal information."

Privacy impact assessments

"A privacy impact assessment is a sub-set of a larger risk assessment," Warburton continued. "We need to identify and minimise the privacy risks of any new projects and policies that are put into place. This helps us to identify potential problems at an early stage to try and minimise them, allowing for a better and cheaper solution, in the long run, to produce better policies and increase the trust between ourselves and our customer base going forward."

Warburton summarised three key areas of importance in a privacy impact assessment, as follows: identify and minimise the privacy risks of new projects or policies; work with internal and external resources to minimise harm; and create better policies, reduce risk and increase trust. He says it's important to ask questions such as, "Are we collecting new information, or using information in a way that it wasn't used before? Are we using new technology, for example introducing biometrics into the workflow?"

The seven steps of a privacy impact assessment were outlined as follows:

1. Identify the need for a privacy impact assessment.
2. Describe the information flows.
3. Identify the privacy and related risks.
4. Ascertain and evaluate the privacy solutions.
5. Sign off and record the privacy impact assessment outcomes.
6. Integrate the outcomes in the project plan.
7. Consult with internal and external stakeholders as needed.

"Once you've recognised the need for a privacy impact assessment, it's important to identify the data flow. This includes tracking the archiving and destruction of the data at the end of the cycle – does this comply with GDPR requirements? All these things need to be considered together. If we look at the increase into the cloud, this too has an impact on the data cycle."

Warburton outlined privacy issues, risk to individuals, compliance risk and associated corporate risk while identifying the privacy and related risks of a privacy impact assessment. "What is the risk to the individual of the data breach – credit card information, reputation damage? The cost to the corporate, in the event of a breach, comes with risks such as reputational and brand damage and the costs of a clean-up."

In terms of integrating the privacy impact assessment, Warburton advised leveraging existing project and risk management frameworks such as Agile, PRINCE2, COBIT, Orange Book and ISO31000:2009 and ISO27005:2011, to name but a few. As regards risk assessment frameworks, he noted that this is a cyclical process.

"Choose a risk assessment framework that best fits your business," he advised, adding further that when carrying out a risk assessment overview, it is important to be able to measure your risk assessments, allowing you to show improvement and also for audit purposes.

Who owns the data – who owns the risk?

Warburton explained that information flow contained within the cloud can help organisations to increase their security posture depending on various factors, but he warns that, "You can never remove risk completely. You always own the risk, regardless of where that data is – it's your data and you own it. You can share the risk, which is what is happening in the cloud, but you have a shared responsibility model."

Solutions

Warburton mentioned the importance of access protection, saying that unauthorised access, affecting confidentiality and integrity of data, is caused by such causes as user password fatigue, lack of endpoint visibility, phishing attacks, malware and botnet disruption. Solutions to this include secure authentication, granular and context aware access, encryption, single sign on and endpoint detection and protection.

In terms of application protection, Warburton said that cyber attacks on vulnerable web apps affect confidentiality, integrity and availability. He suggested advanced web application firewalls (WAFs) as the solution here and says the chosen WAF should be cross-platform. As regards Distributed Denial of Service (DDoS) attacks, he recommended multi-layered, application aware DDoS mitigation.

Speaking on single cloud providers, he noted the risk of a lack of resilience, and that the catastrophic failure of such a cloud provider could risks data loss. "Multi-cloud architecture is preferable, deploying apps and data across multiple cloud providers in order to maintain constant application delivery and security policies, and offer automated failover and server/container scale out.

"Security of processing as per GDPR requirements also needs to include the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident."

Breach visibility and reporting

"Breach visibility and reporting is one of the most crucial points of the technical aspects of secure and safe processing of data," advised Warburton. "Organisations must report a breach within 72 hours and yet sometimes, encrypted traffic can limit visibility into a breach, acting as a double-edged sword. Having a solution that can centrally decrypt this traffic – namely, SSL orchestrating architecture – and then send it off to different security appliance will improve our visibility for both attack and genuine traffic but also lets us sort out the solution accordingly."

Conclusion

Simon McCullough, major channel account manager at F5 in South Africa, says, “As David Warburton points out, the GDPR legislation is pragmatic in terms of what it expects. Companies are required to consider the risks associated with their data, and have processes in place, including documentation. Company size is not a factor in whether you do or don’t comply – for example, a doctor could employ a staff of six and his practice could hold incredibly sensitive information, which absolutely requires him to be GDPR compliant. The concept of personal data protection is fascinating in its possibilities.”

Anton Jacobsz, managing director at Networks Unlimited, concludes, “The more the world’s population carries out activities online, the more important it becomes for individuals to have their data privacy. The key to GDPR is giving control of that privacy to the data subject – to the individual. The EU is trying to change the way that we think about protection of data – it shouldn’t be an after-thought, and we welcome the way that the EU is championing the importance of data privacy. The technological processes are challenging but most certainly doable with the correct partner.”