SECURONIX
Security Analytics. Delivered.

7 Things You Need To Know About GDPR

The General Data Protection Regulation (GDPR) is around the corner. Here is what you need to know before the compliance deadline.

1

Deadline is fast approaching!

GDPR is a result of the European Commission's effort to revamp how businesses protect data in order to make Europe ready for the digital age. The exercise took over 4 years and the compliance deadline looms in the very near future – May 25th, 2018. All countries that are members of the EU must have national laws for GDPR compliance by May 6th, 2018.

2

GDPR applies beyond the EU

GDPR applies not just to businesses in the European Union, but also to any business that has operations in the EU. If the business sells to customers within Europe, you will need to comply with the GDPR requirements.

3

What exactly is "personal data"?

GDPR defines what is considered "personal data", and this data must be secured (masked or otherwise obfuscated). GDPR states personal data not only includes include names, address, email & phone data, financial & health information but also biometric and computer-based information like IP/MAC addresses, fingerprints, genetic information in what is considered personal data.

4

New roles, DCO & DPO, are well defined

GDPR mandates accountability, and states that every organization must appoint a "Data Controller" and a "Data Processor". A controller is an entity which within the business, determines how personal data will be used and for what purpose. A processor is an entity which processes the personal data on behalf of the controller.

5

Defines breach notification requirements

A fundamental tenet of the Regulation is the consumer's right to know about certain events concerning their personal data. Businesses must inform people when their data has been breached, and the organization must also disclose any data breaches so abuse preventative measures can be taken right away. Consumers should also have easy access to their personal information collected, held and used by the business.

6

Consumers can request to "be forgotten"

GDPR defines consumer's "right to be forgotten" or "right to erasure" in much clearer terms. This means that people who want their personal information to be completely removed from a business' systems can request this removal. The business must oblige provided there is no grounds for them to continue to retain this personal information.

7

Significant fines for non-compliance

Fines for failure to comply with GDPR are significant and range from 20 million Euro or 4% of the company's annual revenues – whichever is greater. This fine could be levied for a single case of not removing someone's data from IT systems when requested. The burden of proof is on the business, and if you are unable to prove that the organization has indeed removed the data, the fine is a smaller but still hefty 10 million Euro or 2% or revenue.

With so much riding on your business' compliance on GDPR, you need to ensure that the IT and security teams are doing all that is needed to meet the compliance deadline. To learn how to execute on your GDPR compliance goals, listen to our webcast "5 Steps To GDPR Compliance".