

Asavie Moda: General Data Protection Regulation

Protect the user, protect the connection
and protect the device



A lot of IT departments have focused on protecting data within their organization, yet there are risks linked to employees using mobile devices to access sensitive customer or company data. The introduction of the General Data Protection Regulation (GDPR) mandates strict protection of personal data. GDPR protects the data of over 510 million people. Those covered include:

- European Union citizens residing anywhere in the world
- Anyone who resides in or visits any of the EU's 28 member countries

“By the end of 2018, more than 50 percent of companies affected by the GDPR will not be in full compliance with its requirements.”

Gartner Research

Many companies might assume that GDPR does not apply to them, however, this is not the case as an organization does not need a physical presence in the EU to fall within the Regulation's remit. Companies that fail to comply with GDPR face fines of up to €20 million (US equivalent \$23 million), or 4% of the worldwide annual revenue of the prior financial year, whichever is higher. Compliance is no longer a nice to have, it is a necessity.

With the maturity and diversity of mobile devices - smartphones, tablets, laptops, MiFis, and PCs - available today, employees expect to be able to access work systems and applications containing sensitive customer data, hosted on premise or in the cloud. In parallel there has been a growth in the number of cyberattack vectors threatening mobile devices and networks. This places ever greater pressure on organizational IT and OT teams to protect personal data and avoid the potential damage to brand value through failure to adhere to the GDPR regulations.

Asavie Moda helps businesses and their employees comply with GDPR by securing mobile devices and the data on those devices.

Network

We protect data on the mobile network against vulnerabilities before they can affect the device and compromise data. Our private network-based service protects all devices across cellular and Wi-Fi networks and reduces the attack surface for hackers. Asavie Moda stops malware before it can communicate with criminal servers. By making it a more secure environment to access and review private data, Asavie Moda offers businesses an important capability for mobile data protection as part their GDPR compliance strategy.

Data

We protect confidential and personal data on corporate devices by enforcing the application of usage policies for individuals and groups. We minimize the danger of malware or zero-day attacks by blocking malicious and unclassified domains. This ability to secure data through the entire lifecycle as it transits the network is a key enabler for GDPR compliance.

Device

Asavie Moda physically protects the device with Password enforcement, Locate, Lock and Wipe functionalities on mobile devices like smartphones, tablets, laptops, routers and MiFis. This capability ensures that sensitive personal data is not compromised in the event of a lost or stolen device. As per GDPR, organizations that experience a data breach of personal data will have to notify data authorities within just 72 hours after discovery. It is crucial therefore to be able to act immediately since both accidental and unlawful breaches are equally penalizable.

Insight

Visibility of your mobile data traffic is a key contributor to GDPR compliance. Asavie Moda helps you understand what sites your employees are accessing so you can adjust and modify their usage policy dynamically to block malicious websites. By categorizing web content into trusted and untrusted domains we can automatically prevent accidental breaches by unintentional user behaviour. This provides a safer internet experience and denies hackers the opportunity to exploit vulnerabilities to steal personal data. Ultimately these insights enable organizations to manage their employees' mobile experience and reduce the potential for data breaches.

Protect the connectivity

Block malicious content at source across both Cellular and Wi-Fi traffic.

Protect the data

Apply policies that help your mobile workforce adhere to industry regulations and company policies.

Protect the device

Secure devices with password protection, and remote lock and wipe.

