ZIMPERIUM

GDPR & Mobile Devices

The Facts About Mobile Security & Compliance

Fact #1: GDPR has included mobile since it took effect in 2018

By now, anyone who conducts business within the European Union should be familiar with GDPR. The legal framework sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). Every country that does business in the EU must conform to GDPR standards.

What may not be as widely known is that GDPR requirements apply to mobile devices. In fact, just three weeks after the regulation took effect on May 25, 2018, one leading computer publication was calling attention to GDPR's applicability to mobile devices--and to the fact that most companies were overlooking mobile completely.

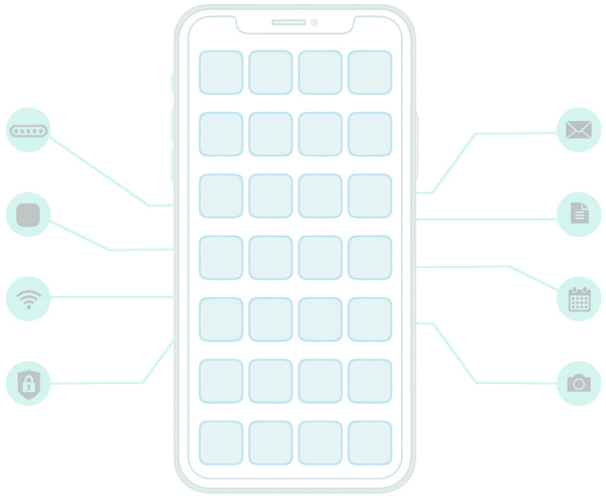
Research showed that most companies could not say with certainty what data their employees had on mobile devices. That lack of visibility into the data on mobile devices (both company-owned and employee-owned), combined with a lack of governance and protection for those devices, constitutes *"a direct challenge to GDPR compliance."*

In other words, if your GDPR compliance measures do not yet include mobile devices, you are out of compliance.

Fact #2: Mobile devices are 60% of GDPR-covered endpoints

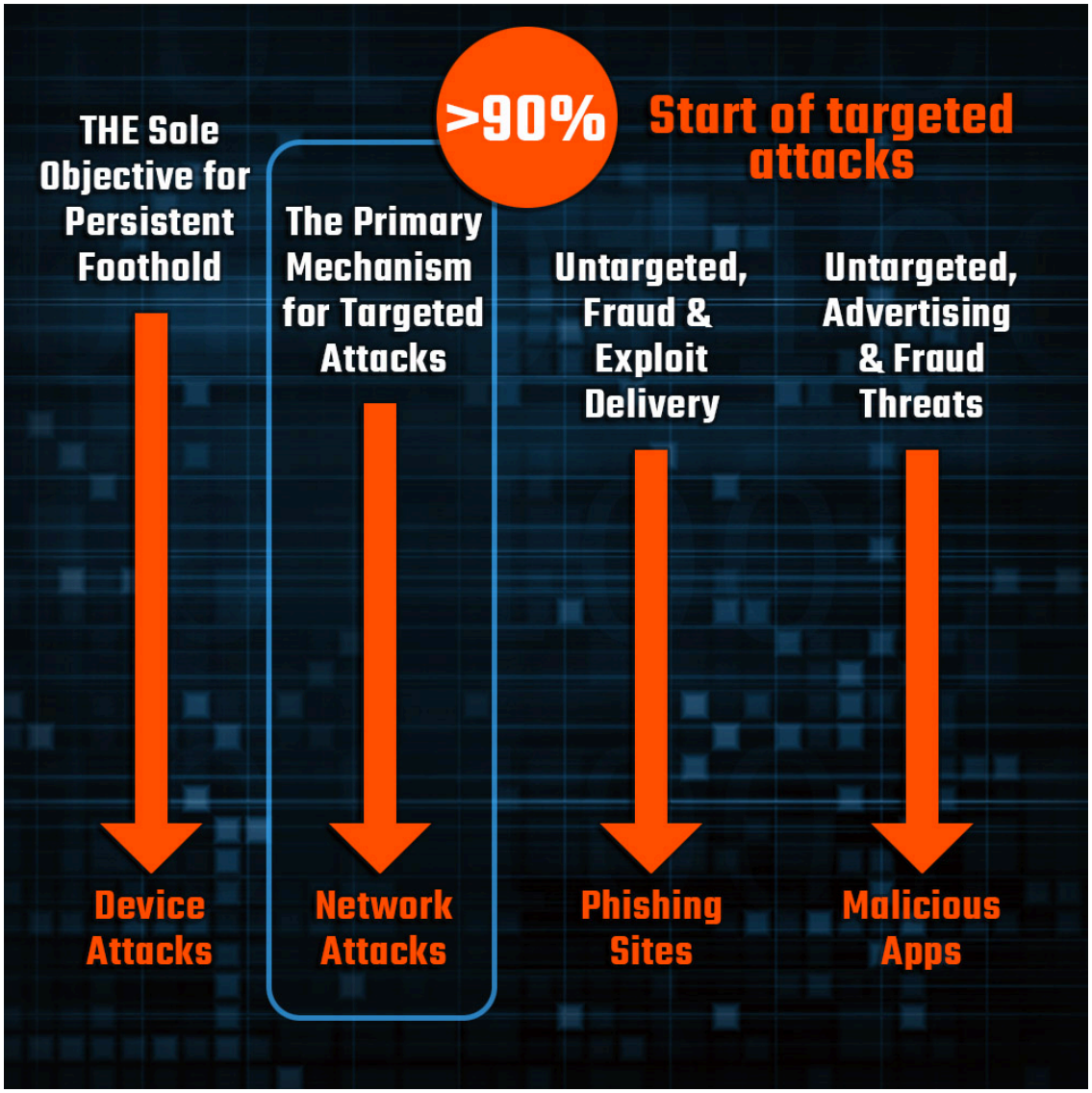
European Commission infographic showed that as of January 2019, fines for GDPR violations had exceeded EURO 50 Million. So it is not surprising that most enterprises subject to the regulation have invested significant resources toward achieving compliance. The problem arises when enterprises focus on protecting endpoints without realizing that **mobile devices are endpoints**, both with respect to GDPR and in general.

Mobile devices are now the de facto platform for productivity in business. That means that the traditional computing devices (e.g., servers, desktops and laptops) that enterprises have focused their security and compliance efforts on are only about 40% of their enterprise's endpoints. The other 60% of devices that connect to your enterprise network—mobile devices—must be made GDPR-compliant as well.



Fact #3: Mobile endpoints are under attack

One critical difference between mobile devices and other types of endpoints is the variety of attack vectors that mobile devices are exposed to. Ensuring the integrity of mobile devices requires protecting them against all of these forms of attack.



Fact #4: GDPR requirements for mobile are explicit

GDPR requirements explicitly apply to mobile and other devices if they hold personally identifiable information (PII) on EU subjects, or sensitive data if it is linked to PII. Since mobile devices are central to productivity in the modern enterprise, they will inevitably interact with systems storing PII. To illustrate, think of the number of emails a typical enterprise worker sends on any given day, and consider that email addresses constitute PII.

Article 5, Principles relating to processing of personal data, states that “(1) Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data... .” In short, your enterprise’s mobile devices must be protected.

Similarly, Article 25, Data protection by design and by default, states in paragraph 1 that businesses subject to GDPR “shall ... implement data-protection principles ... in order to meet the requirements of this Regulation and protect the rights of data subjects.” This means that your enterprise’s mobile devices must be protected by design. Article 25 also requires in paragraph 2 “that businesses shall be responsible for, and be able to demonstrate compliance with, paragraph 1."

Fact #5: Zimperium is the solution for mobile GDPR compliance

Since Zimperium solutions detect threats on-device rather than sending information to a cloud, they can protect mobile devices without the need to collect or processes any personally identifiable information (PII) whatsoever. This is the Zimperium for GDPR configuration. By not collecting or reporting on any PII, Zimperium enables companies to receive all of Zimperium's mobile risk and active threat detection in a completely GDPR-compliant manner.

Zimperium leverages a patented, machine learning-based engine to detect mobile device, network, phishing and app attacks against mobile devices in real time, offering the most comprehensive protection available to mobile devices and the data they contain. To date, the engine has detected 100 percent of zero-day device exploits without requiring an update or suffering from the delays and limitations of cloud-based detection or legacy security architectures, making Zimperium uniquely capable of meeting GDPR mobile requirements.

Contact Zimperium for GDPR mobile compliance

When you are ready to ensure compliance with GDPR mobile requirements, please contact us for a custom evaluation.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244