Skycure
Mobile Threat Defense

Mobile Security

Regulatory Compliance and Privacy Laws

Why enterprises need to make sure their mobile devices are compliant

Mobile device security isn't just a "nice to have"- it's a must have. And one of the reasons for that is because of compliance regulations and privacy laws that exist across the world (and especially in Europe). Since these laws apply to data, they are generally found to be agnostic to the concept of PC or mobile device, making it something enterprises must consider carefully.

In addition to that, many countries are also passing new (or updated) privacy laws that mandate specific requirements for mobile devices operating in their borders or for which their citizens are using. And for enforcement, they have potentially exorbitant fines when enterprises are in violation. It is therefore crucial that enterprises take all appropriate measures to protect their mobile devices and the data which resides on them so that they can remain compliant, continue to do business within all the countries in their market, and avoid hefty fines and bad press from being found incompliant and/or being targeted by a mobile attack.

Here are some mobile and data privacy laws from around the world that enterprises need to be particularly careful of if they operate (or have employees/customers) using mobile apps or devices in these geographies:

United States - Subtitle D of the HITECH Act

Addresses the privacy and security concerns associated with the electronic transmission of health information across any medium which includes mobile devices. There are four categories of violations that reflect increasing levels of culpability and four corresponding tiers of penalty amounts where the minimum penalty amount increases significantly with each violation. A maximum penalty amount of $1.5 million exists for all violations of an identical provision.

Maximum Penalty: $1.5 million

"Security is the largest concern from an IT standpoint—making sure the healthcare workers who are using the devices are in compliance, and that the medical records they access are logged. It's important that the movement and use of any data is constantly tracked and logged, especially when it comes to a lost or stolen device, or if an employee is no longer eligible to view the information."
— Chris Hazelton, Research Director, Mobile & Wireless, 451 Research [1]

"According to the U.S. Department of Health & Human Services (HHS) most breaches reported to HHS so far under the HITECH Act have been theft or loss of mobile computing devices, resulting in the exposure of millions of patients' protected health information." [2]

1,2 https://www.linkedin.com/pulse/hipaa-hitech-help-mobile-device-management-mdm-healthcare-lloyd

United States – Healthcare / HIPAA

As malware and ransomware attacks continue to grow (especially by using mobile devices as entry points), Human Health Services (HHS) stipulates that healthcare organizations are now responsible to:

- Identity cyber-risks and craft a plan to manage the risks, such as limiting access to sensitive patient information only to people who really need it
- Establish explicit policies to protect your systems from malware
- Educate end-users to (1) recognize malware and (2) follow your cyber-security policies and procedure

In addition, for ransomware specifically, companies must (1) implement education for end users, (2) detection must be proactive, and (3) when an attack occurs disclosure must be rapid.

> *"One of the biggest current threats to health information privacy is the serious compromise of the integrity and availability of data caused by malicious cyber-attacks on electronic health information systems, such as through ransomware."*
>
> **— Jocelyn Samuels, Director, HHS Office for Civil Rights**

European Union - General Data Protection Act *Goes into effect May 25th, 2018*

GDPR will force accountability by imposing key principles of privacy across computers and mobile devices, such as:

- Right for users to be forgotten (data purge)
- Privacy by design
- Transparency of what data is collected
- Many more data security and accountability principles.

Companies in the European Union can be fined 20 Million Euros or 4% of their worldwide annual revenue (whichever is greater) for breaking the regulations set out in the GDPR[3]. Mobile security solutions using sideloaded private APIs have the highest risk of violating this.

Mobile security solutions using sideloaded private APIs have the highest risk of violating this.

> *"The authors of GDPR specifically noted the ability of the smartphone to capture private information on users, proscribing understandable privacy notice and active consent from users prior to any collection of private data."*
>
> *"Any website or mobile application that is accessible by a person in the EU will need to comply with GDPR."*

3 http://blog.isc2.org/files/getting-started-on-the-basics-the-eu-general-data-protection-regulation-gdpr.pdf

Germany - Federal Data Protection Act

(also known as Bundesdatenschutzgesetz, or BDSG)

Individuals have the right to grant permission which specifies how, where, how long, and for what purposes their data may be used, and individuals can revoke that permission at any time ("right to be deleted"). Paragraph 6c in particular applies to mobile data-storing and data processing devices, and BDSG violators of this law can face fines up to 300,000 Euros.

"From a German data protection law perspective, health apps are subject to specific requirements for internet services according to the Telemedia Act ("TMG") but a number of other requirements may also apply due to the nature of personal data collected, processed and used." [4]

"The carefree handling of the apps on the part of vendors and users alike in connection with the rapidly increasing dissemination entails risks regarding compliance with data protection regulations." [5]

Singapore - Personal Data Protection Act (PDPA)

Establishes various rules governing the collection, use, disclosure and care of personal data. It recognizes both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organizations to collect, use or disclose personal data for legitimate and reasonable purposes. Essentially, mobile devices, the data, and the apps must all be compliant with the PDPA, otherwise, PDPC (the regulating body) can impose financial penalties of up to $1 million for non-compliance.

Maximum Penalty: $1 million

"Ninety percent of mobile apps in Singapore do not adequately declare what consumer data is collected or how it is used, potentially falling foul of Singapore's Personal Data Protection Act (PDPA)" [6]

Russia

Any foreign cloud service Russians use, requires those services to store all Russian citizen data within the country – meaning any cloud services that will house personal data of Russian citizens must have physical servers located within the Russian Federation. Regulated data will not be allowed to leave the country's borders without meeting strict requirements. This means that any enterprise with Russian employees must make sure any enterprise mobile app which relies on a cloud backend is not collecting, storing or analyzing any private data and is compliant with the law, or risk business disruption if their IT systems become blocked/restricted by Russia's state telecommunications agency.

4 https://www.taylorwessing.com/synapse/april15.html
5 https://www.datenschutz-notizen.de/datenschutzrechtliche-bestimmungen-und-smartphone-apps-04282/
6 http://www.straitstimes.com/tech/90-of-mobile-apps-could-be-in-breach-of-singapore-privacy-law

Hong Kong - Personal Data (Privacy) Ordinance (Cap. 486)[7]

Protect individuals' right to privacy by regulating the handling of personal data in Hong Kong. It applies to any person or organization, both public and private, that collects, holds, processes or uses personal data on any data processing device (computers, mobile devices, etc.). The guidance issued in February 2014 calls for businesses to adopt comprehensive Privacy Management Programs directed at achieving compliance in all aspects of business. Individuals may complain to the Privacy Commissioner about suspected violations of the Ordinance.

The Commissioner can investigate complaints of breach as well as initiate investigations. With increased fines and new regulations, PDPO compliance has to be a priority for enterprises doing business in Hong Kong.

Persons who control or use personal data ("Data Users") must prove they took all reasonable precautions and exercised all due diligence to avoid violation. The burden of proof is on the Data User and it is also liable for its agent's contravention of the legislation. Violations can result in fines and even imprisonment.

Penalties: Fines or imprisonment

United Kingdom – UK Data Protection Act

Employers are expected to make employees aware of any monitoring that's taking place, with the exception of where criminal activity is suspected. This means that any mobile security solution that looks into a user's private information without their knowledge and consent would be in violation of this law.

France

In France, any company with a BYOD policy that involves monitoring an employee's personal device are required to gain the consent of the employee to do so.

Spain – Spanish Law 15/1999

As part of the Spanish Law 15/1999 under the EU Privacy Directive, employees at organizations that implement BYOD policies should be made aware which data will be monitored or collected from their personal devices. In addition, employers in Spain are expected to obtain the consent of an employee before installing any software or technology to their personal devices that monitors data or activity on an employee's device.

Switzerland – Federal Act on Data Protection (FADP)

Provides for numerous principles that regulate the process of personal data across computers and mobile device, including (Article 4, FADP):

- Personal data can only be processed lawfully.
- Personal data processing must be carried out in good faith and must be proportionate.
- Personal data must only be processed for the purpose indicated at the time of collection, that is evident from the circumstances, or that is provided for by law.
- The collection of personal data and in particular the purpose of its processing must be evident to the data subject.

7 https://www.pcpd.org.hk/english/ordinance/ordfull.html

Switzerland – Federal Act on Data Protection (FADP), continued

If the consent of the data subject is required for the processing of personal data, the consent is only valid if given voluntarily on the provision of adequate information. Additionally, consent must be given expressly for processing sensitive personal data or personality profiles, making mobile devices especially sensitive to these laws. Mobile security solutions using sideloaded private APIs have the highest risk of violating this.

Mobile security solutions using sideloaded private APIs have the highest risk of violating this.

Summary

As this list outlines, countries around the world are adopting stricter, more enforceable privacy laws which apply to user data regardless of device type. It is critical that enterprises understand the laws of any countries they operate in, so they can protect themselves from the penalties (and bad press) that would come with non-compliance on any mobile device (for employees and/or customers). Therefore, keeping mobile devices (and their data) properly protected with a comprehensive Mobile Threat Defense solution which doesn't violate individual privacy is a crucial component of staying compliant with these regulations. The following capabilities in particular will be critical to keeping enterprises compliant globally:

- **Public app** – an end user app that is downloaded directly by end users via an official app store, instead of a private app which might be installed and/or collect personal information without employee consent.
- **Proactive protection** – monitoring for malware, ransomware, and malicious networks, and then taking automated mitigation action when they are detected.
- **Global Threat Intelligence** – There is only so much intelligence that can be gathered from a single device, single organization, or a single country. Leverage Global Threat Intelligence to protect from novel and zero-day exploits

Unsure about mobile security regulatory compliance and privacy laws in your industry or geography? Talk to an industry expert:

CONNECT NOW

About Skycure

Skycure is the leader in mobile threat defense. Skycure's platform offers unparalleled depth of threat intelligence to predict, detect and protect against the broadest range of existing and unknown threats. Skycure's predictive technology uses a layered approach that leverages massive crowd-sourced threat intelligence, in addition to both device- and server-based analysis, to proactively protect mobile devices from malware, network threats, and app/OS vulnerability exploits. Skycure Research Labs have identified some of the most-discussed mobile device vulnerabilities of the past few years, including App-in-the-Middle, Accessibility Clickjacking, No iOS Zone, Malicious Profiles, Invisible Malicious Profiles, WifiGate and LinkedOut. The company is backed by Foundation Capital, Shasta Ventures, Pitango Venture Capital, New York Life, Mike Weider, Peter McKay, Lane Bess, and other strategic investors.

Skycure
Mobile Threat Defense