Lookout

WHITEPAPER

Finding GDPR noncompliance in a mobile first world

How to gain visibility into mobile threats & risks that could trigger infringement fines

> "Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."
>
> GDPR Article 5, clause 1(f)

GDPR is unavoidable and will directly impact how your organization handles personal data

GDPR continues to gain a lot of attention in corporate security and IT departments as well as in the C-suites and boardrooms of many global companies, and that's a good thing. The regulation, a set of rules created by the European Parliament, European Council and European Commission, will come into effect on May 25, 2018. It is designed to bolster data protection and rights to privacy for individuals within the European Union (EU). GDPR also addresses the export of "personal data," which is any information relating to an identified or identifiable individual – outside the EU.

Defining Terms

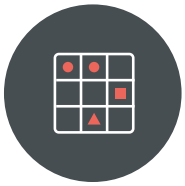
Personal Data	Any information relating to an identified or identifiable natural person ("Data Subject")
Natural Person	A living human being
Data Subject	Any person whose personal data is held by a compan

Any organizations that handle data for individuals in Europe need to be preparing for GDPR compliance today, and that includes many U.S.-based companies that do business or offer services in Europe.

At the same time, mobile technology is everywhere. The digital and mobile transformation has made mobile devices critical infrastructure for day-to-day operations in nearly every organization. This massive shift has put the privacy of personal data on mobile at risk. Every department and each employee in your organization with access to customer, partner, or employee personal data has the potential to have that data compromised through their mobile device – triggering a GDPR infringement event.

As research firm Gartner Inc. noted in a report, Revisit Your Enterprise Mobility Management Practices to Prepare for EU GDPR. "By 2019, 30% of organizations will face significant financial exposure from regulatory bodies due to their failure to comply with GDPR requirements to protect Personal Data on mobile devices."

In order to avoid this outcome, and to be truly compliant with GDPR, companies must understand and address the Spectrum of Mobile Risk by securing personal data from mobility-related risks that can jeopardize their ability to meet compliance requirements.



THE MOBILE RISK MATRIX

Vectors

Components of Risk

	APPS	DEVICE	NETWORK	WEB & CONTENT
THREATS	**App threats** Malicious apps can steal info, damage devices, and give unauthorized remote access.	**Device threats** Device threats can cause catastrophic data loss due to heightened attacker permissions.	**Network threats** Data is at risk of attack via Wi-Fi or cellular network connections.	**Web & content threats** Threats include malicious URLs opened from phishing emails or SMS messages.
SOFTWARE VULNERABILITIES	**App vulnerabilities** Even well known software development companies release apps that contain vulnerabilities.	**Device vulnerabilities** The vulnerability window is the time it takes from the release of a new patch to adoption.	**Network vulnerabilities** Mobile devices encounter more hostile networks than laptops, and have less protection.	**Web & content vulnerabilities** Malformed content, such as videos, and photos can enable unauthorized device access.
BEHAVIOR & CONFIGURATIONS	**App behaviors & configurations** Mobile apps have the potential to leak data such as contact records.	**Device behaviors & configurations** USB debugging for Android or installing apps from non-official app stores.	**Network behaviors & configurations** Misconfigured routers, unknown captive portals, or content filtering.	**Web & content behaviors & configurations** Websites that don't encrypt credentials or leak data.

Get a printable version of the Mobile Risk Matrix here.

Why mobile is a problem for GDPR compliance

Digital transformation is one of the key catalysts for increasing access to regulated personal data on mobile devices. As enterprises embark on digital transformations that include both a big move to the cloud and extensive access to data via mobile devices they also open that data up to compromise from a range of malware, vulnerability exploits, and non-malicious data leakage.

Employees now have more choices than ever over the way they can work and from which locations. They can choose the devices, apps, and networks from which to access corporate data and applications. This includes their own devices and apps as well as those owned or controlled by their organizations. Mobility has enabled employees to work from wherever they happen to be at the moment, and to gain access to work-related data and networks.

Many of the current hardware and software security solutions enterprises have do not address the spectrum of mobile risk. Legacy products developed years ago were not designed to secure mobile endpoints, and even mobile management tools do not address all mobile security threats, vulnerabilities or risky behaviors.

Because of this mobile security gap, companies can suffer significant security breaches that often result in exposed data, financial losses, lawsuits, and damage to corporate reputation and brand. But that's not all. Mobile devices now present a significant compliance risk to organizations as well. The same policies that companies have applied to their fixed endpoints now also need to be applied to mobile endpoints.

Companies need to focus on how data compromise can happen on mobile devices, and how both malicious attacks and non-malicious data leakage from apps can cause an enterprise to be out of compliance—and therefore face significant fines and other negative outcomes.

The question is now: how does my organization ensure the security of the data being accessed by our mobile fleet? Each organization's answer will affect their ability to protect critical intellectual property and achieve compliance.

84%

of US IT executives agree that the personal data accessed on their employee's mobile devices could put their company at risk for GDPR noncompliance*

64%

of US employees say they access their organization's customer, partner, and employee data while on their mobile device*

73%

use the same phone for personal and work purposes*

*An online survey was conducted to a panel of potential U.S. and U.K respondents. The recruitment period was September 5, 2017 to September 15, 2017. A total of 2062 respondents completed the survey (excluding terminates and abandonments). All respondents were 18 years of age or older, employed full time at a company with 1,000 employees or more, and work for a company that has employees and/or customers/partners in the European Union (this excludes the UK; If only customers/partners, the company must store their personal data). 1000 of the respondents were a decision maker or involved in decision making process as related to IT security, and had a title level above intern, entry level, analyst/associate. The remaining respondents were enterprise employees with the same criteria as above. The sample was provided by Market Cube, a research panel company. All were invited to take the survey via an email invitation. The margin of error is 2.2%.

Understanding the threats & risks to GDPR compliance from mobile

While many organizations have already begun the process of GDPR compliance, many are still in the assessment phase.

One of the key elements of GDPR is "Privacy by Design," a framework that is based on proactively embedding privacy into the design and operation of IT systems, network equipment, and business practices.

GDPR formally makes Privacy by Design a legal requirement for organizations, promoting six privacy principles for how EU Personal Data should be handled.

Eight Privacy Principles

- Lawfulness
- Fairness and Transparency
- Purpose Limitation
- Data minimization
- Accuracy
- Storage Limitation
- Integrity
- Confidentiality

According to GDPR documentation, privacy principle 6 states that "personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures."

What many organizations might not fully realize—even those that are further along in their GDPR compliance efforts—is the impact of mobile technology on their efforts to prepare for the new rules.

How exactly do the GDPR requirements apply to mobile?

Data Handling

Companies need to know what data is being accessed on mobile devices, who is accessing the data, how this data access is being controlled, and where the data goes.

Breach Notification

Companies need to know at all times what their visibility is into mobile threats, how they are notified about threats, and how they can remediate mobile threats in a timely manner.

"Privacy by Default"

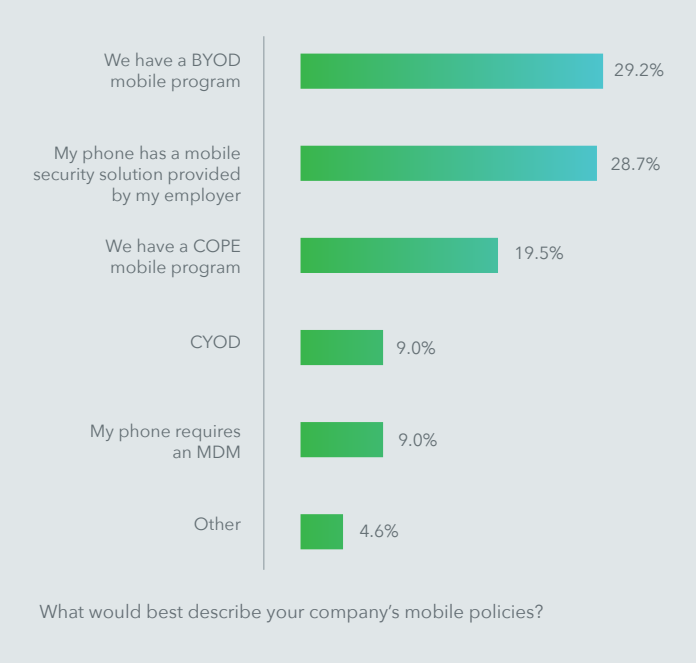
Companies need to know how they can balance control with end-user privacy, and whether they are unwittingly collecting further personal data.

A number of mobile risks can directly violate privacy principle 6 of GDPR

- Malicious apps that can leak or infiltrate information, damage devices by embedding so deeply that they cannot be removed from the device even with a factory reset, and provide unauthorized remote access
- Device threats that can heighten attacker permissions to spy on communications occurring on the device, causing catastrophic data loss
- Mobile apps that access contact records and send data to servers residing outside of the EU
- Mobile devices that are connected to a network that has been compromised by a man-in-the middle attack, resulting in data being siphoned off the device

Given the prevalence of mobile devices access and use of customer data, there's a significant risk factor of data loss or leakage involved. That's true whether the devices are company or employee owned. And the bring your own device (BYOD) phenomenon adds another level of complexity to the challenge. In some countries, many workers continue to bring their own smartphones and tablets into the workplace, which brings an elevated risk of data loss, out-of-date security patches, and other consumer to enterprise mobile issues.

BYOD is the most common mobility policy



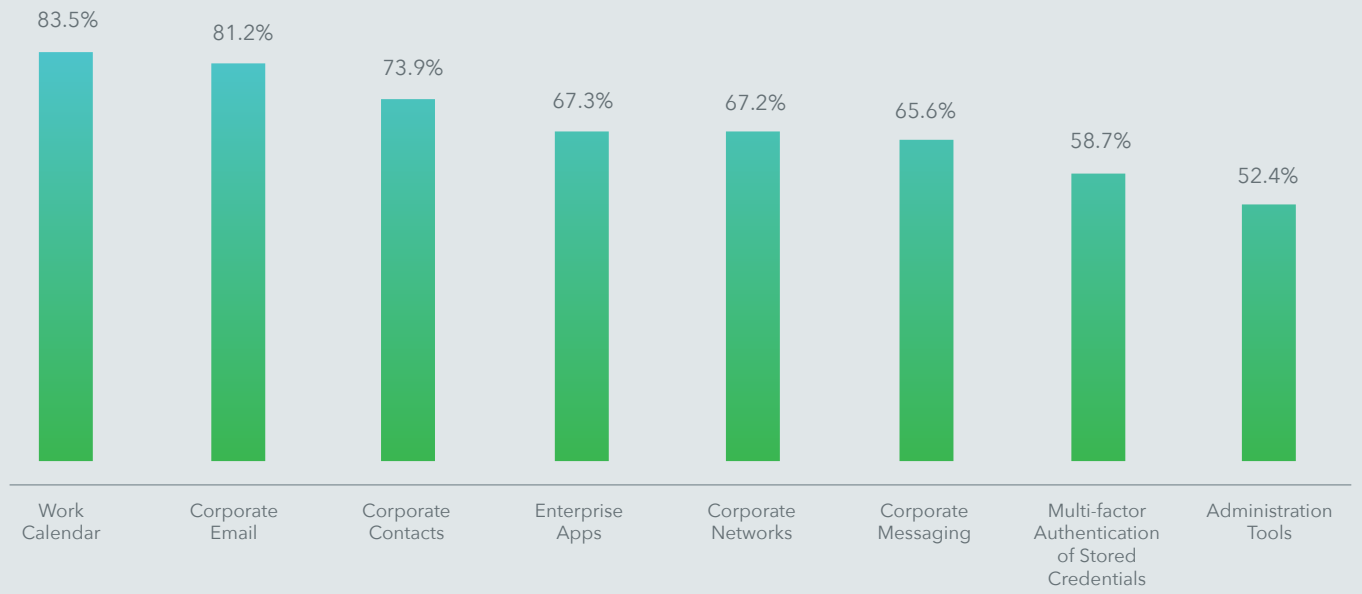
Mobile internet use passed desktop back in November 2016. Your employees are likely spending more time on their mobile devices than on their computers, and spending the vast majority of that time working with mobile apps rather than a browser. In a lot of cases, people are using these devices in public places such as coffee shops and hotel lobbies, and relying on those facilities' open Wi-Fi networks for access to corporate data. As many companies move into the cloud rather than dedicated data centers, and this can heighten the security risks based on accessing data.

The growth of mobility in conjunction with the rise in cloud services and apps has been a great boon to productivity and collaboration for many organizations. But it has also put data and systems largely out of the control of central IT and corporate security programs. Consider the data and other IT resources on a typical smartphone: enterprise email, company and personal credentials, corporate network access, and enterprise apps, as well as capabilities such as built-in high-definition cameras and microphones. Today's smartphone can have access to and store a lot of sensitive data and is frequently on the move.

The growth of mobility in conjunction with the rise in cloud services and apps has been a great boon to productivity and collaboration for many organizations. But it has also put data and systems largely out of the control of central IT and corporate security programs. Consider the data and other IT resources on a typical smartphone: enterprise email, company and personal credentials, corporate network access, and enterprise apps, as well as capabilities such as built-in high-definition cameras and microphones. Today's smartphone can have access to and store a lot of sensitive data and is frequently on the move.

Many users of mobile devices and the mobile apps themselves can potentially put sensitive data at risk. They can access sensitive data such as personally identifiable customer information, upload sensitive data to external servers, violate data sovereignty regulations or send data to risky geographies. There are apps that access cloud storage providers, social networking services, or peer-to-peer networks, apps that don't use adequate encryption when storing or sending data, and apps with known vulnerabilities.

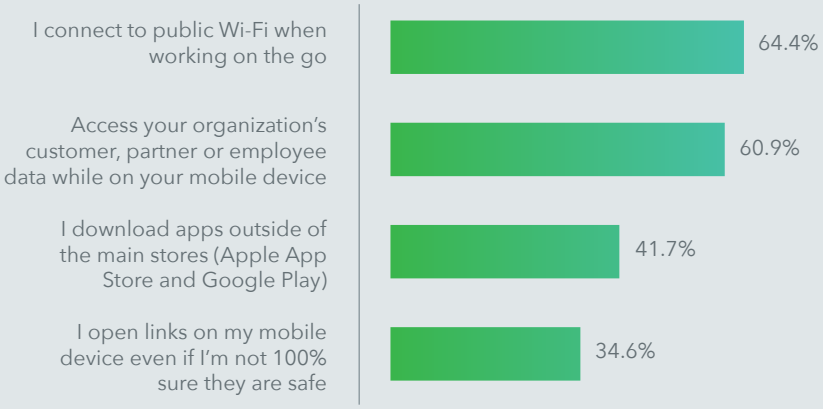
Most employees access enterprise calendar and email apps from mobile



Do you have access to the below on your mobile device? Y/N

As part of their GDPR compliance efforts, organizations need to deploy technology solutions that enable them to understand the capabilities and risky behaviors of the apps on their employees' mobile devices, by analyzing the apps. They need a solution that protects against mobile attack vectors such as malicious and end-user jailbreaks, operating system vulnerabilities, lost or stolen devices, malicious apps, non-compliant apps, app vulnerabilities, data leakage, and malicious man-in-the-middle attacks.

Employee behaviors put personal data at risk on mobile



Which of the following behaviors do you do on your mobile device?

Once organizations have achieved visibility across the spectrum of mobile risk, the next step in protecting EU personal data is to establish policies to remediate threats in a timely manner, mitigate the risk of data-leaking apps at scale, and do so while ensuring end-user privacy. One thing to keep in mind with policies is scale. A single policy engine should allow organizations to specify what kinds of behavior and other risks are non-compliant, which enables them to quickly focus on all the potential problem areas within their mobile fleet.

Finding & stopping mobile threats to GDPR compliance

Organizations facing GDPR compliance requirements need to look to mobile threat defense solutions such as Lookout Mobile Endpoint Security to provide the visibility and policy controls they need to protect EU personal data, enabling them to achieve measurable risk reduction. Here is how such a solution can help organizations prepare for GDPR:

- **Quickly identify risks to EU personal data that mobile devices can present.** Lookout Mobile Endpoint Security provides visibility to quickly identify critical mobile risks across the spectrum of mobile risk, drilling down from a dashboard view into detailed information about a specific threat, software vulnerability or risky behavior and configuration that might be putting EU personal data elements at risk of unauthorized access and loss.
- **Implement comprehensive policy-based protection to remediate mobile risk at scale.** The solution provides the policy controls needed to protect EU personal data at scale, allowing organizations to achieve measurable risk reduction. They can establish policies that can remediate threats in a timely manner, mitigate the risk of data-leaking apps at scale, and do so while ensuring user privacy.
- **Establish risk-based conditional access policies.** Integrating Lookout Mobile Endpoint Security with mobile device management (MDM) lets organizations establish risk-based conditional access policies to ensure that enterprise data is secure. For example, if the Lookout solution determines that a user has sideloaded an app containing malware, it immediately notifies the MDM that the device is out of compliance and the MDM can invoke an appropriate response such as shutting down the device's access to all corporate apps until the risk is resolved.
- **Prepare for GDPR's 72-hour breach notification requirements.** Lookout Mobile Endpoint Security provides timely notifications to administrators whenever data is maliciously exfiltrated or leaked from a mobile device. This gives administrators detailed information about the identified issue within the Lookout console, allowing notification to the supervisory authority "without undue delay".
- **Apply safeguards around transfers of data outside the EU.** The solution provides visibility into apps that are insecurely handling data-at-rest or in-transit, as well as visibility into the locations where data is being sent. This allows organizations to implement safeguards around EU personal data. For in-house developed apps, administrators can upload an app to the console and it will be analyzed for these vulnerabilities, alongside other risky behaviors.
- **Ensure that the mobile security solution adheres to the Privacy by Design principles.** Lookout developed its solutions with the Privacy by Design concept in mind. The company has a heritage of protecting millions of devices worldwide, and its solution has been designed to respect the privacy of end users. For example, it has robust privacy controls, including the ability to restrict collection of any personal information associated with users or devices under management.

What makes the Lookout solution especially effective and unique when it comes to GDPR readiness is its massive global sensor network and threat intelligence capabilities. The success of Lookout's personal and enterprise endpoint products has given the company visibility into threats and risks from more than 150 million mobile devices worldwide.

Every month millions of devices in more than 150 countries send security telemetry to the Lookout Security Cloud, ensuring that Lookout can track evolving threat actors and provide novel threat discoveries such as the Pegasus spyware. The massive mobile dataset that is unique to Lookout gives customers the advantage of security precision and context: it allows organizations to understand if a potential mobile threat signal or characteristic is normal, rare, or truly anomalous in the world, based on more than 50 million unique mobile applications and tracks their prevalence in real-time across its global sensor network.

By fully understanding the requirements of GDPR—including the many implications for mobile devices—and deploying effective technology solutions to protect data in the mobile environment, companies can be best prepared for meeting these new regulatory requirements.

It's important to keep in mind that with security and privacy, it's difficult to know exactly what it means to be in compliance. There are always degrees of compliance; it's not a black and white issue. What one company considers adequate compliance another might consider to be lax, and yet another might think of as overkill. The variance depends on the risk tolerance of the organization. And while no mobile solution will make companies "compliant," a solution should address the mobile threats and vulnerabilities a company can potentially face.

GDPR sets a new standard on how organizations must handle and protect Personal Data. It's not a new concept; it's something most organizations have already tackled in some form. But now it's time to properly scope your privacy program to include the mobile infrastructure.

Next steps: get visibility into mobile threats to extend GDPR compliance to mobile

GDPR sets a new standard on how organizations must handle and protect personal data. It's not a new concept; it's something most organizations have already tackled in some form. But businesses are now facing severe pressure to comply with a growing number of government and industry regulations involving data protection, including GDPR. This makes now the time to properly scope your privacy program to include the mobile infrastructure.

The stakes of non compliance are extremely high, including potentially heavy fines. For example, GDPR states that penalties for noncompliance can be up to 4% of a violating company's global annual revenue, depending on the nature of the offence.

The need for data security and privacy must extend to the mobile environment, because that's where much of day-to-day business operations and processes are taking place today. But it also presents a host of security threats, vulnerabilities and risky behaviors that can jeopardize the confidentiality, integrity, and availability of data.

In the end, the need for regulatory compliance is actually providing organizations with a prime opportunity to strengthen their overall security—including the security of their growing mobile ecosystems.

Visit: www.lookout.com/gdpr to learn more about how your organization can extend GDPR compliance to mobile.

About Lookout

Lookout is a cybersecurity company for a world run by apps. Powered by the largest dataset of mobile code in existence, Lookout is the security platform of record for mobile device integrity and data access. Lookout is trusted by more than 100 million individuals, hundreds of enterprises, and government agencies, and ecosystem partners such as AT&T, Deutsche Telekom, and Microsoft. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto, and Washington, D.C.