GDPR with Lookout

Mobile Endpoint Security

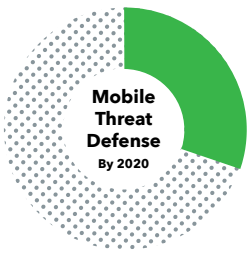
Extending compliance on mobile

The General Data Protection Regulation (GDPR) went into effect on 25 May 2018 and introduced new data privacy requirements to protect EU residents' personal data wherever they may be. Now more than ever, mobile has become the predominant way in which employees are staying productive and their mobile device is a tool used for both business and personal use. As personal and enterprise data are regularly co-mingling on employees' mobile devices, enterprises need to take action on both BYOD and corporate-provided devices to ensure the enterprise's mobile endpoints are secure.

64% of US employees say they access their organisation's customer, partner and employee data while on their mobile device

Organisations need a solution to help address GDPR requirements and gain visibility and control over any personal data that could be compromised. If nothing is done, mobile could be a trigger that could damage brand reputation, customer loyalty and even lead to significant GDPR fines. Now is the time to invest in security measures to safeguard sensitive employee, customer and partner data accessible from mobile devices, and to ensure compliance with GDPR.

By 2020, 30% of organizations will have MTD in place, an increase from less than 10% in 2018.[1]



Examples of personal data that could be compromised:

- Name
- National ID number
- Address
- Personal email address
- Credit card
- Bank account
- Corp email
- Contacts
- Photos
- Location

[1] Gartner Market Guide for Mobile Threat Defense Solutions, Dionisio Zumerle & John Girard, October 2018

Lookout can help organisations avoid GDPR violations

Provide Visibility:

"My MDM allows me to implement management policies, but I need to have visibility into threats, vulnerabilities, and risky app behaviours that can compromise the personal data stored and accessed by my organisation's mobile devices."

Lookout provides visibility into:

- Malicious apps that can steal personal data, damage devices and give unauthorised remote access
- Device vulnerabilities that can be exploited to heighten attacker permissions to spy on all communications occurring on the device, causing data loss
- Apps that access location and therefore turn the mobile device into a proxy of the user's physical location, allowing an individual to be tracked without explicit consent
- Mobile apps that insecurely handle data at-rest and in-motion, opening the door to attackers to compromise the confidentiality of personal data being transferred
- Mobile devices that are connected to a network that has been compromised by a man-in-the middle attack, resulting in personal data being siphoned off the device

Gain Control:

"I need to be able to manage EU personal data accessed by mobile devices in my fleet. My organisation currently lacks both visibility into new risks and control over this data on mobile, leading to potential data compromise."

- Lookout provides policy templates needed to protect EU personal data at scale, enabling organisations to remediate threats in a timely manner and mitigate the risk of data-leaking apps while ensuring end user privacy
- Integrating Lookout Mobile Endpoint Security with your MDM (mobile device management) allows you to establish risk-based conditional access policies to ensure your sensitive data stays secure
- Lookout also provides end users with simple instructions for how to immediately resolve the issue – 95% of Lookout end users self-remediate the risk within 24 hours, further mitigating the data breach risk

67% of US employees say they access enterprise apps on mobile in order to do their job

Art. 32 "Security of Processing"

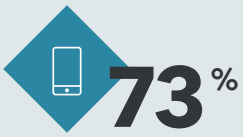
"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk…"[2]

[2] General Data Protection Regulation, Article 32, https://gdpr-info.eu/art-32-gdpr/

Timely Notifications:

"I need to be able to notify the Data Protection Officer (DPO) ASAP if I believe there has been a data breach."

- Lookout Mobile Endpoint Security provides timely notifications to administrators when data may be maliciously exfiltrated or accidentally leaked from a mobile device, arming administrators with detailed information about the identified issue within the Lookout console to enable notification to the supervisory authority "without undue delay"
- Lookout has built connectors to leading SIEM systems such as Splunk, ArcSight and QRadar, enabling security professionals to quickly view threat events and metadata in their SIEM solution



73% of US employees use the same phone for personal and work purposes

74% of US employees say they have access to corporate contacts on their mobile device

Art. 33 "Notification of a personal data breach to the supervisory authority"[4]

"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55..."[3]

Privacy by Design:

"To protect personal data and meet GDPR requirements, my organisation's mobile solutions need to adhere to Privacy by Design principles."

- Lookout adheres to data minimisation and purposeful data collection principles, and has robust privacy controls, including the ability to restrict collection of any PII associated with users or devices under management as well as limit end user information presented to administrators of the Lookout solution
- Lookout has put in processes to adhere to data subject rights under GDPR as detailed below:
  - Know how your data is being processed
  - Obtain the data being processed
  - Correct inaccurate personal data
  - Choose to have your personal data erased
  - Restrict processing of your personal data
  - Object to the processing of your personal data
  - Request not to be automatically profiled based on your personal data
- Lookout is EU-US Privacy Shield certified as of October 2018, ISO 27001 certified as of June 2018, ISO 27018 certified as of June 2018, and FedRAMP In Process as of March 2017.

Art. 25 "Data protection by design and by default"

"The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."[4]

[3] General Data Protection Regulation, Article 33, https://gdpr-info.eu/art-33-gdpr/

[4] General Data Protection Regulation, Article 25, https://gdpr-info.eu/art-25-gdpr/

Closing the GDPR gap on mobile is easy

Now is the time to invest in a mobile endpoint security solution to safeguard your organisation's personal and sensitive data accessible on mobile and to help satisfy GDPR requirements.

Lookout is a solution that can quickly help organisations close the GDPR gap on mobile devices:

- **Extensive global device network:** A global device network of more than 170M+ mobile devices in over 150 countries gives Lookout early and exclusive visibility into new and existing mobile threats.
- **Massive mobile dataset and machine learning technology:** Lookout has the world's largest dataset of mobile code, encompassing over 70M+ unique mobile apps and more than 340,000 daily security events across the app, network, and device vectors. This massive dataset coupled with our machine learning technology allows Lookout to deliver superior protection.
- **Comprehensive policy-based protection at scale:** Lookout Mobile Endpoint Security allows enterprises to set and enforce custom policies at scale to protect against the spectrum of mobile risk.
- **Simple deployment and management:** Lookout integrates seamlessly into your MDM for easy deployment and is easy to maintain, minimising helpdesk tickets.

To learn how you can protect the data accessible from your mobile fleet today and satisfy GDPR requirements, contact us at lookout.com