LAST MODIFIED: APRIL 2018 | V 1.14

Data privacy policy

WANDERA LTD. 45 MORTIMER STREET, LONDON, W1W 8HJ +44 (0) 203 301 2660
WANDERA INC. 220 SANSOME STREET, SUITE 1400, SAN FRANCISCO, CA 94104 +1 (415) 935 3095
WANDERA CZ S.R.O. LIDICKÁ 2030/20, ČERNÁ POLE, 602 00, BRNO, CZECH REPUBLIC +420 538 890 059

Table of contents

1 Introduction

1.1 Wandera solution overview

Wandera provides enterprise security and data management solutions to mobile organizations.

The service consists of a lightweight app that resides on the mobile device and an optional cloud gateway that provides real-time network monitoring. The Wandera mobile app is employee-friendly and helps to educate users on data usage while keeping them notified of relevant policy updates and security events. The cloud gateway sits transparently in the path of mobile devices' web traffic, analyzing data usage, detecting threats and enabling inline policy actions.

Wandera is managed through a web portal that provides administrators with access to information collected from their mobile device estate and allows them to manage Wandera's solutions from one easy-to-use interface.

1.2 Data privacy and Wandera

Data privacy and security are at the core of the Wandera service. As a security service provider, Wandera's aim is to help its customers and end users effectively manage the risks they face in an increasingly mobile world, from threats such as phishing and mobile malware to unpredictable mobile data costs and regulatory compliance obligations.

In addition, Wandera has factored privacy and security into the fundamental design of its products and processes — both internal and external — in order to ensure that the service is delivered securely and that customer data is adequately protected.

Wandera has developed this security and privacy policy to manage and protect the data it processes on behalf of customers.

1.3 Audience

This document is intended for managers and administrators overseeing a Wandera deployment, and for data privacy officers who define privacy best practices and oversee IT compliance issues. It is recommended that this document be reviewed in advance of service deployment to ensure that all stakeholders are fully aware of the service offerings and available privacy controls.

2 The Wandera service

2.1 Risk management use cases

Wandera's mobile security and data management solutions help customers to effectively manage risk across an organization's mobile fleet; these solutions can be purchased and managed separately based on customer need. The most common use cases for the service are outlined below.

2.1.1 Mobile security

Mobile is indisputably the new frontier for cyber threats. Businesses must do more than simply detect when an attack has occurred. For effective risk management and protection against threats, it is imperative that security leaders have meaningful visibility into how devices are being used. Wandera enables organizations to configure security policies that respond to threats in real-time with a configurable set of options, including notifications, blocks and escalations to the organization's mobility management suite.

2.1.2 Acceptable use enforcement

Mobile devices give employees a world of freedom to access any site, anywhere, at any time. That might also mean accessing the wrong sites, in the wrong place and at the wrong time. Wandera enables organizations to make rules about which behaviors and sites are considered acceptable and gives them the power to enforce those policies in real-time.

2.1.3 Expense management

The increasing popularity of services like YouTube and Netflix mean that data pools are being drained much faster. Wandera enables organizations to set intelligent rules about which employees can access which services, keeping tabs on mounting data usage. Wandera can apply caps at specified thresholds to avoid bill shock events and can warn users about their data usage at regular intervals.

2.2 Architecture

The Wandera solution is comprised of the following components:

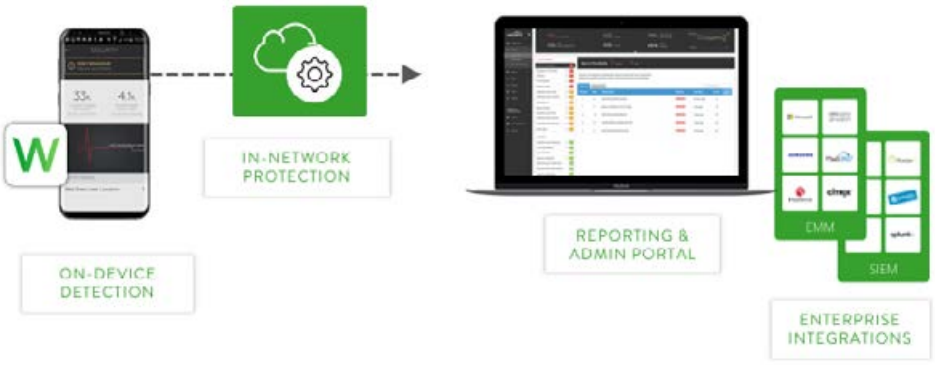

Figure: Wandera Solution Architecture

2.2.1 Mobile app

The Wandera service starts with an application installed on employee devices. The app is designed to scan for security threats and vulnerabilities, giving administrators visibility of the device status and protecting against attacks. It shows employees the latest security alerts and information about their device and gives them an overview of which services they're spending their mobile data on. There's also the option for administrators to send out usage or security notifications directly to employee devices.

2.2.2 Mobile gateway

When employees access the Internet on an enrolled device, the data passes through Wandera's gateway before reaching the intended destination. The gateway operates in the pathway of the data flowing into and out of every device, for cellular connections like 4G, and also when devices are connected to Wi-Fi.

Wandera utilizes intelligent traffic vectoring techniques that ensure that all data remains encrypted - with minimal latency or impact upon battery performance.

2.2.3 Administrator portal

Wandera's administrative portal, RADAR, is the place for administrators to get full visibility and control of their organization's mobile fleet. Accessed through a web browser, it features a variety of different reports showcasing security and usage information, with every dashboard being updated in real-time. It is also where administrators can configure and enroll new devices and get instant alerts for new security incidents.

2.2.4 Enterprise integrations

Wandera is designed to work seamlessly with whatever mobility technology stack is used within an organization. That includes a wide range of different devices and operating systems, as well as a powerful array of different integrations with EMM tools. Organizations can also extend their mobile security policy by exporting directly into a SIEM platform by using Wandera's integration with SIEM tools.

2.3 Data collection and storage

Wandera collects information about user devices in order to provide its security and data management services.

Internally, Wandera controls access to personally identifiable information based on a role-based permissions framework. Data restrictions are applied to prevent employees and partners from accessing sensitive data without a well-defined, documented need. Pseudonymization is utilized to protect unique identifiers when reports are produced.

User data is stored within Wandera's infrastructure hosted by the Amazon Web Services data center in Dublin, Republic of Ireland. This includes all SIEM data exports. By enabling EMM Connect, customers are allowing data transfers between Wandera's infrastructure in the Dublin data center and their EMM's infrastructure using secure API calls.

Customers are able to control what data is visible to their own RADAR administrators using a number of different privacy control options, as described in section 3 of this document. The exact information collected depends on the use case and platforms used.

2.3.1 Privacy by design approach

Wandera's privacy controls utilize a Privacy by Design[1] approach to handling personal data. Pseudonymization and anonymization are applied wherever possible while ensuring the process does not affect product functionality.

Wandera has designed an information architecture that fragments each identifiable individual record (often called a "Golden Record") and distributes parts of that identity over multiple databases and schemas. This ensures the resulting records cannot be individually attributable to any unique user.

2.3.2 Third-party systems used by Wandera

Wandera employs a number of additional services to perform functions on its behalf.

These services have access to limited amounts of Personal Data based on the requirements of the service. These services include customer relationship management (e.g. Salesforce), email providers (e.g. Google), marketing tools (e.g. Marketo), internal communication tools (e.g. Slack), notification systems (e.g. Mandrill) and software development tracking systems (e.g. Atlassian Suite).

These third-party companies are leading providers in their area and store their information in their globally distributed infrastructures. These organizations are certified to transfer this information internationally according to their Binding Corporate Rules and comply with data privacy regulations such as GDPR as well as the EU-US Privacy Shield.

2.3.3 Data retention

All the personal data collected is retained for a period of 12 months and is accessible to only the relevant entities during this period of time. This excludes customer support cases and customer bugs, which are currently kept for an indefinite period of time to provide the best customer service possible.

3 Customer privacy controls and considerations

The specific data collected by Wandera and shared with administrators will be determined by the use cases selected by the customer. Furthermore, configuration and deployment decisions made by the administrator will impact the granularity of data collected.

3.1 Wandera service capabilities

Wandera supports two distinct service deployment models: (1) device-only mode; and (2) device and gateway mode.

3.1.1 Device-only mode

Device-only mode allows for on-device security protection only and does not provide Wandera with any information on the data used by the device. This service does not utilize Wandera's gateway. Wandera recommends that customers consider this service capability in Bring Your Own Device (BYOD) scenarios, and in cases whereby the device type and model may not be compatible with the network monitoring service.

3.1.2 Device and gateway mode

Device and gateway mode provides access to the full suite of Wandera functionality, including all security and data management services summarized in the use cases section. Consistent with this service description, Wandera will collect information on the data usage that occurs on the device and will report on this within the RADAR portal. This is the recommended mode for most scenarios, particularly for any corporate liable devices.

3.2 RADAR portal

Within RADAR, customers are able to manage granular administrator access permissions. Super administrators, the highest level of administrators, are able to manage other administrators and define access to particular sections of Wandera. Wandera offers both read-write as well as read-only administrator permission options, and all actions taken by administrators are stored in Wandera's audit logs.

The RADAR portal uses email addresses, user names and other additional identifiers to identify users throughout the portal. The specific information used here is up to the customer. It is possible to use identifiable email addresses and user names to distinguish between the different users, but it is equally possible to use pseudonyms which will provide an additional layer of privacy to the end users.

For more information regarding the data collected and used, please refer to Appendix A.

3.3 RADAR privacy mode

Privacy mode is an additional feature developed by Wandera that allows customers to limit the personal data that administrators are able to view within RADAR. With privacy mode enabled, data management reports such as the block report and data usage report will use pseudonyms instead of user names, allowing administrators to continue receiving a holistic view of the data used by their devices, without the ability to view this information on a per-device level. Per-device usage reports are disabled when privacy mode is switched on.

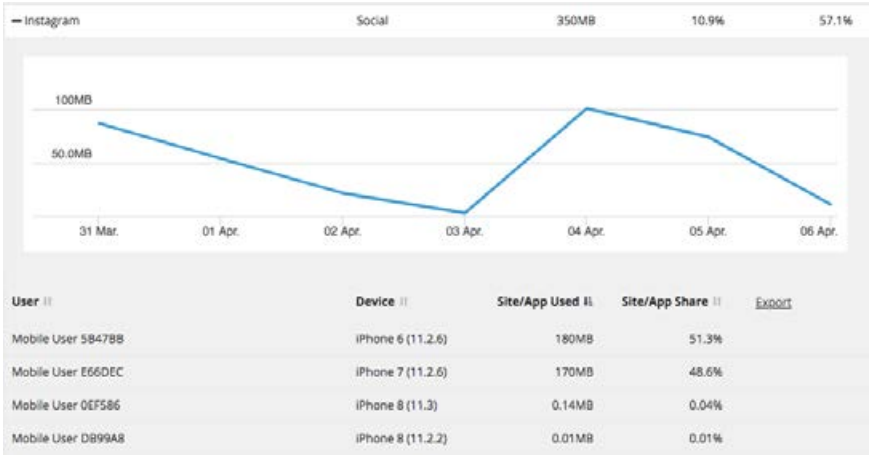

Figure: Pseudonymization applied to a report using Privacy Mode

The privacy mode option can be controlled by super administrators only within the 'service controls' section of Wandera. For more information on privacy mode, please refer to the Wandera Support Center within RADAR.

4 Corporate security policies

Wandera has defined a number of policies regarding general information security, password management, availability, confidentiality, integrity, data classification, physical access, vulnerability management, incident response and disaster recovery.

These policies cover a wide range of security related topics, ranging from general policies that each employee must comply with, to more specialized policies regarding the secure use of internal applications and systems. All policies in the Information and Security Management System (ISMS) are updated and reviewed by senior management at regular intervals.

4.1 Security at Wandera

Wandera's security is managed by the Security team which reports into the Chief Information Officer. This team is responsible for maintaining security at the company's perimeter, creating processes for secure development and review, and building customized security infrastructure. It also has a key role in the development, documentation, and implementation of Wandera's security policies and standards. Wandera's Security team undertakes the following activities:

- Review security plans for Wandera's networks, systems, and services.
- Conduct security design and implementation-level reviews.
- Provide ongoing consultation on security risks associated with a given project.
- Monitor for suspicious activity on Wandera's networks, systems and applications, and follows formal incident response processes to recognize, analyze, and remediate information security threats.
- Drive compliance with established policies through security evaluations and internal audits.
- Develop and deliver training for employees on complying with Wandera security policy, including in the areas of data security and secure development.
- Run vulnerability management programs to help discover problem areas on Wandera's networks and web services, and participate in remediating issues within expected timelines.

All Wandera employees receive comprehensive and regular security training.

4.2 Wandera internal compliance and certification

Wandera adheres to ITIL best practice procedures for internal operational and support processes. Where appropriate, Wandera follows standards and procedures as defined by accredited organizations.

Wandera also conducts annual reviews of partners to ensure that they continue to maintain or improve upon the standards that they have been certified against. Wandera follows best practices defined by various bodies in relation to standards and procedures. These include but are not limited to: SSAE 16 or SAS 70 Type II, PCI DSS, HIPAA, ISO9001, ISO 27001 and ITIL.

4.3 Management of data

4.3.1 Production environment

Access to the production environment is restricted to Technical Operations staff. Wandera operates a limited access control policy to maintain the integrity of production data. Defined operational data cannot be copied to any device outside the production environment. All production resources are password-protected, configured securely and maintained to reduce the risk of unauthorized access or use. Where possible, devices are configured to provide additional authentication, credential checks or secure interfaces, such as two-factor authentication.

4.3.2 Media disposal

When a storage device has reached the end of its useful life, Wandera and its providers use a decommissioning technique as described in DoD 2550.22-M or NIST 800-88.

If a device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry standard practices, thereby complying with the data remnants requirements.

4.4 Access control

Wandera uses a role-based access control approach in order to secure its data assets. The Wandera security team assigns limited access to data based on the specific role and duties of the employee in question. Wandera employs a number of authentication and authorization controls that are designed to protect against unauthorized access. Wandera assigns unique credentials to each employee. These credentials are used to authorize each person's activity on Wandera's network, including any access to customer data.

New joiners are provided access as documented on Wandera's new joiner form, which is then forwarded to the security team once all hiring processes have concluded.

At the end of a person's employment, their access to Wandera's network is immediately disabled and any associated permissions are retracted.

Where passwords or passphrases are employed for authentication (e.g. signing in to workstations), device management systems enforce Wandera's password policies, including password expiration, restrictions on password reuse, and sufficient password strength. Wandera makes widespread use of two-factor authentication mechanisms, such as certificates and one-time password generators. Third party applications using G Suite are also required to use two-factor authentication, which is regularly audited to ensure compliance across the entire business.

Wandera's security team is responsible for user access list reviews. This task is performed twice-yearly as a manual process where all users are reviewed to ensure that access rights match the user role. Access is granted according to the least privilege policy, whereby permissions are only given to assets required for the effective completion of the user's job and are revoked when no longer necessary.

4.4.1 Personnel security

Pre-employment screening by role takes place within Wandera. Upon employment, every staff member must sign a contract to confirm their compliance with the protection of confidentiality, integrity and availability of sensitive data and intellectual property.

Individuals requiring physical access to the Wandera premises must be identified, authorized and authenticated. This is achieved by identifying the roles that require both regular as well as occasional physical access and identifying the individuals that fill these roles. Standing authorization and a permanent authenticator are provided for individuals that require regular access.

Wandera also makes use of physical access logs to document the occurrence of external visitors, namely the date and time of arrival, name, reasons for access, name and title of authorizing individual and date and time of departure.

4.4.2 Physical and environmental security

Access to Wandera's offices is granted using uniquely identifiable smart cards that contain photo identification. Visitors must sign in at reception and security staff and video surveillance monitor the buildings 24/7.

Each service provider utilized by Wandera is carefully chosen to ensure the correct architectural and engineering approaches are taken with regards to security controls. These controls must include, but are not limited to, fire detection and suppression, uninterruptible power supply, climate and temperature control, preventive maintenance of operational equipment and storage device decommissioning.

4.5 Infrastructure security

Wandera's infrastructure follows the Security by Design[2] architectural model. The service is operated and maintained by Wandera, without the need for the customer to provide or host any hardware.

4.5.1 Network security

The Wandera network is constantly monitored for incidents and outages as well as risks and undergoes regular threat assessments to ensure data protection. Multiple internet backbone connections with DoS/DDoS mitigation tools provide routing redundancy and high-performance upstream provides network connectivity.

Dynamic firewalls and host-based intrusion detection systems protect the cloud infrastructure across all instances and applications. Regular vulnerability assessments and penetration tests are carried out across every host on the network, in order to maintain a consistent and complete assessment.

4.5.2 Application security

Service administration of Wandera is provided via the secure web portal RADAR, where administrators control the account settings of all Wandera users and can easily and securely configure policy settings. Granular access to the portal can be configured by Super Administrators, the highest level of administrators. Log ins as well as changes are recorded in the Audit Logs section. RADAR uses HTTP Strict Transport Security (HSTS) and certificate pinning technologies to ensure all end users are communicating via a secure, encrypted channel.

Wandera's mobile application is designed to allow for better visibility for end users and uses encryption while transferring data to and from the device. Profiles are delivered to mobile devices over an encrypted tunnel and signed from signed.wandera.com as the trusted source.

Web and application vulnerability assessments are factored into each release cycle, and new features go through extensive security testing both during and after development.

4.6 Systems and software development and maintenance

Wandera's systems are developed using established best practices, according to the OWASP framework. All Wandera developers must complete training on Wandera's coding best practices, and all code is written according to standard coding conventions. All code is subject to peer review and comprehensive unit tests before being committed.

The Chief Information Officer is accountable for maintaining the development environment to ensure that all intellectual property is protected and that the integrity, confidentiality and availability of the environment are maintained. The development environment is hosted in ISO 27001 certified public clouds. Access to the development environment is restricted to development staff. At no time can data be copied onto any device, which is not permanently connected to the development network.

Development devices have been built to ensure that the development network cannot be compromised or become available to employees outside the department. All development resources are password-protected, configured securely and maintained to reduce the risk of unauthorized access or use. Where possible, devices are also configured to provide additional authentication, credential checks or secure interfaces, such as two-factor authentication.

4.7 Systems and software monitoring

Wandera has created a 24/7 multi-layered systems monitoring system, based on both technical solutions and automatic triggers a well as manual checks and processes. These are regularly reviewed, and handled by Wandera's operations team, to ensure the solution is performing as expected, and to protect against any security risks.

Wandera has a detailed disaster recovery and business continuity plan (DRBC plan) that is circulated to all employees and kept in multiple federated cloud platforms to ensure it is always available in the event of emergency. This document is reviewed at least every 6 months by senior level management.

The DRBC describes precisely what constitutes a plan triggering event, whom to escalate to and how, as well as recovery plan invocation. It also includes procedures around dealing with all relevant parties in case of a data breach.

Specialized emergency response and disaster recovery teams have been outlined with a focus on establishing facilities for an emergency level of service, restoring key services and recovering to business as usual.

5 Privacy regulation considerations

Wandera has developed a solution for the global market and has optimized its product to meet the strongest of regulations. Many countries have data privacy regulations in place that may affect the installation of a solution such as Wandera. Wandera recommends seeking legal advice and following internal procedures before deploying Wandera.

5.1 European Union: General Data Protection Regulation (GDPR)

5.1.1 Wandera's service and EU GDPR

Wandera adheres to the European Union's General Data Protection Regulation which comes into force in May 2018.

The installation of the Wandera service falls under the GDPR's "Legitimate Interests". This regulation (article 6(1)(f)) gives the controller (customer) a lawful basis for processing under most circumstances when using Wandera. The use of the service does not require explicit consent from the individual end user to install the solution. Companies acting as controllers operating within the European Union are advised to undertake a Legitimate Interest Assessment[3] to ensure that they can install Wandera without requiring consent.

The end users have the right to transparency regarding the data collected by Wandera on behalf of their employer and have the right to object and ask for the reasoning behind the Legitimate Interests.

Wandera suggests giving end users access to a privacy notice tailored to the company's specific environment. A template notification can be found below:

> We process personal information using the Wandera service for legitimate business purposes, which include the following:
>
> - to identify and prevent fraud and protect company and personal data
> - to enhance the security of our network and information systems
> - to ensure compliance with our internal business policies regarding data that can be accessed on company devices
> - to avoid large and unexpected costs to the business due to excessive mobile data usage
>
> Whenever we process data for these purposes we will ensure that we always keep your Personal Data rights in high regard and take account of these rights. You have the right to object to this processing if you wish, and if you wish to do so please contact us. Please bear in mind that if you object this may affect our ability to carry out the tasks above for your benefit.

Wandera recommends consulting internal compliance and legal teams on these matters before proceeding with employee communications.

5.1.2 Right to be forgotten and data portability requests

Wandera's team has built the necessary technical capabilities and processes to deal with both right to be forgotten ("right to erasure") as well as data portability requests as per GDPR. If an end user within the organization requests for their data to be deleted, please contact Wandera at dataprivacy@wandera.com.

5.1.3 Wandera's internal adherence to GDPR

Aside from ensuring that its solution meets its customers' demand to comply with GDPR, Wandera itself is also an employer with employees within the European Union.

Wandera has completed its own extensive GDPR readiness review in respect of its own employee data and has taken the steps required to ensure its own compliance, including the updating of its employee terms and conditions, assessing what information is collected, and ensuring that data privacy is considered and prioritized at all times.

5.2 Australia: Notifiable Breaches Scheme

The Australian Notifiable Breaches Scheme (NDB) came into effect on the 22nd of February 2018. According to the NDB all Australian companies with a turnover of $3,000,000 AUD are required to notify their end users if any breaches occur.

Wandera is able to report on potential security risks and threats to assist with the establishment and analysis of such breaches. If a breach has indeed been found, the customer has the responsibility to notify their end users within 30 days. For more details, please refer to Australian Government – Office of the Australian Information Commissioner[4].

5.3 United States of America: HIPAA and PCI data regulations

The American Health Insurance Portability and Accountability Act (HIPAA) and the The Payment Card Industry Data Security Standard (PCI DSS) are two examples of industry-wide American data privacy. These were set up to ensure adequate security assessments and processes in their respective industries as they deal with particularly sensitive types of data.

Wandera provides an additional layer of security and visibility for mobile devices that can form an essential part of an enterprise's data security policy to help meet these industry standards.

6 Contact information

6.1 Data Protection Officer

Wandera has assigned a Data Protection Officer responsible for Wandera's compliance with GDPR and other data protection laws. Any enquiries for the Data Protection Officer can be sent to a Wandera representative, or by writing directly to dataprivacy@wandera.com.

6.2 Enquiries

For any enquiries related to this document, please get in touch using the following contact details:

- **Wandera Ltd.** 45 Mortimer Street, London, W1W 8HJ +44 (0) 203 301 2660
- **Wandera Inc.** 220 Sansome Street, Suite 1400, San Francisco, CA 94104 +1 (415) 935 3095
- **Wandera CZ S.R.O**. Lidická 2030/20, Černá Pole, 602 00, Brno, Czech Republic +420 538 890 059
- Via email at dataprivacy@wandera.com

7 Appendices

7.1 Appendix A: Data collection

7.1.1 Personal data | Access Key

The table below lists out Personal Information*** stored by Wandera.

Data collected		Access provided									
Name	More information	CA**	CSA	PA	WCS	WSE	WS	WP	WO	EMMC	SIEM
Access point MAC address	To assist network security threat investigations	X	X	X	X	X	X	X	X		X
Audit logs (RADAR)	Administrator log in and change events		X	X	X	X		X	X		
Device external ID	Acts as a unique identifier of the device	X	X	X	X	X	X	X	X	X	X
Device location country (e.g. Canada)	Wandera uses location services to extrapolate the country the device is located in	X	X	X	X	X	X	X	X	X	X
Device name**	Used as unique identifier	X	X	X	X	X	X	X	X	X	X
Domains accessed by device (e.g. youtube.com)	Gateway mode only. Wi-Fi only on +WiFi devices. Wandera does not collect further information regarding the specific domain such as the exact URL accessed. Certain types of domains, such as adult, are redacted from RADAR	X	X	X*	X	X	X*	X	X		
Email address**	Used as unique identifier	X	X	X	X	X	X	X	X	X	X
IMEI	Unique identifier tied to phone				X	X		X	X	X	
Mobile phone number	Used as identifier	X	X	X	X	X	X	X	X	X	
Proxy address and port	Gateway mode only				X	X		X	X		
Public IP address of the device (cellular)	To assist with identifying and categorizing the traffic from the device.	X	X	X	X	X	X	X	X		X
Public IP address of the device (Wi-Fi)	To assist with identifying and categorizing the traffic from the device.	X	X		X	X	X	X	X		X
Serial number	Device serial number	X	X	X	X	X	X	X	X	X	
Username in data usage reports**	Gateway mode only	X	X		X	X		X	X		
Username**	Used as unique identifier	X	X	X	X	X	X	X	X	X	X

**Pseudonymization applied*

***Optional pseudonymization available*

****Personal data according to GDPR. The definition according to the GDPR: Personal Data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

The following list describes the entities that have access to the data described below.

CA: Customer Administrators
CSA: Customer Super Administrators
PA: Partner Administrators (if Wandera solution was bought through a Wandera partner)
WCS: Wandera Customer Services department
WSE: Wandera Sales Engineering department
WS: Wandera Sales department
WP: Wandera Product department
WO: Wandera Operations department
EMM: Compatible EMM systems via EMM Connect, if enabled by the customer
SIEM: Compatible SIEM platforms, if enabled by the customer

7.1.2 Support cases – restricted access options

Support cases and bug tickets opened will be accessible by Wandera employees with the relevant permissions from various locations. Support cases are stored in Google's data centers across the world, as well as Salesforce's worldwide data centers. Wandera accepts support cases from any Wandera administrator, and the information contained within may include some of the personal information from the list above if relevant to the case.

On request, Wandera is able to restrict support access to either EU or US employees only.

7.1.3 Other data

Aside from the information that can be considered personal data as listed in section 7.1.1, Wandera collects certain other information in order to provide its customers with the services it provides. These are listed below. The access key can be found in section 7.1.2.

Data collected		Access provided									
Name	More information	CA**	CSA	PA	WCS	WSE	WS	WP	WO	EMMC	SIEM
Amount of data used by device	Gateway mode only. Wi-Fi collected for +WiFi devices only.	X	X	X	X	X	X	X	X		
Apple locale (e.g. English-US)	iOS only				X	X		X	X		
Applications installed	Used for App Insights report	X	X	X	X	X	X	X	X	X	
Battery percentage	Fast battery drain can indicate a security issue				X	X		X	X		
Blocked or allowed according to current policy	Gateway mode only	X	X	X*	X	X	X*	X	X		
Carrier detected (e.g. Vodafone, AT&T)	Used to apply correct APN modification	X	X	X	X	X	X	X	X	X	
Carrier mobile country code					X	X		X	X		
Carrier mobile network code					X	X		X	X		
Carrier name		X	X	X	X	X	X	X	X		
Current data policy: Wi-Fi, domestic, roaming	Gateway mode only				X	X		X	X		
Data Center in use					X	X		X	X		
Data amount used (upload and download) via gateway on cellular/Wi-Fi data	Gateway mode only. Wi-Fi collected for +WiFi devices	X	X	X	X	X	X	X	X		
Date and time accessed	Gateway mode only	X	X	X*	X	X	X*	X	X		
Developer Mode Enabled (enabled/disabled)		X	X	X	X	X	X	X	X	X	X
Device country and time zone	Alternative method to detect location				X	X		X	X		
Device currently charging (yes/no)					X	X		X	X		
Device lock screen enabled/disabled	Security risk purposes	X	X	X	X	X	X	X	X	X	X
Device model (Galaxy S8, iPhone 7 etc.)		X	X	X	X	X	X	X	X	X	X
Device OS		X	X	X	X	X	X	X	X	X	X
Device OS version		X	X	X	X	X	X	X	X	X	X
Device platform (iPhone, Android etc.)		X	X	X	X	X	X	X	X	X	X
Device type	Used as unique identifier	X	X	X	X	X	X	X	X	X	X
Device uptime					X	X		X	X		
DeviceStorageEncrypted (enabled/disabled)		X	X	X	X	X	X	X	X	X	X
Jailbreak status		X	X	X	X	X	X	X	X		X
Lower power mode enabled (enabled/disabled)					X	X		X	X		

Name	More information	CA**	CSA	PA	WCS	WSE	WS	WP	WO	EMMC	SIEM
Proxy installed (enabled/disabled)		X	X	X	X	X	X	X	X	X	X
Security Patches installed		X	X	X	X	X	X	X	X	X	X
Tethering active		X	X	X	X	X	X	X	X	X	X
Tethering session detected	Gateway mode only	X	X	X	X	X	X	X	X		X
Unknown Sources Enabled (enabled/disabled)	Allowing installation of software from unknown sources indicates a security risk.	X	X	X	X	X	X	X	X	X	X
USB App Verification Enabled (enabled/disabled)		X	X	X	X	X	X	X	X	X	X
USB Debugging Enabled (enabled/disabled)		X	X	X	X	X	X	X	X	X	X
User currently on Wi-Fi (enabled/disabled)		X	X	X	X	X	X	X	X	X	X
User currently roaming (enabled/disabled)		X	X	X	X	X	X	X	X	X	X
VPN active (enabled/disabled)					X	X		X	X		
Wandera app location services enabled	To detect misconfiguration	X	X	X	X	X	X	X	X		
Wandera app background refresh permissions enabled	To detect misconfiguration	X	X	X	X	X	X	X	X		
Wandera app push notification permissions enabled	To detect misconfiguration	X	X	X	X	X	X	X	X		
Wandera application version		X	X	X	X	X	X	X	X	X	
Wi-Fi auto join option enabled (enabled/disabled)					X	X		X	X		
Wi-Fi network SSID and encryption type	Collected for network security purposes	X	X	X	X	X	X	X	X		X
Wi-Fi signal strength					X	X		X	X		
WWAN enabled on device					X	X		X	X		

**Pseudonymization applied*

7.2 Appendix B: Data center locations

7.2.1 Locations

Wandera has deployed a global network of secure mobile gateways (proxies) for its customers using local ingresses. These data centers are subject to change depending on customer demand.

All data centers employ physical security, strict access policies and secure vaults and cages in line with the industry leading data center accreditations including SSAE16, SAS 70 Type II, ISO 27001, ISO 9001 and ISO 20000. The locations are listed below:

Europe

- London, United Kingdom
- Paris, France
- Frankfurt, Germany
- Biere, Germany
- Milan, Italy

Americas

- Palo Alto, California, United States
- Ashburn, Virginia, United States
- Dallas, Texas, United States
- Washington DC, United States
- Toronto, Ontario, Canada
- Sao Paulo, Brazil

Asia

- Hong Kong
- Tokyo, Japan
- Singapore

Australia

- Sydney, Australia

7.3 Appendix C: References

1: GDPR – Article 25: Data Protection by Design and by Default: https://gdpr-info.eu/art-25-gdpr/

2: GDPR – Article 25: Security by Design: https://gdpr-info.eu/art-25-gdpr/

3: Information Commissioner's Officer – Guide to Legitimate interests: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

4: Office of the Australian Information Commissioner: https://www.oaic.gov.au/