Privacy Policy Install App

Introduction

This is the privacy and security policy of M2M CLOUD LIMITED. Legal Name & Registered Office:

M2M CLOUD LIMITED
1 Stanyards Courtyard
Stanyards Farm
Chertsey Road
Chobham
Surrey
GU24 8JE
Company No. 06016849

The purpose of this document is to tell you how we process data from in accordance with any service provisioned from M2M CLOUD LIMITED or via a reselling party.

In particular what this Privacy Policy will address:

What data we collect and store.
How we use it.
How we protect it.
To whom we disclose it.

We agree not to process data other than in accordance with this policy. We may vary this policy. If you have any queries concerning this policy, please contact your reseller or contact us directly on hello@m2mcloud.com.

What data do we collect and store?

The purpose of our solutions is to track vehicles using telematic devices. We therefore collect, process and store Vehicle, Telematics Device and User related data.

Vehicle Data

When a vehicle is registered we store:

- Vehicle ignition on/off.

Telematic Device Data

When a telematic device is registered and active we store:

- GPS Location Data from telematics units fitted to vehicles.
- Serial number of the telematics device.
- ICC (Sim number) of the telematics device.
- MSISDN (telephone number) related to the ICC (Sim number).
- Model of the telematics device.

User Data

When a user is registered we store:

- IP address.
- Browser type.
- Cookies.

How do we use this data?

We use this Vehicle, Telematics Device and User data to:

- Install a telematics device.

Vehicle Data

We use:

- Vehicle ignition on/off to verify the install.

Telematic Device Data

We use:

- GPS Location Data to verify the install.
- Radio Location Data to provide location services.
- Serial number of the telematics device for identity.
- ICC (Sim number) of the telematics device for billing.
- MSISDN (telephone number) related to the ICC (Sim number) for command and control.
- Model of the telematics device for management.

User Data

We use:

- IP address is used for auditing, to enhance security logging and improve threat detection.
- Browser type to apply styling.

Other User Data considerations:

- We use cookies to provide a more personalized and user-friendly visit to our website and to help us track user traffic patterns, store customer web application related configuration information. A cookie cannot read your hard disk or other cookie files. Usually you can modify the settings of your browser to accept or reject all cookies or as an alternative to be notified when a cookie is set.

- We may use User Data to send you important notices concerning our services. We do not routinely access User Data for other purposes. However, we may do so in exceptional circumstances, meaning where:

    - We consider in our discretion that it breaches acceptable usage.

    - It is necessary to protect us or our other customers or the public and/or to minimize our exposure to breach of regulation or the risk of civil or criminal proceedings and/or to respond to claims of violation of third party rights.

    - We are required to by Regulation or competent authority.

    - We are required to debug a device or web application problem.

How do we protect data?

- Security is a high priority. We take reasonable precautions to protect data from loss, misuse, unauthorised access or disclosure, alteration or destruction.

- Passwords are encrypted using Salted Password Hashing standards as set out in [RFC 8018] (https://tools.ietf.org/html/rfc8018) with a higher than recommended iteration count.

- Production system administrative access is limited to key staff.

- Data is protected physically by security card and biometric access and NVR camera systems at our various datacentres.

- System integration data (API communication) protected by TLS (Transport Layer Security) / SSL (Secure Sockets Layer).

To whom do we disclose data?

We may disclose data so far as reasonably necessary:

- To provide our services to a reseller.
- When there are Exceptional Circumstances.
- In the context of a sale or merger of all or part of our business.
- To law enforcement to provide recovery assistance.
- We are required to by Regulation or competent authority.

We may disclose vehicle data to organizations with which we have a business relationship for the purpose of system integrations (API communications) or product features.

How can you access and rectify data?

- You can access and rectify Vehicle Data by contacting us via your reseller.
- You can access and rectify Telematics Device data by contacting us via your reseller.
- For information about your rights under UK data protection laws, see the website of the UK Data Protection Commissioner.

Data Retention

- Data is retained on M2M CLOUD LIMITED solutions until a device is unallocated from a Customer Account. A device is unallocated from a Customer Account when a customer terminated the service with a partner of M2M CLOUD.

  When a device is unallocated data is deleted. The times it takes to remove this data varies depending on the volume collected while the device was allocated to a Customer Account.