2025

MINT Data Policy 2025

VERSION 1.2
03/2025
EN

Table of Contents

1 Table of Revisions

Date	Version	Description of Changes	Status	Author
01-01-2025	0.1	Draft	Internal	Frederik Leempoels
13-01-2025	1.0	1st Review	Internal	Frederik Leempoels
15-01-2025	1.1	2nd Review	Internal	Frederik Leempoels
19-03-2025	1.2	3rd Review	Released	Frederik Leempoels

2 Disclaimer

Even if Phoenix Contact takes every precaution to ensure that the content of this Data Policy is both accurate and complete, unintentional errors can occur. In addition, given the continuously evolving nature of legislation, rules and regulation, there may be delays, omissions or inaccuracies in the information contained in this Data Policy. Phoenix Contact is not responsible for such errors, delays, omissions or inaccuracies, nor for the consequences resulting from its use.

3 Contact Information

For questions or concerns related to this MINT Data Policy, contact Phoenix Contact at info@phoenixcontact.be.

4 Policy Changes

Phoenix Contact reserves the right to make changes to this MINT Data Policy. All versions will be documented in the table of revisions. MINT Customers will be notified of changes to this MINT Data Policy via e-mail.

5 Definitions

For the purposes of this MINT Data Policy document the following definitions shall apply:

“Capacity” a smart parking and electric vehicle platform for complex business environments, provided by Cegeka;

“Customer” the legal entity purchasing the MINT System;

“Data Processing” any operation or set of operations which is performed on data or on sets of data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

“MyCapacity” an app that enables authorised users to start and stop EV charging sessions and securely enter their parking location. The app is provided by Cegeka and works for all locations that the driver has access to;

“Personal Data” any information relating to an identified or identifiable natural person (“Data Subject”); 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;

6 Purpose

This MINT Data Policy document defines how data is managed in the MINT System of Phoenix Contact, ensuring transparency, privacy and security in data handling, while complying with relevant legal and regulatory frameworks. The purpose of this policy is to define the types of data collected by the MINT System and explain how this data is used, stored, shared and secured. This document also aims to inform MINT System users about their rights, to ensure transparency, and to reinforce the commitment of Phoenix Contact to safeguarding personal and organisational information.

7 Scope

The MINT System[1] consists of two components, on the one hand the MINT Controller located at the Customer premises, managing local energy assets, and on the other hand the MINT Platform with the MINT DataHub providing access to a variety of MINT services (Figure 1).

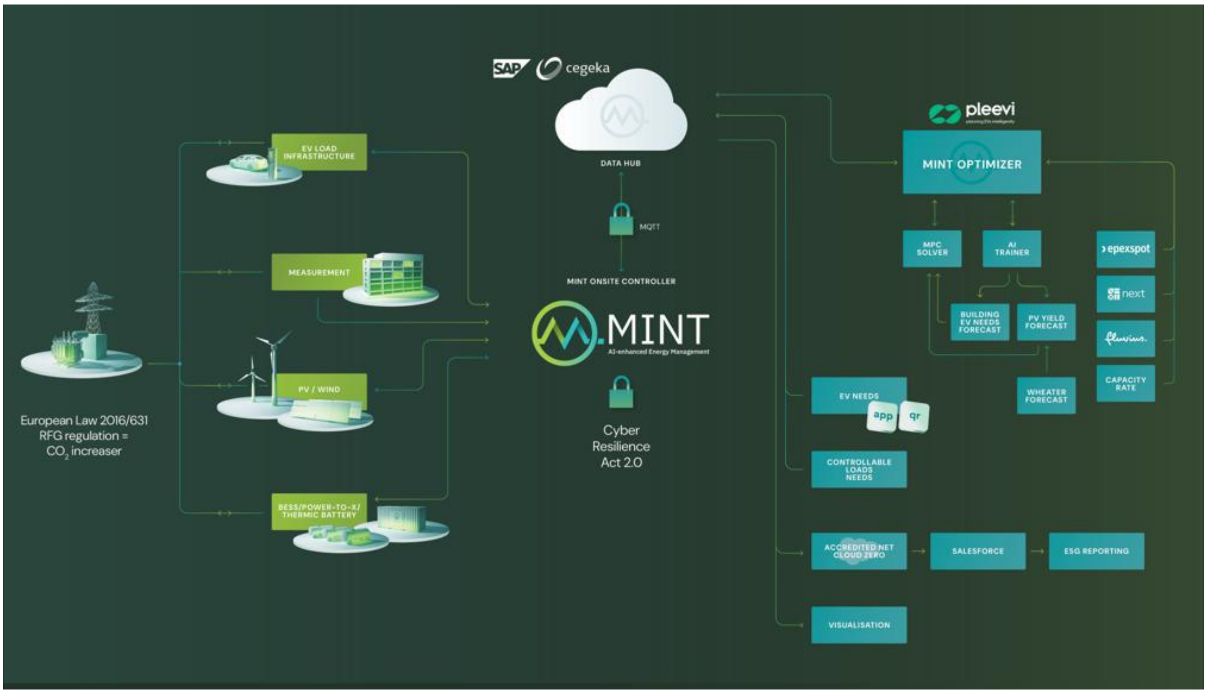

Figure 1 - MINT ecosystem

The local MINT Controller includes a DataGateway that connects to the MINT DataHub through a secured MQTT communication program. The MINT DataHub is part of the MINT Platform and enables a range of services offered by Phoenix Contact (accessible via the MINT Portal, such as user management, site management, driver pool management, dashboard

[1] More detailed information on the MINT System is available in MINT_E-book_EN.pdf.

and reporting functionalities) and/or external service providers (such as the Pleevi Platform for AI-based energy optimisation, or the Capacity Platform of Cegeka for smart EV charging).

This MINT Data Policy applies to all data collected, processed and stored within the MINT System.

8 Policy baseline

The MINT Data Policy is based on the principle that a MINT Customer is and remains owner of its own data. The MINT System uses data exclusively to **fulfil its role as an energy management system in the interest of the Customer, distributing available energy over time, while taking into account different user needs and dynamic prices, maximising the use of locally produced and renewable energy, limiting peak consumption and avoiding power outages**. Even when MINT data is shared with external systems, it is for no other purpose than to contribute to the role of the MINT System as defined above.

The following sections provide more specific details on the applicable data policy for each of the MINT System components.

9 The MINT Controller

The MINT Controller is the local PLC controller that integrates and manages all energy assets of the Customer in real-time. Energy assets include solar panels, wind turbines, CHP units, charging stations, BESS, thermal ESS, heat pumps, e-boilers, as well as the connection with the power grid. The MINT Controller always remains in charge of the Customer's energy management and ensures that energy flows are never interrupted. It is the MINT Controller that ultimately sends the commands to all energy assets of the Customer.

9.1 Data collection

The MINT Controller collects the following types of data:

- Measurement Data
- Personal Data
- System Data

9.2 Data usage

Measurement Data covers all locally measured data coming from energy meters, charging points, batteries, solar panels, … i.e. technical data made available by all local energy assets. Measurement Data is used locally in the MINT Core PLC program to allocate power to controllable assets, to perform proactive and reactive peak shaving, to protect fuses and to ensure that all systems continue to operate.

In the MINT Advanced solution, the local MINT Controller can also collect **Personal Data** in the form of a driver RFID badge number or a unique identification number (UID or EVI) which is the MAC-Address of the vehicle provided by the local charger, and send it to the MINT DataHub to identify the corresponding user profile and start a smart charging session.

Finally, the MINT Controller collects and uses internal **System Data** to ensure its own operation, such as system settings, PLC settings, boot messages, system health/alerts and maintenance logs.

9.3 Data storage

The local MINT Controller does not store data, it only runs the MINT Core PLC program.

9.4 Data sharing and protection

The MINT Core PLC program shares data exclusively with the MINT DataHub. This is done via the DataGateway of the MINT Controller, which is running an MQTT communication program with firewall protection. The communication itself is secured by a certificate that needs to be installed in the MINT Controller as part of the configuration of the MQTT driver program.

Minimum firewall settings to be applied:

- MQTT Data: in and outgoing data
- Port number: 8883
- Endpoint URL: iot-mint-Production.azure-devices.net

10 The MINT Platform

The MINT Platform includes all services provided by Phoenix Contact and, in case of MINT Advanced, related third party service providers.

10.1 The MINT DataHub

The MINT DataHub is MINT’s central data exchange and storage unit, which exchanges data between all on-site MINT Controllers on the one hand, and the MINT Platform and/or external service providers on the other hand.

10.1.1 Data collection and usage

The MINT DataHub handles all incoming and outgoing data from the MINT Controllers, as well as the set-up of the connections to the on-site clients, i.e. the DataGateway in each local MINT Controller. Furthermore the MINT DataHub is the location where all data related to the Customer's MINT System is stored, including configuration data, measurement data, system data, dashboard and reporting data, and in some cases also Personal Data (of individual EV drivers). The MINT DataHub is hosted in a separate *Microsoft Azure* environment, on servers located in Germany.

10.1.2 Data storage

The following is an overview of all types of data storage in the MINT DataHub:

1. Azure Blob Storage
    - Data stored: user profiles, raw PLC messages
    - Expires: never
    - Opt-in/out: no
    - Security: encrypted, protected by Azure RBAC rules

2. Azure Table Storage
    - Data stored: EV driver data, EV charging session data, site and asset details
    - Expires: never / after 30 days (for EV driver and EV charging session data)
    - Opt-in/out: no
    - Security: encrypted, protected by Azure RBAC rules

3. Azure App Insights
    - Data stored: MINT Portal access and error logs, incoming and outgoing API traces, visitor portal traces, Pleevi traces, OCPP traces
    - Expires: after 90 days
    - Opt-in/out: no
    - Security: encrypted, protected by Azure RBAC rules

4. Azure Data Explorer (ADX)
    - Data stored: energy reports, advices, charge transactions
    - Expires: never
    - Opt-in/out: yes
    - Security: encrypted, protected by Azure RBAC rules

10.1.3 Data sharing and protection

The DataGateway of the local MINT Controller connects with the MINT DataHub via the *Azure IoT Hub* using unique credentials and trust certificates placed on the local MINT Controller. A shared access signature (SAS) is used to provide secure delegated access to resources in the MINT DataHub. The SAS is never stored and is generated via the MINT Portal only with the correct user rights.

strCredentials.sClientId:=	Client_location_site_controller
strCredentials.sHost:=	iot-mint-Production.azure-devices.net
strCredentials.sPort:=	8883
strCredentials.sUserName:=	iot-mint-Production.azure-devices.net/Client_location_site_controller/?api-version=2021-04-12
strCredentials.sPassword:=	SharedAccessSignature

10.2 The MINT Portal

The MINT Portal is a front-end application allowing MINT Customers to manage their complete MINT System. The MINT Portal is accessible via login credentials and includes:

10.2.1User management

The MINT Portal provides user management functionality which allows a MINT Customer (administrator) to configure different user levels supporting multiple users, each having access to specific data and user rights via individual credentials. The user management in the MINT Portal is GDPR compliant. User management data is confidential and only accessible by the Customer's administrator(s).

10.2.2Site management

The site management part of the MINT Portal allows the MINT Customers to manage all the necessary settings to connect, monitor and maintain their local on-site MINT installations. MINT site management allows to import site details using the site configuration tool, manage MINT Controllers, check which data connections are active, etc. Site management data contains no Personal Data and access is restricted to users authorised by the MINT Customer.

10.2.3Dashboarding

A centralised dashboard allows users to visualise and monitor energy flows of several MINT sites at the same time. A number of default dashboard templates are available, which automatically collect and visualise information based on the MINT site structure drawn in the MINT site configuration tool. The MINT dashboard contains only technical and performance related data. Access is restricted to users authorised by the MINT Customer.

10.2.4Reporting

The MINT reporting tool analyses historical data and delivers a report in which CO_2 reduction, price shifting and peak shaving results are documented in a human readable and printable format. The MINT reporting tool provides only technical and performance related data. Access is restricted to users authorised by the MINT Customer.

10.3 MINT Advanced

MINT Advanced is an AI layer on top of the MINT Core PLC program to further optimise energy management. MINT Advanced aims to optimise comfort for all end-users, such as for EV drivers who can specify their individual preferences for EV charging. Moreover, as the AI learns from consumption patterns, it will become increasingly precise.

10.3.1 MINT Optimiser

The MINT Optimiser is an external AI service provided by Pleevi that receives measurement data from the MINT Controllers. Using additional information such as dynamic energy prices, weather forecasts, building load forecasts, grid connection constraints, grid peak penalties and user patterns/preferences, it advises the local MINT Controller(s) how to match demand and supply in the most economical and ecological way. For now the MINT Optimiser is limited to EVs and stationary batteries, but it can be extended to optimise all controllable electrical assets.

10.3.2 Smart EV charging

In particular, the Pleevi AI service is used to optimise EV charging on MINT controlled charging points, taking into account each EV driver's individual parking duration and requested km-range to be charged. MINT provides two options to enable this service:

1. Charging by scanning a **QR code** on the charging point. The QR code then redirects the EV driver to a visitor portal of the MINT Platform, where parking duration and requested km-range to be charged can be specified and managed for the charging session without sharing any Personal Data, i.e. anonymous charging. The QR code is generated in the MINT Portal and is linked to the equipment ID of the charging point in the MINT System.

2. Charging by using an **RFID badge** to identify the EV driver. For this case MINT works with the Capacity Platform of Cegeka, including the related MyCapacity smartphone app. In order to enable MINT controlled smart charging, eligible EV drivers and their associated RFID badges are registered and managed via the MINT Portal. The RFID badge will identify the EV driver to activate the MyCapacity app on their smartphone, and allow them to specify and manage parking duration and requested km-range to be charged via a MINT extension in the MyCapacity app. As this method involves Personal Data, it is subject to the GDPR.

11 GDPR and Personal Data

This part describes the different aspects of MINT in relation to GDPR rules and regulations. In general, GDPR applies only to the parts of MINT where Personal Data is involved, i.e. the pool of EV drivers that are registered to make use of the MINT Optimiser services.

11.1 Different roles

GDPR defines the following roles:

- Data Subject: an EV driver whose name, e-mail address and RFID badge is registered in MINT
- Data Controller: the MINT Customer, which determines the purpose (why) and means (how) of the processing of EV driver Personal Data; the Data Controller bears the end responsibility for GDPR compliance.
- Data Processor: the MINT System as well as the Capacity Platform, which process EV driver Personal Data on behalf of the MINT Customer.

GDPR requires a data processing agreement to be in place between the Data Controller and the Data Processor(s). The data processing agreement between the MINT Customer (as Data Controller) and the MINT Platform (as Data Processor) is included in the MINT service contract between Phoenix Contact and its MINT Customers, whereas the data processing agreement between the MINT Platform and the Capacity Platform is part of the MINT-related cooperation agreement between Phoenix Contact and Cegeka.

11.2 Personal Data

Via the MINT Portal, the MINT Customer can register a list of EV drivers that have RFID access to EV charging infrastructure managed by its MINT System(s). This list is not stored in the MINT DataHub, but is an API to the Capacity Platform of Cegeka.

When registering an EV driver via the MINT Portal, the MINT Customer (or, if authorised as a portal user, the EV driver directly) can add the following Personal Data in the Capacity Platform:

• First Name	- Mandatory
• Last Name	- Mandatory
• Contact Phone	- Optional
• Contact e-mail	- Mandatory
• Country code	- Optional
• License plate	- Optional

- Access granted from - Optional
- Ends at - Optional
- RFID badge - Mandatory

The MINT Optimiser can operate with only the mandatory data fields. In order to be GDPR compliant, the MINT Customer shall always inform the EV driver which (mandatory and optional) Personal Data is shared via the MINT Portal with the Capacity Platform.

11.3 Privacy settings

When a MINT Customer is granted access to Cegeka's Capacity Platform, part of the onboarding process is to determine which Personal Data will be shared. The MINT Customer is free to provide mandatory and optional information, for which the following privacy settings are specified in the Capacity Platform:

- Data storage policy this informs the admin for what period the charging data is being stored in the Capacity Platform (6 months). After this period, all Personal Data will be anonymised, so the charging sessions can still be used for analytics. This is not a setting the MINT Customer can configure.

- Shared data this Personal Data is mandatory to provide the smart parking services to the registered EV driver. This is not a setting for MINT Customer to configure.

- Shared data (optional) these data fields are optional, the MINT System can operate without them, but it makes certain scenarios easier if the info is shared. This can be configured per item by the MINT Customer.

A MINT Customer can only search for the details of a specific EV driver in the Capacity Platform. The MINT Customer can never see a complete overview of all EV drivers who have ever used MINT-controlled charging points (privacy by design). Depending on the privacy settings, the MINT Customer can find a complete or limited view when searching on a specific EV driver name, e-mail address or RFID badge.

11.4 Data Subject rights

According to GDPR the Data Subject (registered EV driver) has certain rights. These are not limited to the ones described in this section, but these are the relevant rights for MINT.

11.4.1 Right of access

The registered EV driver has the right to obtain insights in the Personal Data being processed by the Data Controller, i.e. the MINT Customer. In practice, when a registered EV driver wants to obtain these details, a request can be made towards the MINT Customer. In that case, the MINT Customer can use the MINT Portal to get the required insights from the Capacity Platform.

11.4.2 Right to rectification

When the registered EV driver notices inaccurate Personal Data being stored, he/she/x has the right to rectification. In essence, as registering the Personal Data is the responsibility of the MINT Customer via the MINT Portal, it can be corrected by the MINT Customer directly as well.

11.4.3 Right to erasure (right to be forgotten)

The registered EV driver has the right to erasure of all Personal Data that is stored. Again, a request can be made towards the MINT Customer, who in turn shall request Cegeka to remove the Personal Data from the Capacity Platform. As a consequence however, the EV driver can no longer use the parking services provided by the Capacity Platform.

12 Data sharing and protection

The MINT Platform shares data with the following external parties:

12.1 Auth0

the MINT Platform uses Auth0 as an external user authentication service allowing users to securely log in to the MINT Portal. It provides user authentication and enables user management, distinguishing different user levels that can be specified and managed in the MINT Portal, to ensure that users can only access resources they are authorised for. Auth0 meets various compliance frameworks and certifications, including GDPR, ensuring that the MINT API security practices adhere to industry standards.

Characteristics

- Mandatory login service
- Data forwarded: personal information portal
- Expires: never
- Opt-in/out: no
- Security: see Auth0 data policy (www.auth0.com)

12.2 Pleevi

The MINT Platform relies on Pleevi to provide a smart charging solution for EVs, that optimises the available demand and supply in the most economical and ecological way. Using AI technology, Pleevi generates an optimised charging profile for all charging points in the Customer's MINT architecture, by taking into account the EV driver's parking duration and requested km-range to be charged, local energy sources such as stationary batteries, solar energy forecasts, building load forecasts, connection constraints, grid peak penalties and dynamic energy prices.

Characteristics

- Optional licensed service
- Data forwarded: site energy reports, charging transactions
- Expires: never
- Opt-in/out: yes
- Pleevi APIs
  - Site management API
  - Planning API
  - Insights & Benefits API
- Security: see Pleevi data policy (www.pleevi.ai)

12.3 Capacity

The Capacity Platform is a GDPR-compliant, hardware agnostic smart parking and EV platform for complex business environments, provided by Cegeka. It is linked to the MINT Platform via a platform-to-platform connection, allowing an integrated approach to EV charging, including charging point reservations, charging notifications, EV arrival/departure time and requested km-range to be charged for all charging sessions in which the user is identified as a MINT user (via RFID badge). For these users, MINT Advanced will generate an optimised charging session, taking into account their arrival/departure time and requested km-range to be charged, along with other parameters.

Characteristics

- Optional licensed service
- Data forwarded: driver data (GDPR)
- Expires: never
- Opt-in/out: yes
- Security: see Capacity data policy (www.cegeka.com/en/solutions/products-platforms/capacity)

12.4 DSO/TSO

Electricity costs are not the only interest of the MINT Customer, stability and continuity of electricity supply are even more crucial. This is a responsibility of the local DSO and TSO. Therefore, irrespective of the MINT Customer's electricity provider, aggregated and anonymised MINT data can also be made available to the local DSO and TSO in order to, on the one hand, get (real-time and forecast) information on electricity production and consumption directly from MINT Systems distributed over their local, regional and/or national grid, and on the other hand, ensure stability and continuity of supply on the same local, regional and/or national grid.

In exceptional circumstances where stability and continuity of supply are ultimately at stake, e.g. due to a threat of imminent local congestion (at DSO level) or a threat of ultimate imbalance (at DSO and/or TSO level) that cannot be remedied by flexibility services providers (FSP) or balancing services providers (BSP), it is possible to use the MINT Systems that would otherwise suffer a power outage to temporarily adjust electricity production or consumption, while maximally respecting the MINT Customer's priorities and leaving the MINT Customer's comfort minimally or not affected.

For this interaction between the MINT Platform and the local DSO/TSO, Phoenix Contact cooperates with iSea as a trusted third party implementing and operating an intermediate (critical) technical data exchange that

(i) aggregates relevant MINT data on local, regional and/or national grid level,

(ii) shares the aggregated MINT data with the involved DSO/TSO, directly and/or indirectly (via involved FSPs, BSPs or BRPs), and

(iii) contributes to stability and continuity of supply in critical cases of emergency, by triggering the involved MINT Systems to temporarily adjust electricity production or consumption.

Characteristics

- Mandatory data interface
- Data forwarded: aggregated and anonymised energy reports
- Expires: never
- Opt-in/out: no
- Security: this info is classified (critical infrastructure)

13 Company data

- Auth0, Inc. is a limited liability company incorporated and existing under the jurisdiction of the state of Delaware, United States, with company number 5467370 and registered address at 10900 NE 8th Street, Suite 700, Bellevue, WA 98004, United States, in this document referred to as "**Auth0**".

- Cegeka NV is a limited liability company incorporated and existing under the laws of Belgium, with registered office at Kempische steenweg 307, 3500 Hasselt, Belgium, and company number 0882.419.490, in this document referred to as "**Cegeka**".
- iSea NV is a limited liability company incorporated and existing under the laws of Belgium, with registered office at Koningsstraat 154-158, 1000 Brussels, Belgium, and company number 0507.587.934, in this document referred to as "**iSea**".
- Phoenix Contact NV is a limited liability company incorporated and existing under the laws of Belgium, with registered office at Minervastraat 10-12, 1930 Zaventem, Belgium, and company number 0407.736.629, in this document referred to as "**Phoenix Contact**".
- Pleevi BV is a limited liability company incorporated and existing under the laws of Belgium, with registered office at Koning Albert II-laan 4, 1000 Brussels, Belgium, and company number 1017.187.332, in this document referred to as "**Pleevi**".

14 Abbreviations

ADX	Azure Data Explorer
AI	Artificial Intelligence
API	Application Programming Interface
BESS	Battery Energy Storage Systems
BRP	Balancing Responsible Party
BSP	Balancing Service Provider
CHP	Combined Heat and Power
DSO	Distribution System Operator
ESS	Energy Storage Systems
EV	Electric Vehicle
EVI	Electronic Vehicle Identification
FSP	Flexibility Services Provider
GDPR	Global Data Protection Regulation
MQTT	MQ Telemetry Transport
OCPP	Open Charge Point Protocol
PLC	Programmable Logic Controller
PV	Photovoltaic
RBAC	Role Based Access Control
RFID	Radio-frequency identification

SaaS	Software as a Service
SQL	Structured Query Language
TSO	Transmission System Operator
UID	Unique Identifier
VIN	Vehicle Identification Number