Electric Vehicle (Smart Charge Points) Regulations 2021

Technical File (updated for Schedule 1 – Security)

Daniel Hollingworth

1st December 2022

Ohme Technologies Ltd, Unit 74, Penrose Wharf, Penrose Quay, Cork T23 HF51

www.ohme-ev.com

Registered in Ireland number 619562

1. Introduction

This document contains information describing the technical solutions adopted to comply with the Electric Vehicles (Smart Charge Points) Regulations 2021, herein referred to as the "Regulations".

This is provided to assist sellers of Ohme products to meet the requirements of Regulation 13, which requires the seller to have a technical file for any relevant charge point that they sell, and to supply a copy of the technical file to any purchaser on request.

This document applies to the following Ohme products:

Product Family	Product Code	Description
Ohme Home Pro	OHME0002GB002	Home Pro Type 2 (5 metre)
	OHME0002GB002-8M	Home Pro Type 2 (8 metre)
Ohme ePod	OHMEX1GB003	Ohme ePod Type 2 socket

Other versions of Ohme products (e.g. Ohme Home and Go) are not covered by this document.

This document only applies to the above products sold by Ohme Operations UK Ltd in Great Britain, it does not apply to products sold to other countries, including Northern Ireland.

Version History

Version	Date	Notes
v1.0	30th June 2022	Initial release
V2.0	1st December 2022	Included compliance with Schedule 1 Included Ohme ePod in scope of document

2. Achieving compliance with Ohme products

Ohme's service consists of three aspects: the Ohme app, the Ohme backend and Ohme hardware.

The products above are compliant with the Regulations (**excluding** Schedule 1: Security) where:

- The Ohme app is installed after 30th June 2022, or an existing app has been updated since this date
- The Ohme hardware is installed after 30th June 2022 and connected to the internet (allowing Ohme to update the firmware if the unit is running a pre-compliance version), see section 5.

Ohme products are fully compliant with the Regulations (**including** Schedule 1: Security) where:

- The Ohme app is installed after 30th November 2022, or an existing app has been updated since this date
- The Ohme hardware was shipped by Ohme after 30th November 2022

For units purchased indirectly (e.g. through wholesalers) during the transition period, the Statement of Compliance provided in the box will confirm the compliance status. Otherwise, contact Ohme customer services at help@ohme-ev.com for any queries.

Note that all ePod units are fully compliant with the Regulations, include Schedule 1: Security.

3. Product Description

3.1 Ohme Home Pro (GB002 products)

The Ohme Home Pro devices on the market in Great Britain are mainly intended for the charging of electric vehicles in domestic settings. The units may be used in workplace settings but are not intended as public charging devices.

The Ohme Home Pro is an electric vehicle charging device, with:

- Input cable for connection to a power supply
- Charging unit, including:
    - Integrated residual current protection device
    - PEN fault detector
    - Integrated GSM modem and SIM card
    - Colour LCD screen
    - Three touch sensitive switches
- Tethered charging cable, with Type 2 IEC62196 connector
- Current measurement clamp, used for limiting the property maximum demand (automatic load balancing)
- Wall mounting accessories and cable holder

The charger is to be used with a single-phase electricity supply.

They are fixed charging units primarily complying with product standard BS EN IEC 61851-1:2019 Electric vehicle conductive charging system, General requirements.

Figure 1 – Ohme Home Pro installed

Controlling the operation of the product is through either a smartphone app or via buttons and the LCD TFT colour screen on the unit. This allows charging to be scheduled in line with dynamic energy tariffs or forecasts of the carbon intensity of electricity generation.

3.1.1 Firmware

The firmware on Ohme Home Pro units is updated automatically with no user interaction needed. Updates are pushed to the unit from the Ohme backend servers and once downloaded, they are installed either by rebooting the unit, by cycling the power or at a quiet time when the product is unplugged from a vehicle.

It is not possible for installers or users to select which firmware runs on the product. As Ohme controls the firmware version on its products, Ohme warrants that all chargers described in this document are compliant with the Regulations. It is not necessary for re-sellers of Ohme products to maintain separate registers of firmware version.

The display on Home Pro units (Info screen) indicates the firmware version running. Any version higher than v1.18 is compliant with the Regulations (excluding Schedule 1 – Security) and v1.31 (including Schedule 1 – Security).

3.1.2 Specification

The main specification of the Home Pro devices are as follows:

Voltage	**230 V AC**
Frequency	50 Hz
Max Current, Power Output	32 A, 7.4 kW
Operating Temperature	-25 ^{o}C to 45 ^{o}C
Storage Temperature	-40 ^{o}C to 85 ^{o}C
Cable length (output to vehicle)	5 metres
Cable length (input, supply)	1 metre
Residual current function	Type A 30 mA DC 6 mA
PEN fault detection	Conforms to 722.411.4.1 (iv) of BS7671 18th edition
Overcurrent protection	None
Ingress protection	IP55
Communications	2G/3G/4G GSM data
Shipping weight	5.3 kg
Colour	Black

3.1.3 Product Manual

The product manual is available on the Ohme website in the Resources section and is provided in print form in the box.

3.2 Ohme ePod (GB003 products)

The Ohme ePod devices on the market in Great Britain are mainly intended for the charging of electric vehicles in domestic settings. The units may be used in workplace settings but are not intended as public charging devices.

The Ohme ePod is an electric vehicle charging device, with:

- Type 2 IEC62196 socket
- Charging control unit, including:
    - Integrated residual current protection device
    - PEN fault detector
    - Integrated GSM modem and SIM card
    - Three touch sensitive switches
- Current measurement clamp, used for limiting the property maximum demand (automatic load balancing)
- Wall mounting accessories

The charger is to be used with a single-phase electricity supply.

They are fixed charging units primarily complying with product standard BS EN IEC 61851-1:2019 Electric vehicle conductive charging system, General requirements.

Figure 2 – Ohme EPod

Controlling the operation of the product is through either a smartphone app or via three touch sensitive buttons on the front of the unit. This allows charging to be scheduled in line with dynamic energy tariffs or forecasts of the carbon intensity of electricity generation.

3.2.1 Firmware

The firmware on Ohme ePod units is updated automatically with no user interaction needed. Updates are pushed to the unit from the Ohme backend servers and once downloaded, they are

installed either by rebooting the unit, by cycling the power or at a quiet time when the product is unplugged from a vehicle.

It is not possible for installers or users to select which firmware runs on the product. As Ohme controls the firmware version on its products, Ohme warrants that all chargers described in this document are compliant with the Regulations. It is not necessary for re-sellers of Ohme products to maintain separate registers of firmware version.

The installer portal (a web app for use by installers) indicates the firmware version running. Any version higher than v1.31 is compliant with the Regulations (including Schedule 1 – Security).

3.2.2 Specification

The main specification of Ohme ePod devices are as follows:

Voltage	**230 V AC**
Frequency	50 Hz
Max Current, Power Output	32 A, 7.4 kW
Operating Temperature	-25 ^{o}C to 50 ^{o}C
Storage Temperature	-40 ^{o}C to 85 ^{o}C
Cable length (output to vehicle)	N/A (untethered)
Cable length (input, supply)	N/A (wired direct at installation)
Residual current function	Type A 30 mA DC 6 mA
PEN fault detection	Conforms to 722.411.4.1 (iv) of BS7671 18th edition
Overcurrent protection	None
Ingress protection	IP54
Communications	2G/3G/4G GSM data
Shipping weight	1.8 kg
Colour	Black

3.2.3 Product Manual

The product manual is available on the Ohme website in the Resources section and is provided in print form in the box.

4. Solutions Adopted for Compliance

4.1 Smart Functionality

Requirement	Technical solution adopted to meet the requirement
Charge point is able to send and receive information via a communications network	All Ohme units have communications capability via a GSM modem and SIM card. Units are pre-configured at the factory to communicate with Ohme servers without further user configuration.
Charge point is able to respond to signals or other information received by it by: • Increasing or decreasing the rate of electricity flowing through the charge point • Changing the time at which electricity flows through the charge point	All Ohme units use OCPP1.6 JSON to accept charging schedules based on user preferences. These schedules change the charging time and increase and decrease the charging rate.
Charge point is capable of using this functionality to provide demand side response services, including response DSR services	The charge schedules in Ohme units can be updated in real time to start charging, stop charging or alter the rate of charging in line with products or commercial arrangements that we may have with the energy industry.
Charge point has at least one user interface, incorporated in the charge point or otherwise made available to the owner	Ohme units are coupled with a smartphone app which is paired to the charger. This allows the charge point to be controlled by the user. Ohme units also have limited user functions available at the charge point through switches/buttons.

4.2 Energy supplier interoperability

Requirement	Technical solution adopted to meet the requirement
Charge point is configured such that is will not cease to have smart functionality if the owner changes their electricity supplier	Ohme units are independent of energy suppliers. The user has the ability, through the smartphone app, to configure their suppler and tariff details (or make up their own).

4.3 Loss of communications network access

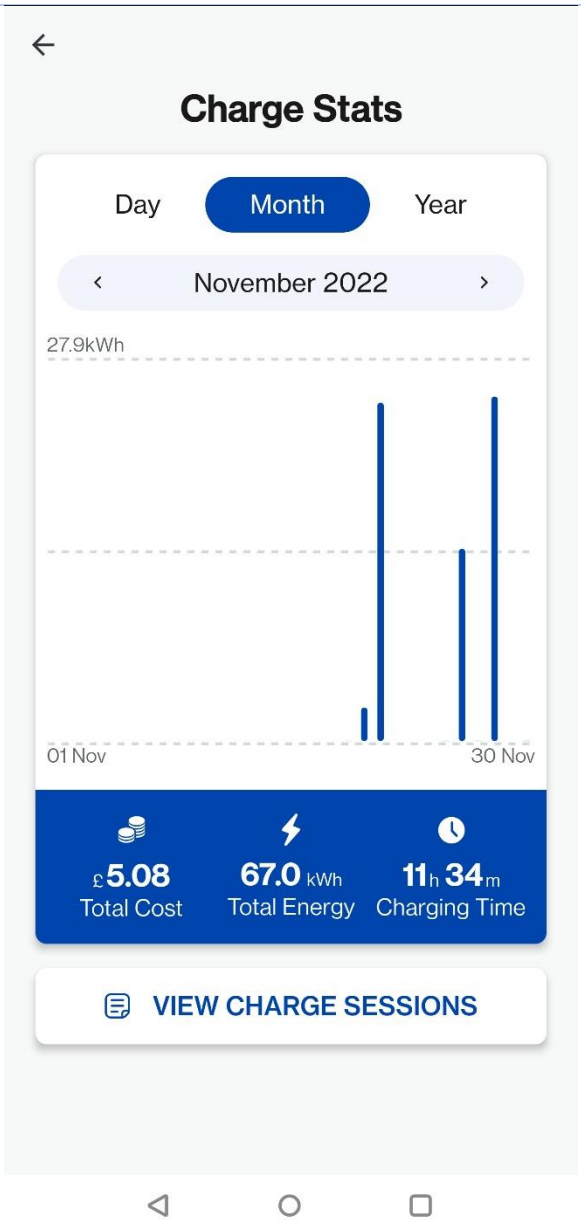
Requirement	Technical solution adopted to meet the requirement
Charge point is configured such that, in the event it ceases to be connected to a communications network, it will remain capable of charging an electric vehicle	In the event that Ohme units cease to be connected to a communications network, the following occurs: • If the car is plugged in to a vehicle and the unit has already accepted a charging schedule, the unit will continue to follow that schedule. • If the car is not plugged in, the unit will not be able to accept a charging schedule and therefore, once plugged in, the vehicle will start charging once the randomised delay has concluded. Users who wish to start charging immediately but the unit (without communications) is delaying charge, can simply unplug and re-plug the vehicle to start charging.

4.4 Safety

Requirement	Technical solution adopted to meet the requirement
Charge point is configured such that it will not allow a relevant person to carry out a specified operation where to do so would or may result in a risk to the health or safety of persons. "Relevant persons" means the owner, or an end-user of the relevant charge point who is not the owner. "Specified operation" means: • Overriding the default mode of charging during the default charging hours • Overriding the provision of demand side response services • Overriding the random delay	Ohme units are configured such that the local safety configuration always takes precedent over any remote commands/charging schedules. Examples of local settings include: • The maximum amperage of the charging device • Any load balancing constraints following readings from the current sensor • Any measured safety issues such as high/low voltage, high temperature or high residual current Note that changes to the charging rate due to dynamic readings from the load balancing system are not subject to randomised delays, as to do so would compromise safety.

4.5 Measuring system

Requirement	Technical solution adopted to meet the requirement
On each occasion it is used, the charge point measures or calculates: • The electricity it has imported or exported (in watt-hours or kilowatt-hours) • The amount of time for which it is importing or exporting electricity	Ohme units incorporate a metering system that calculates and reports: • Electricity consumed (kWh) • Time stamps at which energy was being transferred, which is used to derive the amount of time the unit was consuming electricity
The charge point is configured such that the owner can view the information in reference to: • Any occasion on which it was used to import or export electricity within the past 12 months • Any month within the past 12 months • The entirety of the last 12-month period	Below is a screenshot of the app showing the ability to view individual charging sessions in addition to charging sessions being grouped by month and year. This charging session information includes the amount of energy consumption, the charging times and the cost of charging (assuming the user has entered tariff information).

	
The charge point is configured such it can: • On each occasion it is used, measure or calculate every one second the electrical power it has imported or exported (in watts or kilowatts) • Provide this information via a communications network	Ohme units measure energy consumption several times a second. It uses this information to provide charging session information that is sent to the Ohme remote server, displayed in kWh.
The charge point is configured such that:	The metering accuracy of Ohme units is around 1%. Any systematic inaccuracy will be within 1% of the actual value. Measurement is provided by a metering system integrated

• The figures measured or calculated are accurate to within 10% of the actual figure • Any inaccuracies are not systematic	into the product. There is nothing inherent in the design, manufacture or the processing of values that would lead to a consistent or predictable error.

4.6 Off-peak charging

Requirement	Technical solution adopted to meet the requirement
The charge point: • Has pre-set default charging hours which are outside of peak hours • Offers the owner the opportunity to accept, remove, or change the default charging hours on first use • Offers the owner the ability to change, remove, or set default charging hours any time after first use unless the charge point is sold with a DSR agreement, configured to comply with the requirements of this agreement, and details of the agreement are included in the statement of compliance	Ohme units will avoid charging at peak times by default. As per the Regulations, the peak times are set to 8am to 11am and 4pm to 10pm weekdays. On first use of the charger, users are prompted to download the Ohme smartphone app and pair the charger. This is via the screen (Home Pro) or the accompanying product documentation (ePod). The setup flow/wizard on first using the app prompts the user to: • Set schedules for their charging. An example of a charging schedule is "On weekdays, add 50 miles of range to my car". • Add details of their energy tariff or create their own time-of-use tariff • Provide details of their vehicle, which allows the Ohme service to quantify the energy requirement. Once the user has gone through this process and enabled at least one schedule, the default hours are deselected. Once this flow is completed, each charging session will be optimised to the preferences set by the user. The main factors that determine the charging times are: • When they have set the charging session to end (expected next journey time) • The energy tariff, to favour charging times at the least expensive periods (if set as a user preference) • The forecast carbon intensity of national electricity generation, to favour charging at lower carbon periods (if set as a user preference) The user also has the ability to remove the default hours settings without creating alternative charging schedules if they wish.

	At any time, the user has the ability to re-select the default hours, or create new tariff and schedule details to move charging to alternative times.
The charge point is configured: • To charge a vehicle during the default charging hours (if any), unless the owner overrides the default mode of charging during this time • Such that the owner can override the provision of demand side response services	Ohme units will restrict charging during the defined peak times by default. In any circumstance, users with an app paired to the charger can select "Max Charge" to override any settings and begin charging immediately. This will ignore any charging schedules and will not apply the randomised delay. Users also have the ability to create their own charging schedules which will drive charging at different times, dependent on their preferences (e.g. energy tariff, estimated departure time).

4.7 Randomised delay

Requirement	**Technical solution adopted to meet the requirement**
The charge point is configured such that it must operate, at each relevant time, with a delay of random duration up to 600 seconds, determined to the nearest second each time	By default (i.e. before the charging unit is paired by a user), the charging will be delayed by a random time between 0 and 600 seconds. This figure can be changed via a configuration change from the server (does not require a firmware update). The randomised delay function does not operate when the unit is still in commissioning mode. This is to permit testing of the charge point which requires the charging to commence to test the safety functions. The Ohme server has been configured that any device being paired after 30th June 2022 will have randomised delays applied. Any new charging schedule that is sent to the unit will have the randomised delay built into the schedule. This randomised delay will also apply to charging schedules based on the off-peak default hours. The randomised delay applies to both commencing charging, increasing the charging rate, reducing the charging rate and stopping charging.
The charge point is configured such that the maximum duration of this delay can be remotely increased to up to 1800 seconds if required	The randomised delay time has been implemented as a configurable field, which can be changed at the server level and updated to all applicable devices without a firmware update.
The charge point is configured such that the random delay will not operate where:	The randomised delay will not operate in cases where:

• The owner or another relevant end-user has manually overridden it • An equivalent random delay has already been applied to the operation of the relevant charge point • The charge point is responding to a response DSR service	• Ohme and/or the user has separate DSR contracts in place of which the charge point is enlisted, and the charge point is being asked to provide a response • The user has adjusted their charging session requirements and asked for an amount of charge that cannot be provided within the time window set. Ohme will not apply the randomised delay to maximise the amount of charge the user will receive (note: this will not lead to synchronised charging across multiple chargers as the start time will be dictated by when a single user has accessed the app/user interface) • The user has set the charger to "Max Charge" which will override any charging restriction • Where the customer has selected a car that does not support smart charging and a trickle charge has been applied (6 amps), this is not subject to the randomised delay to avoid the car from not charging • Where the charging rate is being adjusted in response to a current measurement to avoid an overload

4.8 Security

Requirement	Technical solution adopted to meet the requirement
General Principles 1. A relevant charge point must be designed, manufactured and configured to provide appropriate protection— (a) against the risk of harm to, or disruption of, the electricity system; (b) against the risk of harm to, or disruption of, the relevant charge point; (c) for the personal data of the owner and any other end-user of the relevant charge point	The solutions adopted for each clause are: (a) Randomised delays are applied to the operation of the charge point as described in section 4.7 Measures are taken (in line with Regulation 8-9) to protect the unit from attack. Default charging hours have been applied as per Regulation 10. After a power outage, the device will apply a randomised start delay once the power is back. (b) Measures are taken (in line with Schedule 1, clause 8-9) to protect the unit from attack (c) No personal data is stored on the unit and data transfers between the unit and the Ohme backend are adequately protected as described below
Passwords 2. A relevant charge point must be configured so that where passwords are used on it—	No passwords are used or stored on the device

(a) the password is unique to that relevant charge point and not derived from, or based on, publicly-available information, or is set by the owner; and (b) the password cannot be reset to a default password applying to both that relevant charge point and other charge points	
Software 3.—(1) A relevant charge point must incorporate software which is able to be securely updated. (2) In sub-paragraph (1), securely updated means updated using adequate cryptographic measures to protect against a cyber-attack.	A secure update process has been implemented which involves using Public Key Infrastructure (PKI) to authenticate the transfer of data between the device and the backend server. The device will only accept and install firmware updates that were digitally signed by Ohme.
(3) A relevant charge point must be configured so that— (a) it checks, when it is first set up by the owner, and periodically thereafter, whether there are security updates available for it; (b) it verifies the authenticity and integrity of each prospective software update by reference to both the data's origin and its contents and only applies the update if the authenticity and integrity of the software have been validated; (c) by default, it provides notifications to the owner about prospective software updates; (d) the owner can implement software updates without undue difficulty.	Updates are applied remotely via the backend server. The server sets a flag that a firmware update is available. The device, as part of the bootup process and then periodically afterwards, checks for the presence of the flag and, if set, the update process begins. PKI is used to authenticate the server before the download commences. The file to be transferred is digitally signed. The contents of the downloaded file are verified using the key and checked for integrity. The file is only applied to the default boot directory if the authenticity and integrity are verified. The owner/charge point user are notified of the firmware version via the app. Notifications are not provided as the update is applied without any user action needed. Ohme controls the update process.
(4) A relevant charge point must be configured so that— (a) it verifies, via secure boot mechanisms, that its software has not been altered other than in accordance with a software update which has been	On boot up of the device, the bootloader checks the integrity of the firmware file. It does this by using a hardware root of trust system. If an unauthorised change is detected, a previous "known good" firmware is used. This version will usually be the firmware version applied at the factory. At this point, the firmware sends a notification to Ohme's servers whereby a notification is pushed to the user via the smartphone app.

validated in accordance with sub-paragraph (3)(b) above; (b) if an unauthorised change to the software is detected, it notifies the owner and does not connect to a communications network other than for the purposes of this notification.	
Sensitive security parameters 4.—(1) A relevant charge point must be configured so that— (a) where security credentials are stored on the relevant charge point, these are protected using robust security measures; (b) its software does not use hard-coded security credentials. (2) In this paragraph— (a) "hard-coded" means data forming part of the relevant charge point's source code and which is unalterable except by means of modification of the source code; (b) "security credentials" means ways of verifying that the relevant charge point is being used or accessed by a person properly authorised to do so.	The devices use a unique X.509 certificate to authenticate itself with the server. This certificate was assigned at the factory and robust security measures have been taken to prevent access or modification. This is achieved using hardware provided security features. Hard-coded security credentials are not used.
Secure communication 5. A relevant charge point must be configured so that communications sent from it are encrypted.	Communications to and from the device are encrypted using industry standard protocols.
Data inputs 6.—(1) A relevant charge point must be configured so that— (a) data inputs are verified so that the type and format of the data is consistent with that expected for the function to which the data relates;	Data validation is performed by the firmware on all input parameters sent to the unit. Any parameters which are not in the correct format or outside of allowable ranges are discarded. The server has been configured with data validation to ensure that inputs from the smart phone app or the device are within allowable ranges. Data outside of those ranges for formats are discarded.

(b) if such data cannot be verified, it is discarded or ignored by the relevant charge point in a safe manner. (2) The data inputs referred to in sub-paragraph (1) include data that is inputted via a user interface, an application programming interface or a communications network.	Inconsistent data is flagged and an entry made to the security log.
Ease of use 7.—(1) A relevant charge point must be configured so as to minimise the inputs required from the owner in connection with the set-up and operation of the charge point. (2) A relevant charge point must be configured so that any personal data can be deleted from it by the owner without undue difficulty.	Only necessary information is requested from users to obtain a high standard of smart charging services. This includes information on the vehicle (to understand battery size), the energy tariff (to understand costs and any time-of-use elements) and, if they wish, schedules of when the vehicle needs to be ready. No personal data is held on the charge point. Should a user wish to dispose of the Ohme's services (e.g. moving house), they can re-register their device from their account or delete their account.
Protection against attack 8.—(1) A relevant charge point must be designed and manufactured to provide an adequate level of protection against physical damage to the charge point.	Ohme units are impact protected to the levels described in IEC61851-1:2019.
(2) In particular, a relevant charge point must incorporate a tamper-protection boundary to protect the internal components of the charge point.	For all Ohme units, the tamper protection boundary is defined as the zone within the outer case allowing access to the internal components of the unit. A tamper detection device is installed which senses if the case is opened. An alarm is sent to the Ohme server which is relayed to the user via the smartphone app, alerted them to check the unit.
(3) A relevant charge point must be designed and manufactured to provide an adequate level of protection— (a) for its user interfaces; and (b) against use or attempted use of the relevant charge point other than through the user interfaces.	The main user interface is via the smartphone app. This is password controlled. Control of the device is also possible via buttons on the device. The user has the option to lock the buttons and authorise each plug in, to prevent unauthorised use. All other interfaces are within the tamper protection boundary and require PKI keys to allow access to the device functions.
9. A relevant charge point must be configured so that— (a) if there is an attempt (whether or not successful) to breach the tamper-protection boundary, it notifies the owner;	(a) If the tamper protection boundary is breached, a notification is relayed from the Ohme backend server to the owner via their smart phone app. (b) Ohme units do not have additional layers of access privileges, so in the event of a tamper detection, continues to operate in a normal way.

(b) its software runs with only the minimum level of access privileges required for it to deliver its functionality; (c) any logical or network interfaces that are not required for the normal operation of the relevant charge point, or otherwise to comply with the requirements in these Regulations, are disabled; (d) software services are not available to the owner unless necessary for the relevant charge point to operate; (e) any hardware interfaces that are used for the purposes of testing or development, but not otherwise during the operation of the relevant charge point, are not exposed.	(c) Ohme units do not have logical or network interfaces. (d) no additional software services, relevant to the charge point, are provided unless they are necessary to offer enhanced smart charging features. (e) Ohme units have a factory interface to allow initial setup of the charge point. This interface is within the tamper protection boundary and is locked down prior to sale.
Security log 10.—(1) A relevant charge point must incorporate a security log. (2) In this paragraph, "security log" means an electronic record on the relevant charge point of events relevant to the security of the relevant charge point including attempts (whether or not successful) to— (a) breach the tamper-protection boundary; (b) tamper with the relevant charge point; or (c) gain unauthorised access to the relevant charge point. (3) Entries in the security log must record, by reference to Coordinated Universal Time, the time and date on which the event occurred.	Ohme has implemented a Security Log for each charge point which it maintains on the customers behalf. Notifications are sent to the customer of all entries to the Security Log. Customers can contact Ohme to request a copy of the Security Log and review the contents. The Security Log contains any attempt to breach the tamper protection boundary and any firmware related events (e.g. failed authentication and resort to back up firmware version). All entries are time-stamped and are referenced to UTC, although the notifications are referenced to the users time zone.
Provision of information 11.—(1) When a relevant charge point is sold, information complying with the requirements in sub-paragraphs (2) to (4) must be supplied with it. (2) The information must specify how the owner can report concerns or problems identified regarding the security of the	A printed product manual is shipped with each device. This document includes information on how to contact Ohme if users have concerns or problems regarding the security of the device. The manual includes information on - the minimum period that software updates will be provided - Guidance on how to setup the charger

relevant charge point, including regarding its vulnerability to a cyber-attack. In particular, the information must provide contact details to which such concerns or problems can be reported. (3) The information must specify the period, if any, for which software updates will be provided by or on behalf of the relevant charge point manufacturer. (4) The information must— (a) provide guidance on how to set up the relevant charge point with adequate security protection; (b) include instructions on how to delete personal data from the relevant charge point.	- Information on the security features - Instructions on how to unpair the charger and delete the account

5. Software Versions

Firmware in Ohme units is automatically updated without any user interaction. Ohme guarantees compliance with the technical aspects of the Regulations in the following circumstances:

ePod

All ePod units sold in Great Britain are fully compliant with the Regulations, **including** Schedule 1: Security.

Home Pro

Any Home Pro unit sold in Great Britain, if it is first installed after 30th June 2022 will be compliant with the Regulations **excluding** Schedule 1, regardless of the supply date from Ohme.

Home Pro units shipped direct from Ohme after 30th November 2022 will be compliant with the Regulations, **including** Schedule 1: Security. Earlier units may comply, contact Ohme to discuss.

6. Register of Sales

Ohme, as the product manufacturer, maintains a register of sales for all its direct customers, which contains information of each product, the serial number and its compliance status/firmware version.

Any direct customers of Ohme can request a copy of this information for the charge points they have acquired.

7. Statement of Compliance

A Statement of Compliance is provided with each product, either within the product manual or as an addendum to the product manual. Alternatively, copies of the Statement of Compliance are held on the website.