



## smart Europe GmbH Privacy Statement

We are well aware of the importance of personal information to you and will do our best to keep your personal information safe and secure. This page outlines our Privacy Statement and explains, in a concise, clear and easy-to-understand manner, how smart Europe handles your personal information. Please see section II below for the full content of the smart Europe Personal Information Privacy Statement (section I provides a brief overview).

### I. General Information

The controller within the meaning of the UK General Data Protection Regulation (UK GDPR) is:

smart Europe GmbH  
Esslinger Str. 7, 70771 Leinfelden-Echterdingen, Germany  
E-Mail [eu.corporateoffice@smart.com](mailto:eu.corporateoffice@smart.com)

Data protection officer:

smart Europe GmbH  
Data Protection Officer  
Esslinger Str. 7, 70771 Leinfelden-Echterdingen, Germany  
E-Mail [eu.dataprotection@smart.com](mailto:eu.dataprotection@smart.com)

### Scope of this Privacy Statement

This Privacy Statement applies to our website and social media accounts, the Hello smart App, the Internet of Vehicle (IoV) services and other services offered by smart Europe.

Specific products and services may be subject to separate privacy statements. We will inform you accordingly in cases where a separate privacy statement applies.

### What information do we collect from you and your vehicle?

We may collect the following types of information (as set in further detail in section II below), which may be related to you or your use of our products and services, in accordance with the principles of UK GDPR, including the principles of lawfulness, fairness, transparency and purpose limitation:

- Identification data, e. g. name, address, phone number, e-mail etc.
- Technical Data, e.g. VIN number, model, maintenance history, usage statistics, etc.

- Driving analysis data, e.g. position, speed, car mode, warnings, status codes, battery status, search history etc.
- Contract data, e.g. purchase information, service information, smart ID, preferences etc,
- Other data, e.g. credit information, bank details, appointment booking history etc.

For more details, please read “How we collect and use personal data” section below. Some of our functions need to invoke your device permission. We will use the system pop-up window or application pop-up window to ask you for authorization. You can always switch the relevant permissions at any time in the settings function of your device.

We collect your personal information either directly from you (e.g., in forms you provided us when creating your Smart ID, or when you interact with us through your vehicle), or from third parties (including publicly available sources).

### How do we share your personal information?

We will share your data if it is necessary within the “smart Ecosystem”, our Financial Service Partner (Deutsche Bank AG, Taunusanlage 12, 60325 Frankfurt am Main, Germany), our Leasing Service Partner (Santander Consumer UK plc, 86 Station Road, Redhill, Surrey, RH1 1SR, United Kingdom) or other third-party Financial Service Providers with whom you have entered into a contract.

We will only share your personal information for the necessary purpose and scope (e.g. if you purchase products or digital services or use after-sales services, it may be necessary for your customer data to be exchanged between the respective companies involved in the smart Ecosystem) as set in further detail in section II below.

The “smart Ecosystem” includes the smart Europe GmbH, the local smart branches (entities), the smart Agents and smart Authorised Service Partners and other partners involved in the smart daily business.

#### Smart branches (entities) are:

smart Europe GmbH, Esslinger Str. 7, 70771 Leinfelden-Echterdingen, Deutschland

smart Austria Automotive GmbH, Am Belvedere 10, 1100 Wien, Österreich

smart Schweiz GmbH, Richtistrasse 2-6, 8304 Wallisellen, Schweiz

smart Belgium Srl, Avenue du Péage 68, 1200 Woluwe-Saint-Lambert, België

smart Automobile France SAS, 7 avenue Niépce, 78180 Montigny-le-Bretonneux, France

smart Italia S.r.l., Via di Quarto Peperino, 2200188 Roma, Italia

smart Nederland B.V., Ravenswade 4, 3439 LD Nieuwegein, Nederland

smart Portugal Unipessoal Lda., Rua Gottlieb Wilhelm Daimler, 2710-037 Sintra, Portugal

smart España A.E., S.L., avenida de Bruselas 30, Alcobendas, Madrid 28108, España

smart UK Automotive Ltd., Delaware Drive, Tongwell, Milton Keynes, MK15 8BA, United Kingdom

smart Sweden AB, Skrivaregatan 21, 215 37 Malmö, Sverige

Mercedes-Benz AG, Mercedesstraße 120, 70372 Stuttgart, Deutschland

### smart Agents and smart Authorised Service Partners, and other partners:

Your data will not be automatically shared with smart Agents and smart Authorised Service Partners. An exchange of data only takes place if this is necessary for the fulfilment of a contract with you, if the exchange serves a legitimate interest or you have given your express consent, e.g. in case of a Test drive, on-site appointment for vehicle service, repair or consultation, telephone advice, vehicle handover or trade-in.

A data transfer to carefully selected and checked service providers and business partners with whom we work can take place to be able to offer you products and services. We only do this within the framework of the strict requirements of data processing on behalf of smart Europe GmbH, to fulfil a contractual obligation (e.g. forwarding to the insurance provider in case of warranty claims).

In case we share your data based on a consent, an overview of the smart Agents and smart Authorised Service Partners for whom your consent applies can be found at any time in the Self Care Portal of your smart Account. There you also have the possibility to revoke your consent.

### Data transfer to third countries

We may transfer your data to recipients in a third country outside the United Kingdom (UK), European Union (EU) and European Economic Area (EEA). We only do so if an adequate level of data protection is ensured by an adequacy decision of the European Commission or other appropriate safeguards, such as EU standard contractual clauses or binding corporate rules.

All transfer of data including transfer of data within the UK, EU and EEA will be encrypted.

### How long do we store your personal information?

We will store your personal data for no longer than it is necessary for the purposes specified in this Privacy Statement, in particular for the fulfilment of our contractual and legal obligations. We may also store your personal data for other purposes if or as long as the law allows us to store it for particular purposes.

If you choose to cancel your account, we will delete all the data we have stored regarding you. If it is not possible or necessary to completely delete your data for legal reasons, the relevant data will be blocked for further processing and deleted after the legal retention period has terminated. For example, we are legally obliged to retain order and payment data in connection with a purchase for tax audits and financial audits for up to ten years. Before we can finally delete this data.

### For which purposes and on what legal basis do we process your data?

We only process your personal data if there is a legal basis for the processing. We rely on the following legal grounds for data processing in most cases (as set in further detail in section II below):

- your consent pursuant to Article 6 (1) lit. a UK GDPR:
  - o We rely on your consent for marketing purposes;
  - o Feedback surveys and market research questionnaires in order to improve our products and services;
  - o For other purposes (e.g. display of personalized content or advertisements based on your usage behavior), we and, if applicable, selected third parties will use your data.
- where necessary for the conclusion or performance of a contract entered in your interest pursuant to Article 6 (1) lit. b UK GDPR:
  - o We use technical and driving analysis data to provide roadside assistance and security services to you;
  - o We use professional or employment related information when you apply for a job in our job portal to receive and process job applications;
  - o For the execution of a contract as well as for customer administration reasons and – if necessary – for the execution and settlement of any business transactions, we use the data in each case only to the extent necessary for this purpose;
  - o For training purposes (e.g. registration for face-to-face training or live online training), your data will be used by us and, if applicable, by selected third parties;
  - o For customer management purposes (e.g. registration and use of smart systems for sales and aftersales purposes);
  - o We use your data if you book a test drive or a workshop appointment with a smart sales partner near you via our website;
  - o We use your data for the organization of giveaways and raffles, as well as to notify the winners, manage related activities and send out the prizes.
  - o We use your data for pre-contractual purposes.
- to fulfil a legal obligation concerning smart pursuant to Article 6 (1) lit. c UK GDPR:
  - o We use your data for the purpose of operating the 112 emergency e-call from the vehicle pursuant to Regulation (EU) 2015/758;
  - o We retain your data for the purpose of complying with mandatory retention periods;
  - o We use your data for the purpose of complying with court orders or similar investigation orders with public authorities of member States of the EEA;

- We use your data for the purpose of operating the Vehicle Security Operations Center pursuant to the UN Regulation No. 155 requiring the presence of a cybersecurity management system (CSMS) in vehicles.
- We use your data for the purpose of providing the Driver Drowsiness and Attention Warning System (DDAW) pursuant to Regulation (EU) 2019/2144.
- where it is necessary to realize a legitimate interest by smart, except where such considerations are overridden by the need to protect your interests or fundamental rights, is Article 6 (1) lit. f UK GDPR:
  - We use the collected personal data when you visit our applications (e.g. Hello smart App and our website) to operate them as conveniently as possible for you and to protect our IT systems from attacks and other illegal activities.

### What are your rights as a data subject?

As a data subject, you have, under certain conditions, the right of access (Art. 15 UK GDPR), rectification (Art. 16 UK GDPR), data erasure/deletion (Art. 17 UK GDPR), restriction of processing (Art. 18 UK GDPR) and data portability (Art. 20 UK GDPR). More details including how you can exercise your rights are provided in the end of this Statement under **"HOW TO EXERCISE YOUR DATA SUBJECT RIGHTS"**.

### How to contact us?

You can easily contact us by calling our customer service number:

AT +43 1 2536442  
BE +32 2 5889656  
FR +33 1 84883613  
DE +49 711 5507 7020  
IT +39 06 94503682  
NL +31 30 8081521  
PT +351 210 201 582  
ES +34 91 9491521  
CH +41 43 5081946  
UK +44 1908 086064  
SE +46 8551 22321

or sending an email to:

[hallo@support.smart.com](mailto:hallo@support.smart.com) (German)

[hello@support.smart.com](mailto:hello@support.smart.com) (English)

[ciao@support.smart.com](mailto:ciao@support.smart.com) (Italian)

[bonjour@support.smart.com](mailto:bonjour@support.smart.com) (French)

[hola@support.smart.com](mailto:hola@support.smart.com) (Spanish)

[hoi@support.smart.com](mailto:hoi@support.smart.com) (Dutch)

[ola@support.smart.com](mailto:ola@support.smart.com) (Portuguese)

[hej@support.smart.com](mailto:hej@support.smart.com) (Swedish)

You can contact our privacy team by sending an email to – [eu.dataprotection@smart.com](mailto:eu.dataprotection@smart.com).

Smart Europe GmbH

Esslinger Str. 7, 70771 Leinfelden-Echterdingen, Germany

## II. HOW WE COLLECT AND USE PERSONAL DATA

### 1. WHEN YOU USE OUR WEBSITE

#### Server-Log-Files

Whenever you visit our websites, we automatically collect and store information in so-called server log files, which your browser automatically transmits to us. These are:

- IP address (Internet protocol address) of the terminal device from which the online offer is accessed;
- Internet address of the website from which the online offer was accessed (so-called origin or referrer URL);
- Name of the service provider through whom the online offer is accessed;
- Name of the files or information accessed;
- Date and time as well as duration of the retrieval;
- Amount of data transferred;
- Device (PC, mobile, other), operating system and information on the Internet browser used, including installed add-ons (e.g. for the Flash Player);
- http status code (e.g. "request successful" or "requested file not found").

The above data is stored in the log files without your full IP address, so that no conclusions can be drawn about your IP address.

This data is not merged with other data sources.

The collection of this data is based on Art. 6 (1) lit. f UK GDPR. We have a legitimate interest in the technically error-free presentation and optimization of our website. For this purpose, the server log files must be collected.

#### 1.1. Cookies

Cookies may be used when visiting our web applications. Technically, these are so-called HTML cookies and similar software tools such as web/DOM storage or local shared objects (so-called "flash cookies"), which we refer to collectively as cookies.

- Cookies are small files that are stored on your desktop, notebook or mobile device while you visit a website. Cookies make it possible, for example, to determine whether there has already been a connection between the device and the websites; take into account your preferred language or other settings, offer you certain functions (e.g. online shop, vehicle configurator) or recognize your usage-based interests. Cookies may also contain personal data.
- Whether and which cookies are used when you visit our websites depends on which areas and

functions of our websites you use and whether you agree to the use of cookies that are not technically required in our Consent Management System.

- The use of cookies also depends on the settings of the web browser you are using (e.g., Microsoft Edge, Google Chrome, Apple Safari, Mozilla Firefox). Most web browsers are preset to automatically accept certain types of cookies; however, you can usually change this setting. You can delete stored cookies at any time. Web/DOM storage and local shared objects can be deleted separately. You can find out how this works in the browser or device you are using in the manual of the respective manufacturer.
- The consent to, and rejection or deletion of, cookies are tied to the device and also to the respective web browser you use. If you use multiple devices or web browsers, you can make decisions or settings differently.
- If you decide against the use of cookies or delete them, you may not have access to all functions of our websites or individual functions may be limited.

#### 1.1.1. We use the following types of cookies:

##### a. Essential Cookies

These cookies are necessary for the functionality of our website and the provision of our services such as but not limited to the authentication of the user or content streaming. Legal basis for their use is contract fulfillment pursuant to Article 6 (1) lit. b UK GDPR, if cookies are used to enable the ordering process, or our legitimate interest pursuant to Article 6 (1) lit. f UK GDPR in the provision of our website and services.

##### b. Functional Cookies

With these cookies we are able to provide advanced functionality and personalization based on your preferences (e.g., language of the user interface). They can be set by us or by third parties whose services we use on our website. Legal basis for the use of functional cookies is your consent pursuant to Article 6 (1) lit. a UK GDPR.

##### c. Performance Cookies

We use these cookies with your prior consent to analyze and improve the use of our website and services. Legal basis for the use of performance cookies is your consent pursuant to Article 6 (1) lit. a UK GDPR.

##### d. Marketing Cookies

Marketing cookies are used by our advertising partners to serve advertisements based on your interests and usage behavior. They do not directly store personal data, but are based on a unique identification of your browser and internet device. Legal basis for the use of marketing cookies is your consent pursuant to Article 6 (1) lit. a UK GDPR.

For more information about our used Cookies, purpose and storage of Cookies please read section



---

"Cookies" at the bottom of the page. There you can manage your cookie settings and revoke your consent at any time.

To collect and manage your consent we use the Consent Management Platform (CMP) from OneTrust (OT Technology, Spain, S.L.U., Paseo de la Castellana, 77, 8th floor, Madrid, 28046, Spain).

## 2. WHEN YOU USE OUR SOCIAL MEDIA CHANNELS

You can use social media channels and messaging services as a user to react, reply, comment on social media posts shared by smart Europe. In addition, you can tag or mention smart Europe accounts on different social media channels and messaging services. Lastly, you can use social media channels and messaging services to reach out to smart Europe. The legal basis for this processing is our legitimate interest pursuant to Article 6 (1) lit. f UK GDPR of managing our relationship with you.

The operators of the respective social networks may collect information on your usage behaviour via cookies and similar technologies. When you use social networks, the nature, scope and purposes of data processing are determined by the social network operators acting as independent controllers.

Details of the processing activities on the platforms you can find under following links:

Facebook (Meta): <https://www.facebook.com/privacy/explanation>

TikTok: <https://www.tiktok.com/legal/page/eea/privacy-policy/en>

LinkedIn: <https://www.linkedin.com/legal/privacy-policy>

Twitter: <https://help.twitter.com/rules-and-policies>

Pinterest: <https://policy.pinterest.com/privacy-policy>

## 3. WHEN YOU SIGN UP FOR AN ACCOUNT

When you register as a user via our web services, we will create a user account using your e-mail address as the identifier (smart ID) which will be your identifier within the smart Ecosystem. Your created smart ID is the basis for your connected customer experience and enables you to: save your individual vehicle via our online customizer, book a test drive, buy the vehicle or digital services, connect to the vehicle, purchase aftersales packages, manage workshop services and use other services offered by smart.

### 3.1. Private person registration:

You can sign up for an account via the [id.smart.com](https://id.smart.com) website or via the Dashboard in the outlet of your smart Agent. We distinguish between two levels of registration.

The soft registration is only used for the purpose of obtaining information, e.g. for the logging of your customized car via our online customizer, which supports you online in the configuration

of your desired model. The following data is collected from you: Title, First Name, Last Name, Email

The full registration is required for all other purposes, e.g. for the booking of a test drive or for the purchase of the vehicle. Following data is collected additionally to the data collection of the soft registration: Date of Birth, Street, City, State, Postal Code, Country, ID type and ID number.

The legal basis for the processing of your data is contract fulfillment pursuant to Article 6 (1) lit. b UK GDPR and our legitimate interest pursuant to Article 6 (1) lit. f UK GDPR.

### 3.2. Business registration:

Via the sed.smart.com website, the account is created for business customers including our smart Agent network in order to get registered to access the systems to get access to the necessary customer information. For business customers and our smart Agent network, we distinguish between two levels of registration. The initial registration is for the User to get the smart ID (email address), post which they will receive the email for the verification. After verification, the user can continue with the Registration process to link themselves with the respective workshop. The following data is collected from you: Title, First Name, Middle Name, Last Name, Email, VAT number, company name, fiscal code.

The legal basis for the processing of your data is contract fulfillment pursuant to Article 6 (1) lit. b UK GDPR and our legitimate interest pursuant to Article 6 (1) lit. f UK GDPR.

## 4. WHEN YOU BOOK A TEST DRIVE OR APPOINTMENT

When you book a test drive, we will collect your name, email address, date of birth, address and phone number and your driver's license to ensure that you are legally qualified to drive the vehicle.

We use this data for:

- The execution of your appointments, e.g., test drive, incl. creation of contracts
- Forwarding your appointment details and requests to the dedicated contact within the smart Ecosystem
- Contacting you for appointment management

The legal basis for the processing of your data is contract fulfilment pursuant to Article 6 (1) lit. b UK GDPR.

With your prior consent, we may also use this data to contact you for customer satisfaction consultations, for targeted consulting based on previous activities or for marketing purposes.

## 5. WHEN YOU PURCHASE A VEHICLE OR OTHER PRODUCTS OR SERVICES

If you instruct us to register your vehicle, we may transmit your data, such as name, address, smart ID, e-mail address, telephone number, VIN, vehicle type, model, EVB no. for the purpose of

registration to our service provider in the respective country.

To provide you with vehicle services, we will collect your name, mobile phone number, e-mail address, vehicle type, VIN, vehicle configuration model, registration city and sales service area information. We will share your VIN number with our third party provider for activating your digital services, read more under section III. 1. Authentication and registration of vehicle SIM card.

During the checkout process for your smart vehicle, we offer you the option to purchase repair cost insurance as an extended warranty. For this service, we partner with the insurance provider Real Garant, located at Marie-Curie-Straße 3, 73770 Denkendorf, Germany.

If you choose to purchase the extended warranty during checkout, we will forward your customer and vehicle information, such as name, address, e-mail address, phone number, Vehicle Identification Number (VIN) to Real Garant in order to establish the insurance contract. Additionally, in the event of a warranty claim on your vehicle, we will transfer your customer master data, contact data, vehicle data and claims information to Real Garant to facilitate the reimbursement of the claim.

When you purchase a product or a service and you choose to pay cash we will collect your billing address and register your preferred payment method (e.g. Credit /Debit). If you choose a financed payment and want smart to facilitate the financing smart will collect your billing address, your name and ID and forward this to Deutsche Bank (Deutsche Bank AG, Taunusanlage 12, 60325 Frankfurt am Main, Germany) which is our preferred financing partner.

If you choose to lease the vehicle, smart may share your data with our Leasing-Partner Santander Consumer UK plc, 86 Station Road, Redhill, Surrey, RH1 1SR, United Kingdom ) or other third-party providers of financial services with whom you have concluded a contract.

As part of the purchase your identity may need to be verified. For this reason we use a third party provider Onfido Limited, 3 Finsbury Avenue, EC2M 2PA London, and we will redirect you to the website of our partner.

The legal basis for the processing of your data is contract fulfilment pursuant to Article 6 (1) lit. b UK GDPR.

When you purchase a product or a service, we conduct a compliance check which involves a comparison of the customer's personal data (such as name, address and ID) with relevant regulatory due diligence lists, in particular based on the EU sanction regulations. The legal basis for processing, if there is a legal obligation to perform compliance/sanctions list screening, is Art. 6 (1) lit. c) UK GDPR. In individual cases, depending on a balancing of interests, a compliance/sanctions list screening may also take place if there is no mandatory legal obligation. In this case, the legal basis is our legitimate interest pursuant to Art. 6 (1) lit. f) UK GDPR in avoiding potential sanctions by foreign authorities.

---

## 6. WHEN YOU PURCHASE THIRD PARTY PRODUCTS (WALLBOX)

As part of the checkout of your order we also offer our smart charge@home services for home charging, consisting of the option to purchase wallbox hardware, a pedestal and an installation service. For this purpose, we have a third-party provider ABB E-Mobility B.V., Heertjeslaan 6, 2629JG – Delft/NL. In case you purchase a smart charge @home wallbox and for the installation we will forward your data to ABB. We will forward the following data: name, address, contact details, preferred installation date.

## 7. WHEN YOU USE THE HELLO SMART APP

With the Hello smart App you are able to connect to your vehicle and to access vehicle remote functions and other services via your smartphone. To provide the App, we process your personal data according to the respective description of the functions or services you use. This data processing is necessary to provide the functions of the App according to your specifications. The legal basis for this processing is contract fulfillment (Art. 6 (1) lit. b) UK GDPR), unless otherwise stated for individual functions or services in this privacy statement.

### 7.1 App login

To log into the App, you need a smart account (for account registration, see section 3). If you do not have a smart account yet, you sign up via the app. In this case, you will automatically be forwarded to our website to get registered for a smart account. We collect your first name, last name and your e-mail address as well as your country code. With this data we generate your personal smart ID which is linked to an individual unique ID (UUID) at smart. After generating the smart account you can log into the Hello smart App. You can also delete your account via the Hello smart App. Please read more under the section IX. Cancellation of your account.

When you login to the App, you will also be asked for permission to activate certain cookies and similar technologies, such as SDK's, for purposes like improving your user experience, analyzing the use of our services and supporting our marketing activities (please refer to section 1.1. for further information on how we use cookies). To collect and manage your consent we use the Consent Management Platform (CMP) from OneTrust (OT Technology, Spain, S.L.U., Paseo de la Castellana, 77, 8th floor, Madrid, 28046, Spain). The consent is voluntary. You can change your privacy preference settings at any time.

### 7.2 App permissions

When you open the app for the first time, you will be asked for your consent to enable certain features or access certain information. Your consent is voluntary and can be revoked at any time via the settings of your end device. If you do not activate individual functions, certain services of the App may not be available.

#### 7.2.1 Camera

---

The use of certain functions (e.g. vehicle activation and login via QR-code) requires the app to be able to access your camera. The camera function can only be used if you have activated this function in the app. You can subsequently activate or deactivate this function in your device settings at any time. When this function is activated, we process the personal data that you record with the camera when using the respective app functions. This data processing is based on your express consent (Art. 6 para 1. Lit. a) UK GDPR). If you revoke your consent, the app will not access your camera. Please note that without access to your camera, some functions are not available.

### 7.2.2 Location

The use of certain functions (e.g. public charging with smart charge@street) requires the app to be able to access your location and geographical data. Your location will only be processed if you have activated this function in the app. You can subsequently activate or deactivate this function in your device settings at any time. This data processing is based on your express consent (Art. 6 para 1. Lit. a) UK GDPR). If you revoke your consent, the app will not access your location. Please note that without access to your location, some functions are not available.

### 7.2.3 Push Notifications

When you open the app for the first time, you will be asked for your consent to receive push notifications. Push notifications may include alerts, sounds and icons. With push notifications, we can inform you about certain functions or services when the App is running in the background (e.g. in the case of charging the vehicle). You can activate and deactivate push notifications at any time in your device settings. If you have activated push notifications, we store a push token of your end device in order to be able to send you push notifications. For the sending of push notifications we use Google Firebase, a service of Google Ireland Ltd., Google Building Gordon House, Barrow Street, Dublin 4, Ireland. Access to the information by Google LLC in the United States cannot be excluded. This data processing is based on your express consent (Art. 6 para 1. Lit. a) UK GDPR). If you revoke your consent, we will delete the push token and you will not receive any further push notifications.

## 7.3 Vehicle Pairing

In order to activate certain digital services and control the vehicle via the app, it is necessary to pair the vehicle with your smart account via the App. To pair the App with your vehicle, you will be asked to scan the vehicle pairing QR code shown on the Digital Head Unit (DHU) of the vehicle. For pairing, the VIN, email address and UUID will be exchanged. The App collects your first name, last name and e-mail address which you shared within the registration process as well as license plate number and registration date. Your vehicle will automatically be recognized by the VIN and UUID number.

For pairing and activation of the digital services, we use a third-party provider for Telematic Service.

You can use the Unpairing function to remove the vehicle from your App. In this case you will not be able to use the remote control functions of the App anymore. The collected data will be deleted.

## 7.4 Digital Key and App Key-Sharing

You can create a digital key which you can use to open, close and start the vehicle and share it with other users. In order to create a digital key, it is necessary that you have activated a Bluetooth connection. To create the key, we process the vehicle identification number (VIN), vehicle location and basic vehicle information (vehicle series code and model code), your user name and user ID as well as the calibration values. When you use the digital key, we also process information about the door status, lock status, usage mode and engine status.

When you share the digital key, we process additional information to enable the key sharing and to verify the recipient's authorization (including the e-mail address, app id, share id, user id, user type, phone model and operating system as well as the time and duration of the sharing).

To provide the digital key services, we use a third party provider for Telematic Service.

## 7.5 Public Charging

We offer our smart charge@street public charging services for your vehicle in cooperation with Digital Charging Solutions GmbH, Rosenstraße 18-19, 10179 Berlin ("DCS"). The charging services are provided by DCS. The user can access the smart charge@street website operated by DCS via the Hello smart App to conclude a contract for charging services or to manage their existing contract. DCS is the data controller and responsible for the data processing in this regard. Please see the smart charge@street website for more information on how DCS processes your personal data.

Via the App, users can display nearby charging points, provided they have permitted access to their location. In addition, users can view the availability, available cable type and price. The user may use third-party map services (by Google Ireland or by Apple Inc.) to navigate to a Charging Point. For this purpose, Google Maps or Apple Maps need access to your location. Please note that Google Ireland Limited processes your location data within the Google Maps service and Apple Inc. within the Apple Maps service respectively as sole data controllers. Please see <https://policies.google.com/privacy?hl=en> for more information on how Google Maps processes personal data within the Map services and <https://www.apple.com/legal/internet-services/maps/terms-en.html> for more information on how Apple Maps processes personal data within the Map services.

## 7.6 Wallbox

If you purchased a smart charge@home wallbox via our partner ABB E-Mobility B.V., Heertjeslaan 6, 2629JG – Delft, Netherlands ("ABB") with a connectivity function, you can pair your wallbox with the vehicle via Bluetooth in the App. Successful pairing will allow you to use the Bluetooth Plug & Charge functionality. To establish this connection, we need to process the VIN of your vehicle.

## 7.7 Remote control and remote App configuration

Google firebase remote function is used for remote control of the App and to store the configurations of the App. This information is collected during the initialization of the App. For this function we use Google (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland) as a data processor. Firebase retains the Firebase installation IDs until the Firebase customer makes an API call to delete the ID. After the call, the data will be removed from live and backup systems within 180 days. For further details on data processing see [Privacy and Security in Firebase \(google.com\)](#).

Collected data: Firebase installation IDs.

Legal basis for the processing of your data is our legitimate interest pursuant to Article 6 (1) lit. f UK GDPR in the provision of our App and services.

## 7.8 Localization and Translation Management

In order to provide you with over the air translation of the App we use Lokalise (Lokalise Inc. 3500 South DuPont Highway, Suite BZ-101, Dover, Delaware, DE 19901, USA) as our data processor.

Legal basis for the processing of your data is our legitimate interest pursuant to Article 6 (1) lit. f UK GDPR in the provision of our App and services.

## 7.9 Maps and Location

"MapKit" (Apple Distribution International, Hollyhill Ln, Hollyhill Industrial Estate, Cork, T23 YK84, Ireland) and "Google Maps" (Google Ireland Limited, Gordon House, Barrow Street Dublin 4, Ireland) are the official providers of the maps in our App. These are used to display the current location of the vehicle and the Public sharing point-of-interest ("POI").

Collected data: vehicle location (longitude and latitude), device location (longitude and latitude) and point-of-interest ("POI").

Legal basis for the processing of your data is our legitimate interest pursuant to Article 6 (1) lit. f UK GDPR in the provision of our App and services.

## 7.10 Crash reporting

Google Firebase Crashlytics is used for stability and troubleshooting of the App. Crash reports are sent to Google Firebase for error and crash reporting and fixing. For this function we use Google (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland) as a data

processor. Firebase Crashlytics uses crash stack traces to associate crashes with a project, send email notifications to project members and display them in the Firebase console, and help Firebase customers debug crashes. It uses Crashlytics installation UUIDs to measure the number of users affected by a crash and minidump data to handle NDK crashes. The minidump data is stored while the crash session is being processed and then discarded. The Firebase installation ID enables upcoming features that improve crash reporting and crash management services. Firebase Crashlytics stores crash stack traces, extracted minidump data and associated identifiers (including Crashlytics installation UUIDs and Firebase installation IDs) for 90 days before beginning the process of removing them from live and backup systems. For further details on data processing see Privacy and Security in Firebase ([google.com](https://firebase.google.com/privacy)).

Collected data: Crashlytics installation UUIDs, Firebase Installation ID, Crash traces, Breakpad minidump formatted data (Only NDK crashes).

Legal basis for the processing of your data is your consent pursuant to Article 6 (1) lit. a UK GDPR.

### 7.11 App Analytics

We collect usage information that is associated with your Adobe account or device to provide you with a more personalized experience and improve our products and services. For this purpose, we use services of Adobe (Adobe Systems Software Ireland Limited, 4-6 Riverwalk, City West Business Campus, Saggart D24, Dublin, Ireland).

Collected data: Geolocation (country, city, postal code), Network (Mobile Carrier, Domain, ISP), Device Info (Device Model, Name), Browser Info (Browser Vendor, Name, Version), Operative System Info (Vendor, Name, Version), Events tracked: Application Launched/Opened, Application Closed, ECID (Adobe ID) and obfuscated IP address (collected but not stored).

Legal basis for the processing of your data is your consent pursuant to Article 6 (1) lit. a UK GDPR.

## **III. WHEN YOU USE VEHICLE-BASED DIGITAL SERVICES**

Depending on your vehicle model and the functions and services you choose, we collect and use your relevant personal information to provide you with more diversified vehicle-based Digital Services. All collected information is generally stored and processed within EU and EEA except for technical data required for Vehicle Performance Analysis and Error identification, which can be transferred outside EU and EEA for third level support. No personal identifiable information will be shared outside EU and EEA.

**Please Note:** In the process of providing the following vehicle-based Digital Services, we may collect your vehicle information, such as: vehicle charging information, parking brake status, cruising range, alarm status, maintenance status, seat belt status, collision status, vehicle travel time, energy consumption. Please note that the vehicle information alone cannot identify



you and does not constitute your personal information. We will treat your vehicle information as your personal information only when it is used in combination with your other information and can identify you. We will process and protect your vehicle information in accordance with this Privacy Statement. The hardware, software of the network system and the data in the system are protected from damage, alteration or leakage due to accidental or malicious reasons, and the system operates continuously and reliably and normally, and the network service is not interrupted.

Some of the following functions and services in the use of the vehicle are provided to you by smart and the third-party service providers that smart connects you to. Except as expressly stated otherwise in this Clause and the applicable user clauses, this Clause does not apply to third-party service providers who independently provide products or services to you. We recommend that you carefully read the privacy clauses or personal information processing rules of third-party service providers before using these services to understand how they will process and protect your personal information, and how you can exercise your relevant rights.

You can activate and deactivate individual services and functions in the privacy settings of your vehicle's DHU, except functions that are necessary for legal, safety and security reasons. You can also control certain services and functions via the Hello smart App. For more information, you can also consult the User Manual, which you can access in your vehicle.

## 1. Authentication and registration of vehicle SIM card

The vehicle-based Digital Services provided by smart or third parties require a mobile network connection.

When you activate and use the vehicle-based Digital Services, we will send an activation request to our Telematic Service Provider and our service provider VODAFONE ENTERPRISE GERMANY GMBH, Ferdinand-Braun-Platz 1 40549 Düsseldorf, Germany ("Vodafone") to activate the related SIM card and provide you with our SIM Service, Connectivity Service as well as our E-Call Service. Your personal data is not shared with our Service Provider Vodafone.

Processed data: Vehicle Identification Number (VIN) and eSIM identifiers (ICCID, MSISDN or IMEI).

Legal basis for the processing of your data is contract fulfillment pursuant to Article 6 (1) b UK GDPR.

If your vehicle is equipped with a wireless network connection, data can be exchanged between the vehicle and other equipment. The wireless network connection can be enabled through the transmission and reception unit of the vehicle or by connecting a mobile terminal equipment, such as a smart phone.

To provide SIM Service, Connectivity Service as well as our E-Call Service, we use a third party provider for Telematic Service as a data processor.

## 2. Vehicle Remote Functions

With the Hello smart App you are able to access and control certain vehicle functions remotely via your smartphone.

You have the Following Remote functions via the Hello smart App:

- You can lock and unlock the door & boot of your vehicle remotely  
Collected data: Vehicle identification number (VIN), vehicle information: door status, door lock status, usage mode and car mode;
- You can use the App to find the vehicle by flashing light or sounding the horn  
Collected data: Vehicle identification number (VIN), Vehicle information: vehicle speed, car location, vehicle direction, usage mode and car mode;
- You can use climate control to manage the temperature in the vehicle, including seat heating and steering wheel heating  
Collected data: Vehicle identification number (VIN), climate status: seat heating status, seat ventilation status, in-vehicle setting temperature, high voltage status, usage mode and car mode;
- You can remotely start and stop charging the vehicle battery  
Collected data: Vehicle identification number (VIN), state of charge, charge remaining time, high voltage status, charging current, charging voltage, charging start time, usage mode and car mode;
- You can access and display status information of the vehicle via the app remotely  
Collected data: Vehicle identification number (VIN), Vehicle status data (such as mileage, battery voltage, door and flap status/position/lock status, the window status/ warning/ position/, vehicle alarm status, sunroof open status, engine status, key status), average consumption and tyre pressure.

Legal basis for the data processing is contract fulfillment pursuant to Art. 6 (1) lit. b) UK GDPR.

To provide Vehicle Remote Functions, we use a third party provider for Telematic Service as a data processor.

## Digital Services via the Digital Head Unit (DHU)

### 2.1 Online Navigation

With this function we enable Route calculation, Map updates, showing charging stations, Parking places and Online traffic information. You can only use the navigation map related functions if you activate this function in the privacy settings on the DHU.

Collected data: Favorites (including name, address, vehicle location (latitude and longitude), phone, etc.), destination name, vehicle location (latitude and longitude), point-of-interest ("POI") address, POI phone, record of consent

Legal basis for the data processing is contract fulfillment pursuant to Art. 6 (1) lit. b) UK GDPR. To provide Online navigation services, we use a third party provider for Telematic Service as a data processor.

## 2.2 App Store

You can download or delete third party applications via the App Store. The App Store is provided by our third-party service provider Faurecia Clarion Electronics Europe, R. Soeiro Pereira Gomes Lote 1 3-Dto, 1600-196 Lisboa, Portugal as a data processor. The respective app providers are responsible for data processing in connection with the installation and use of the apps.

Data collected for the provision of the App Store: User ID, application download record.

Legal basis for the data processing is contract fulfillment pursuant to Art. 6 (1) lit. b) UK GDPR.

## 2.3 Voice Control

You can use voice control to activate vehicle functions through the voice assistant. You only need to say your command, and the system will help you complete the operation. In order to activate the voice assistant function you need to ensure that the voice assistant is activated in your vehicle privacy settings on the central display. After this function is turned on, native applications such as multimedia/navigation/voice assistant can be operated by voice command. Some functions such as multimedia/navigation can be operated by voice command without voice wake-up.

Collected data: Voice input, Device ID, longitude and latitude, coordinates, phone book contact information.

Legal basis for the data processing is contract fulfillment pursuant to Art. 6 (1) lit. b) UK GDPR.

To provide voice control functions, we use a third party cloud provider (Cerence B.V., CBS-weg 11, 6412 EX Heerlen, The Netherlands) as a data processor.

## 2.4 User Profile

You can create your individual user profile and store your preferred settings such as seat position, door mirrors and, if applicable, head up display). Your profile is connected with your smart ID. When you log in to the vehicle, your profile settings as well as further information you have provided in your smart account (e.g. username) will be loaded.

Collected data: Vehicle identification number (VIN), user ID, username, account type, ergonomic settings (e.g. seat adjustment, door mirrors and, if applicable, head up display).

Legal basis for the data processing is contract fulfillment pursuant to Art. 6 (1) lit. b) UK GDPR. Please note that after deactivating this function, you will not be able to use several vehicle connectivity functions, such as remote control and monitoring of the vehicle by mobile phone

(smart Hello App) and the use of digital keys.

To provide the personalized profile functions, we use a third party provider for Telematic Service as a data processor.

## 2.5 Weather

If you activate the weather function, this interface shows you the weather information based on your location and region.

Collected data: Vehicle information number (VIN), vehicle location (latitude and longitude), operator, model, device ID.

Legal basis for the data processing is contract fulfillment pursuant to Art. 6 (1) lit. b) UK GDPR.

To provide you with location based weather information, we use a third party provider for Telematic Service as a data processor.

## 2.6 Energy Management

The energy management function allows the user to set charging schedules and to select the time at which the vehicle's battery will be charged at a charging location. In addition, the user can choose whether the vehicle should be air-conditioned and the battery warmed up at the desired departure time.

Collected data: Travel time, charging time, air conditioning preheating, battery pre-temperature, user ID, energy consumption, electricity consumption.

Legal basis for the data processing is contract fulfillment pursuant to Art. 6 (1) lit. b) UK GDPR. To provide you with energy management services, we use a third party provider for Telematic Service as a data processor.

## 2.7 Online Music

Using the Online music function allows you to display the QR code of third-party application multimedia services (including Spotify, TuneIn). You scan the QR code to log in or you enter the username and password in the third-party multimedia service interface. It connects you to the third-party application multimedia service installed on the vehicle. You can activate or deactivate the online music function via the privacy settings. The respective providers are responsible for the processing of data in connection with the use of third party multimedia services.

Collected data: Record of consent or disapproval; information on the music collection (last song played, picture, Media ID, search records) will only be stored locally.

Legal basis for the data processing is contract fulfillment pursuant to Art. 6 (1) lit. b) UK GDPR.

---

To provide you with the online music function, we use a third party provider for Telematic Service as a data processor.

## 2.8 112 E-Call

The "EU Emergency Call" is an emergency assistance system regulated by the European Union and required by law. When you are in an emergency situation while driving, including but not limited to physical discomfort, encountering a safety threat, a safety accident, or an emergency response of the vehicle (such as airbag deployment), and you manually use/activate the function or the function is automatically triggered (such as when a vehicle airbag deploys), the E-Call system transfers data to the emergency call center of the emergency call system. An "EU emergency call" is made uniformly via the European emergency number 112.

Collected data: Emergency call trigger mode (automatic/manual), call trigger time, TCAM SIM number (vehicle built-in SIM number), vehicle information number (VIN), Vehicle type (passenger car or light-duty commercial vehicle), Vehicle energy/power type (gasoline/diesel/CNG/LPG/electricity/hydrogen), Vehicle location, Driving direction, Vehicle speed, Number of persons in the vehicle, Battery status, Door status, Vehicle collision status (collision location, collision type, collision acceleration, airbag status, anti-theft system status, etc.).

The recipients of the data processed by the in-vehicle E-Call system are the relevant public safety answering points designated by the relevant public safety authorities in their country (such as local police, hospitals, rescue agencies and your emergency contact for emergency rescue services) to first receive and process emergency calls to the European emergency number 112.

The data contained in the system memory is not available outside the system before the in-vehicle system is triggered. The in-vehicle E-Call system is untraceable and is not subject to any continuous tracking under normal operating conditions. The data in the internal memory of the in vehicle E-Call system can be automatically and continuously deleted. The vehicle position data is continuously overwritten in the system's internal memory in order to always maintain the latest vehicle location data required for the normal operation of the system. Activity data logs in the in-vehicle E-Call system are kept no longer than the time required to process an emergency call.

Legal basis for the data processing is our legal obligation pursuant to Art. 6 (1) lit. c) UK GDPR specifically our legal obligation pursuant to Regulation (EU) 2015/758.

## 2.9 Private E-Call

Instead of the 112 e-call, you can activate a Private E-call in the DHU settings. If you have selected the Private E-Call, the emergency call as well as the relevant data is not directed to the public safety answering points, but to a private provider (ARC Europe SA, Av. des Olympiades 2, 1140 Evere, Belgium) as a data processor.

---

Collected data: Vehicle information number (VIN), number of passengers, vehicle type, vehicle direction, car location, vehicle speed, usage mode and car mode. The provider of the Private E-Call may also collect additional information in order to provide you with further services. Legal basis for the data processing is contract fulfillment pursuant to Art. 6 (1) lit. b) UK GDPR.

To provide you with the Private E-Call function, we use a third party provider for Telematic Service as a data processor.

## 2.10 Roadside Assistance (B-Call)

The B-Call allows the user to contact a private roadside assistance provider in the event of a breakdown. Roadside assistance is provided by ARC Europe SA, Av. Des Olympiades 2, 1140 Evere, Belgium ("ARC") as a data processor. If the user triggers the B-Call, all relevant data about the vehicle's condition as well as the vehicle location are transmitted to ARC and a voice connection is established.

Collected data: Vehicle information number (VIN), vehicle location, license plate number, mobile phone number, mobile phone location, emergency contact name, emergency contact phone number, fault information (including fault code and fault light information). The provider of the B-Call may also collect additional information in order to provide you with further services.

Legal basis for the data processing is contract fulfillment pursuant to Art. 6 (1) lit. b) UK GDPR. To provide you with the B-Call function, we use a third party provider for Telematic Service as a data processor.

## 2.11 Stolen Vehicle Call (S-Call)

The purpose of the Stolen Vehicle Call is conducting stolen vehicle tracking service. Stolen Vehicle Call is provided by ARC Europe SA, Av. Des Olympiades 2, 1140 Evere, Belgium ("ARC"), as a data processor.

For this service, the following data is processed: Data provided by local authority, Vehicle location, Leasing description, if applicable, Main user, Caller/Driver Description, (such as but not limited to): Email/smart ID, First Name, Last Name, Gender/Salutation, Company, Phone Number, Language.

Legal basis for the data processing is contract fulfillment pursuant to Art. 6 para. 1 lit. b) UK GDPR.

## 2.12 Remote Vehicle Diagnostics

smart vehicles are equipped with a real time remote safety monitoring system, which is used to collect and save various system data of the vehicle to facilitate remote vehicle diagnostics, trouble detection, pre-warning for maintenance, fault and quality analysis as well as safety monitoring for your vehicle.

---

Collected data: Vehicle information number (VIN), Battery identification number (BIN), vehicle trouble codes originating from various vehicle components, position and motion data (such as time, position, speed, direction, pedal), Vehicle maintenance data (due date of next service), vehicle status information (including VIN and time stamp) of various components' control units including but not limited to battery, e-motor, ADAS, air condition, chassis, environment information (temperature, air pollution), e-motor, high voltage battery and alarm information, vehicle location data (longitude and latitude data), door and flap status/position/lock status and other functions as well as in specific cases log data of various components' control units.

Legal basis for the data processing is contract fulfillment pursuant to Art. 6 (1) lit. b) UK GDPR.

To provide you with real time remote safety monitoring, we use a third party provider for Telematic Service as a data processor.“

### 2.13 "Over-the-Air"-Software Updates (OTA)

The vehicle software (infotainment system, ECU firmware) can be updated via "over-the-air"-updates in order to obtain new functions, to provide system updates or to correct bugs and errors.

Collected data: Vehicle identification number (VIN), vehicle hardware and software version, software package, vehicle and software configuration information, operating system, date and time of software upgrade.

Legal basis for the data processing is contract fulfillment pursuant to Art. 6 (1) lit. b) UK GDPR. To provide you with OTA-Updates, we use a third party provider for Telematic Service as a data processor.

For customer support: In the unlikely event that OTA installation is aborted, the B-CALL can be triggered, Location and movement data (possible): Geo data, Vehicle status: before/after upgrade failure.

For continuous improvement of the OTA service: Vehicle configuration, Software configuration, e.g. release notes, date of publishment

In the unlikely event of an aborted the OTA where a roadside assistance is initiated, the following data is shared with the third-party support service: Vehicle Identification Number (VIN), Location and movement data: Geo data.

### 2.14 Online Services

This function requires the collection of your vehicle networking data and enables all functions which need access to the Internet.

---

This switch is disabled by default. With this function enabled you will be able to access vehicle related functions on the "Hello smart" App, including remote functions and digital key.

Legal basis for the data processing is contract fulfillment pursuant to Art. 6 (1) lit. b) UK GDPR. Please note that after deactivating this function, you will not be able to use several vehicle connectivity functions, such as remote control and monitoring of the vehicle by mobile phone ("Hello smart" App) and the use of digital keys.

## 2.15 Anti-theft system

The anti-theft system prevents others from illegally starting your vehicle. If the antitheft system is enabled, the vehicle status will be continuously monitored. The alarm will be triggered when the door/liftgate is not opened legally. If the remote anti-theft system is activated, a message that the vehicle cannot be started will pop up on the central display.

Collected data: Vehicle information, such as door open status, door lock status, windows open status, and trunk open status.

The vehicle is also equipped with a tracking system, which can track and locate the vehicle and remotely activate the antitheft system to prevent the vehicle from being started.

Collected data: Vehicle information number (VIN), event time, contact name, contact phone number, vehicle location before and after the event, vehicle information (model, color, language setting) for activating the stolen vehicle location service. When you activate the stolen vehicle location service, the vehicle will continuously upload the above information to our call center to provide the police or the user with vehicle location information to help locate the vehicle.

Legal basis for the data processing is contract fulfillment pursuant to Art. 6 (1) lit. b) UK GDPR. To provide you Anti-theft services, we use a third party provider for Telematic Service as a data processor.

## 2.16 Driver Drowsiness and Attention Warning (DDAW)

The "Driver Drowsiness and Attention Warning" system assesses the driver's alertness and warns the driver if necessary. DDAW function captures the movement of the driver's face including facial characteristics, such as eyelid opening and closing, length of eye closure, blinking frequency, etc. The data collected by DDAW is limited to the processing of the aforementioned monitoring of facial movements and remains in the vehicle and is not stored or transmitted. Legal basis for the data processing is our legal obligation pursuant to Art. 6 (1) lit. c) UK GDPR specifically the Regulation (EU) 2019/2144.

## 2.17 Valet Mode

Before handing over your vehicle to another person, you can turn on the Valet Mode for privacy protection. The Valet Mode can be activated either through tapping the user icon on the top right



---

corner on the central display or by opening the drop-down menu and selecting the Valet Mode in the smart modes tab. To activate the Valet Mode, you will be asked to enter a password on the central display. This password must also be used to deactivate the Valet Mode. If you activate the Valet Mode in your vehicle, the system will log out your profile ID. Certain functions such as Bluetooth, voice assistant and multimedia functions will be switched off leaving only the basic driving functions active.

Collected data: Vehicle identification number (VIN), driving status of the vehicle, the Valet Mode password and the network data required for the remote control of the mobile phone.

Legal basis for the data processing is contract fulfillment pursuant to Art. 6 (1) lit. b) UK GDPR.

## IV. OTHER VEHICLE COMPONENTS

### 1.1 Smart Vehicle Diagnostic System

Smart vehicle diagnostic system is used for diagnostic purposes. This system consists of giving repair technicians access to the status of the vehicle's various subsystems in order to detect or rectify a vehicle breakdown.

Collected data: vehicle identification number (VIN), vehicle model, ECU, software and hardware number, serial number, single vehicle test results, pincode VDN and translation, certificate information, flashing information (BSS, target software and hardware number, software package).

Legal basis for such data processing contract fulfillment according to Art. 6 para. 1 lit. b) UK GDPR.

### 1.2 Event Data Recorder (EDR)

Vehicles that fall under the regulation 2144 are equipped with an Event Data Recorder (EDR). EDRs are used in vehicles to record and store data in case of a collision in order to help provide a better understanding of the circumstances in which events occur.

The data stored in EDR must be accessed physically by a connection to the EDR (no remote access to EDR is possible). The data can only be accessed when requested by a customer or law enforcement.

Collected data: the data that the EDR is capable of recording and storing with respect of the period shortly before, during and immediately after a collision includes the vehicle's speed, braking, position and tilt of the vehicle on the road, the state and rate of activation of all its safety systems, 112-based eCall in-vehicle system, brake activation and relevant input parameters of the on-board active safety and accident avoidance systems.

Legal basis for collecting and processing above data is our legal obligation pursuant to Art. 6

para. 1 lit. c) UK GDPR and specifically the Regulation (EU) 2019/2144 requiring the presence of Event Data Recorders (EDR) in vehicles.

### 1.3 Vehicle Security Operations Center (VSOC)

Our Vehicle Security Operations Center (VSOC) safeguards your vehicle against potential and emerging cyber threats. It does that by detecting, overseeing and coordinating necessary measures in response to cybersecurity events and incidents. The vehicle's systems are continuously being monitored for abnormal and non-conforming activities that may indicate potential cyber threats. The primary purpose of this monitoring is to secure the vehicle's electronic components' functionality as well as its integrity – and therefore to protect the vehicle itself, its drivers and passengers.

Collected data: General data such as vehicle identification number (VIN) and report time, network traffic data such as device traffic statistics and information (e.g. Wi-Fi receive and send traffic data, device receive and send data), internet connection information such as connection details and local ports, Wi-Fi information and status, manufacturer information (e.g. vehicle model and brand), system information (system version and type) as well as device hardware information, security configuration information system operating status information, GPS-, camera- and microphone usage information, system log collection, collection of security configuration information.

Legal basis for collecting and processing above data is our legal obligation pursuant to Art. 6 (1) lit. c) UK GDPR and specifically the UN Regulation No. 155 requiring the presence of a cybersecurity management system (CSMS) in vehicles.

## V. WHEN YOU CONTACT US

When you contact us via the contact form provided on our website, via e-mail, phone or direct message, using the chat and voice function provided on our website, the personal data transmitted with your request (i.e. your contact details and the information you provide) will be stored. We only use this data for processing your request.

Legal basis for such data processing is our legitimate interest to process your request pursuant to Art. 6 (1) lit. f UK GDPR or Art. 6 (1) lit. b UK GDPR, if the request is directed to the conclusion or performance of a contract. The data will be deleted when the purpose of the processing no longer applies, e.g. your request has been answered conclusively.

## VI. CUSTOMER CARE AND AFTER SALES SERVICES

When you contact our customer service online, we will offer you automated chat and voice functions which will not process personal data unless you choose the option to continue a live chat with an agent. After 90 days your conversation with the chat and voice functions will be deleted.

To provide you with customer service including verification purposes as well as trouble shooting and issue resolution in accordance with customer care and aftersales processes. It is possible third party service providers (customer engagement center, retailer engagement center, smart Authorized Service Partners and other third party providers such as ABB E-Mobility B.V., Heertjeslaan 6, 2629JG – Delft/NL) will also be share this data to further assist the customer, we will also use this data for daily operation business including but not limited to repair and maintenance, we will collect your name, mobile phone number, vehicle information number (VIN), license plate number, model, address, city, and authorized service provider/repair site information.

Legal basis for the processing of your data is contract fulfillment pursuant to Article 6 (1) b UK GDPR.

## VII. FOR PERSONALIZED PRODUCTS AND SERVICES AND MARKETING

The data we have collected can be used for marketing purposes by the smart Ecosystem based on your consent.

- What marketing purposes does our smart Ecosystem have?

We would like to inform you about new products, services and special offers of the smart Ecosystem and its Service Partners (Finance and Leasing) via email (e.g. Newsletter), telephone (including direct messages), postal mailings or push-notification either by smart or your preferred local smart Agent you have selected in the Self Care Portal. We also would like you to participate in our customer surveys to let us know where we can improve our service and products.

How do we collect your consent? We collect your consent either online or on site at your local smart smart Agent or Authorised Service Partners.

- How do we verify your email address?

We use the double opt-in procedure to verify your e-mail address. After subscribing to our newsletter, you will receive an e-mail from us in which you have to confirm your consent again with a mouse click.

- How can you revoke your consent?

You can always change your marketing consent settings manually in the Self Care Portal under "Settings" in your smart account or you can unsubscribe from the newsletter manually. You may also call our Service Center at any time for support.

- Which data do we process for marketing?

Before we collect your consent we inform you about the type of data we process and the specific purpose of processing, e.g. for email newsletters, events we use your e-mail address, for future

products in case you gave us information about your interests or hobbies, how you use our website, which messages you open, which areas you click, your purchase history, your payment method, how you interact with smart and your sales channel (online or at the local retailer) we may use this information to be able to provide you with special offers tailored to your interests.

- Which data do we process for surveys, questionnaires and market research?

With your consent for surveys and questionnaires, we may send you personalized customer satisfaction surveys, questionnaires and conduct market research to gather feedback on our products and services and to better understand customer preferences. The data we process includes your first name, last name, email address, country, phone number, purchase history (e.g. vehicle model you purchased, date of purchase, order status and shopping cart information), preferred smart Agent, test drive details (e.g. booked or completed test drives), interactions with Customer Service and workshop information (e.g. appointments and repairs). Before taking any survey, we will inform you whether your responses will remain anonymous. Please note that your consent is voluntary and can be withdrawn at any time in your account settings.

- With whom do we share your data?

We only share your data with the companies in the smart Ecosystem that you have selected for one of the following examples: test drive, appointment on site, vehicle handover, trade-in etc. An overview of the smart Agents and Authorised Service Partners for whom your consent applies can be found at any time in the Self-Care Portal.

- When do we delete your data?

Your data will be deleted after your deletion request via your account, when you unsubscribe from our email-newsletter or you send a deletion request to our Service Center. We automatically delete your data if you have not interacted with us after a certain period of time.

## VIII. FOR PRODUCT AND SERVICE IMPROVEMENT

In order to improve and optimize our products and services, and to help you troubleshoot and analyze the problems you may encounter when using products or services through various channels, we will collect and store your problem feedback information and various operation log information (including crash information, device information and error logs). In addition, in order to provide you with a better service experience, when you give feedback and comments on the product, we will collect and store the feedback and comments to analyze user satisfaction.

Legal basis for the processing of your data is our legitimate interest pursuant to Article 6 (1) f UK GDPR to improve our products and services.

## IX. HOW TO EXERCISE YOUR DATA SUBJECT RIGHTS

You have the following rights in connection with the processing of your personal data, subject

to the conditions set out in the UK GDPR:

### Right to access

You have the right to be informed about which data we collect from or about you, for what purpose we process your data and with who we share your data with. You may contact us via [eu.dataprotection@smart.com](mailto:eu.dataprotection@smart.com) to submit an access request.

### Right to rectification

If we hold inaccurate personal data about you, you have the right to request rectification. In general, you can use the following methods in the Hello smart App to change or modify your personal information:

Click "My" - "Settings" - "Personal Information", you can update your avatar, modify your nickname, signature, gender, birthday, use (purchase) car area, hobbies, mobile phone number, and modify or add delivery address. You may always contact us via [eu.dataprotection@smart.com](mailto:eu.dataprotection@smart.com).

### Right to erasure

You can delete your account by visiting the Self Care Portal. You can also contact our Customer Service Center (see contact details in section I above). When you delete your account (through the Self Care Portal or by contacting our Customer Service Center) all data except the data we are legally obliged to retain will be deleted. You will be informed about the deletion process.

For further information we are obliged to delete your personal data without delay where one of the following grounds applies:

- Your personal data is no longer required for the purpose for which it was collected or otherwise processed.
- You are withdrawing your consent and there are no other legal grounds for processing that data.
- You are filing an objection (see below) to the data processing.
- Your personal data was unlawfully processed.
- The deletion of your personal data is necessary to fulfil an obligation under EU law or the law of the Member States.

### Right to restriction

You have the right to request a restriction of our data processing when one of the following conditions are met:

- you are contesting the accuracy of the personal data,
- the data processing is unlawful, but you do not agree to the deletion of the personal data, instead requesting a restriction of its use,

- we no longer need the personal data for the purposes of processing, but you need the data to establish, exercise or defend legal claims; or
- you have objected to processing (see below) and it is not yet clear whether our legitimate interest will prevail.

If you want to request a restriction of processing your personal data, you can contact our Customer Service Center (see contact details in section I) or your local smart Agent. You can also restrict / manage your data via the Privacy settings in the Self Care Portal.

### Right to data portability

If you want to receive the personal data you have provided to us in a structured, commonly used and machine-readable format you can contact smart EU or your local smart Agent. You can also request to have the data transferred to another controller without interference on our part provided that:

- the processing is based on consent granted pursuant to Art. 6 (1) lit. a UK GDPR or Art.9 (2) lit. a UK GDPR or on a contract fulfillment pursuant to Art. 6 (1) lit. b UK GDPR; and
- the processing is carried out using automated methods.

In exercising this right, you may request that personal data related to you be transferred directly from us to another controller insofar as this is technically feasible and does not infringe on the freedoms and rights of any other person.

### Right to object

You have the right to object to our processing of your personal data unless it is based on one of the following grounds:

- the processing of your personal data by us is required for the fulfilment of a task that lies in the public interest or in the exercise of public authority that has been delegated to us; or
- the processing is necessary to safeguard our legitimate interest or the legitimate interest of a third-party, in so far as your interests or basic rights that require protection of your personal data do not prevail.

The right to object also applies to profiling based on these processes.

If the personal data that concerns you is being processed for direct marketing purposes, you have the right to object to the processing of your personal data for such marketing purposes. This also applies to profiling insofar as it is associated with such direct marketing.

You also have the right, on grounds arising from your particular personal situation to object to the processing of your personal data by us for scientific or historical research purposes or for statistical purposes, unless such processing is necessary for the performance of a task in the public interest.

If you want to object to the processing of your personal data, please contact our Customer Service Center (see contact details in section I) or your local smart Agent.

### Right to withdraw consent

You may revoke your consent at any time with future effect. Processing of your data which occurred prior to the withdrawal of consent is not affected.

If you wish to exercise any of the above rights, you can contact us by email at eu.dataprotection@smart.com. Upon receipt of your request, we may first verify your identity and may ask you to provide necessary information for authentication.

### Mobile device authorizations

You may change or revoke our authorization to process your personal information at any time. You can make changes through your hardware device or permanently revoke all of our authorization to continue to collect your personal information by deleting your account.

### Right to lodge a complaint

If you believe that the processing of your personal data violates legal requirements, you have the right to lodge a complaint to the Information Commissioner's Office (ICO) which regulates the processing of personal data in the UK (Art. 77 UK GDPR).

The ICO's address:

Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

ICO website: <https://www.ico.org.uk>

Our lead data protection supervisory authority is:

State Commissioner for Data Protection and Freedom of Information in Baden-Württemberg

Address: Lautenschlagerstraße 20, D- 70173 Stuttgart

Postal address: Postfach 10 29 32, 70025 Stuttgart

Telephone: +49 711/61 55 41-0

Email: [poststelle@lfdi.bwl.de](mailto:poststelle@lfdi.bwl.de)

<https://www.baden-wuerttemberg.datenschutz.de/online-beschwerde/>

You can also lodge a complaint with your local supervisory authority.

## X. CANCELLATION OF YOUR ACCOUNT

You may delete your smart account at any time. You can do this on our website by accessing "My" - "Settings" - "Delete Account" on the "smart" account page; or call our Customer Engagement Team to assist you in deletion.

Once you delete your smart account, you will not be able to log in and use all user products and services. We will delete all information about your account (including related information associated with third parties), unless otherwise provided by law. So please proceed with caution.

## **XI. DATA TRANSMISSION TO RECIPIENTS OUTSIDE OF THE EU AND EEA**

When using service providers and sharing data with third parties, personal data may be transferred to recipients in countries outside the UK, EU and EEA (Iceland, Liechtenstein and Norway) and processed there, in particular in China, USA and India.

For example, we must share data (e.g. Vehicle Identification Number (VIN)) with the manufacturer smart Automobile Co. Ltd, No. 859, Binhai 4th Rd, Hangzhou Bay New District, Ningbo, Zhejiang ProFINce, P. R. China, including, where applicable, the manufacturer's service providers, as necessary to process product liability and warranty claims as well as in specific cases for troubleshooting requests.

In the following countries, from the UK's and EU's point of view, there is an adequate level of personal data protection (so-called "adequacy"), in compliance with EU and UK standards: Andorra, Argentina, Canada (limited to commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland the United Kingdom, the United States (limited to commercial organizations participating in the EU-US Data Privacy Framework) and Uruguay. We agree with recipients in other countries on the use of EU and UK standard contractual clauses, binding corporate rules or other applicable instruments (if any) to create an "adequate level of protection" according to legal requirements. For more information, please contact us: [eu.dataprotection@smart.com](mailto:eu.dataprotection@smart.com).

## **XII. UPDATES TO THIS PRIVACY STATEMENT**

We may change and modify this Privacy Statement from time to time, for example as a result of updates to our products and services and any updates to relevant laws and regulations. We will provide our users with notice of any significant changes to this Privacy Statement, but we would also ask that you re-read this Privacy Statement from time to time.

Last update: November 2024