WESTERN POWER DISTRIBUTION

INNOVATION

NEXT GENERATION NETWORKS

CarConnect
Data Protection Strategy

LCN Fund
Low Carbon Networks

Report Title	:	CarConnect Data Protection Strategy
Report Status	:	FINAL
Project Ref	:	NIA_WPD_013
Date	:	15.06.2016

Document Control		
	Name	Date
Prepared by:	Gill Nowell	10.06.2016
Reviewed by:	Daniel Hollingworth	10.06.2016
Recommended by:	Ben Godfrey	13.06.2016
Approved (WPD):	Roger Hey	15.06.2016

Revision History		
Date	Issue	Status
26.05.2016	1.0	Draft
10.06.2016	1.2	FINAL

Contents

Personal data *refers to data that relates to a living individual who can be identified from those data or from those data and other information that is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (s.1 (1) Data Protection Act 1998)*

1. Introduction

CarConnect[1] is a Network Innovation Allowance research and development project (the "Project"). It is anticipated that the number of Plug in Vehicles (PIVs – Battery Electric Vehicles and Plug in Hybrid Electric Vehicles) will increase significantly over the coming years. This will present a challenge to the GB Distribution Network Operators (DNOs). The Project will develop a strategy to help DNOs minimise this impact.

The Project will be directed by Western Power Distribution ("WPD") and delivered by a partnership of EA Technology, Fleetdrive Management Limited (trading as "DriveElectric") and Lucy Electric Gridkey. EA Technology will be responsible for project management and management of the V2G trial. DriveElectric will be responsible for recruitment of customer trial volunteers and all practical aspects of operating the customer trial. Most importantly, from a data protection perspective, DriveElectric will supply vehicle related trial data whilst EA Technology will use this data in an anonymised format to develop a PIV demand control algorithm in conjunction with Greenflux and CrowdCharge. EA Technology will be responsible for the analysis and reporting of all trial data. Lucy Electric Gridkey will be responsible for collecting and processing LV substation data.

The Project is a mass market trial of PIV/V2G demand control services. This trial will inform the development of an LV Network Assessment Tool and functional specification and commercial framework for PIV Demand Control. Together these will enable DNOs to adopt and implement PIV demand Control services effectively and efficiently as the PIV market penetration grows. Up to 700 new PIV drivers will be recruited to the project from WPD licence areas in order to provide the project with statistically significant data. Project data will be used to develop a control algorithm and research customer behaviours relating to car charging and journey planning. Customer acceptance of charging restrictions will be assessed by a contracted market research company.

DriveElectric will act as 'Data Controller' for the Project. DriveElectric has 18 years' experience in managing customer data through its car lease business and experience in implementing Data Protection procedures across project partners and suppliers.

This data protection strategy covers key questions surrounding how the Project will handle customer and technical data from the initial data capture until the cessation of project

[1] 'CarConnect' is the formal and registered project name for contractual and reporting purposes. The brand name may be different for customer-facing recruitment and dissemination purposes.

activities to the point at which data is destroyed. The strategy also outlines the data security mechanisms being implemented to ensure the security of personal data. These are in accordance with requirements of the Data Protection Act 1998.

If any aspects of the Data Protection Strategy change during the Project's lifecycle, a revised version of this document will be submitted to Ofgem for approval.

2. Key Questions Answered

The Project will collect customer contact, socio-economic data, car usage data and project feedback as well as electrical usage for PIV charging and network information.

This document describes the data protection measures for customer data to be undertaken by DriveElectric and Project Partners or subcontractors contracted to collect, or to perform analytics and modelling using the data.

Diagram a) in section 4 illustrates the overall data flow for the

a) What personal data will be collected for the purposes of the Project?

The Project will collect name, address, telephone number, and email address during recruitment. Note that at no point will sensitive personal data[2] (as defined by the Information Commissioners Office) be collected or recorded as part of this project.

The Project will also collect a number of parameters from participants' vehicles including vehicle state of charge, journey characteristics and car charging patterns, as well as electrical parameters pertaining to the charging of the electric vehicles such as Voltage and Current.

For marketing purposes, customers may be asked to provide quotes for project materials, or to be photographed with their PIVs in their local area or street, by Project Partners. In this instance, customers will be asked for permission prior to any photographs being taken and their consent will be recorded (via a separate consent form). Any photographs used for marketing purposes will only show basic information; only first names and local town/city will be presented with the photograph. The photographs taken will only be used to promote the Project as agreed with the customer at the time of giving consent.

Behavioural information and participant feedback will be collected via a number of different methods, depending on which the participant prefers. This could include

[2] For definition of 'sensitive personal data' see:
http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx

online or written weekly surveys, face-to-face, telephone or email interviews, and focus groups. Residential information will be collected using simple questionnaires.

DriveElectric may collect financial data to allow participants to be part of an incentive scheme for payment purposes only. If this is required this data will be collected via a questionnaire.

The personal non-financial data required in the Project will be collected by DriveElectric, the customer survey sub-contractor or potentially the Mobile App.

b) How will the personal data be used?

The personal non-financial data will be used for technical and socio-economic modelling to understand how the technical solution can be used, the settings required and the benefit that can be achieved. Where possible, the data will be used in an anonymous format. Personal data will only be shared for modelling purposes with stakeholders who are data controllers.

Necessary details such as the name and address of trial participants will be passed to a sub-contractor/s appointed by DriveElectric to provide charge point surveying and installation services. These sub-contractors would act as data controllers in accordance with requirements of the Data Protection Act 1998. As part of the installation process the installer will inform the relevant DNO that a charging point is being fitted as required by the IET's Code of Practice on Electric Vehicle Charging Equipment Installation (this is a process outside the boundaries of the Project).

The address and details of where each charging point is installed will be recorded in an asset management database. This asset management database will be used for maintenance purposes and to allow the speedy resolution of any faults. This will be held by DriveElectric.

WPD will be informed of the addresses where any charge point is installed for information purposes. This would only include the data that they would receive from the notification form as part of the installation process in line with their role as a DNO, in order for them to check that the electric vehicle charge point notifications have been sent to the DNO by the charging point installer. Where a customer is domiciled outside of WPD's licence area, the relevant DNO will be issued with the same information.

Data will also be collected from the PIVs via a Demand Control System ("DCS"). This data is collected from all customers (with their permission). Individuals cannot be identified from the data, therefore it is non-personal information. The data will be stored in accordance with DCS data protection and encryption protocols to which the customers have already agreed. Data will be downloaded as a batch process, the

frequency of which will be determined to balance the need to check the data is correctly recorded without being burdensome on the DCS. Data will be transferred in accordance with the protection measures outlined in this document.

Non-personal data required in the Project will be collected by Lucy Electric Gridkey.

Personal data may be collected by the PIV demand control service providers (Greenflux and CrowdCharge) ahead of inclusion within the project. If the PIV demand control service providers plan or intend to gather personal information from customers then we will require them to register with the Information Commissioners Office as data controllers and comply with the 1998 Data Protection Act. As such a flow of information may come from the service provider to DriveElectric via a secure API.

c) How will consent for use of the personal data be obtained?

All customers participating in the Project will give their consent in a form which will be similar to that included in Appendix A. This will form part of the document pack sent to participants. The Project's Customer Engagement and Recruitment Plan details the full engagement strategy.

DriveElectric will write into contracts with Project Partners and contractors that data shared with Project Partners as part of the Project, and consented to by customers, will not be used for any other purposes than those agreed with the customer for this Project. For example, as a default, Project Partners will not use contact information for their own marketing purposes. DriveElectric will control access to non-financial data and only allow Project Partners to have access to the information that they require to fulfil their tasks within the Project.

Customers will be asked for permission for the Project Partners to take photographs of them. Customers' consent will be recorded in a separate consent form which will state how the photograph will be stored, for what purposes it will be used, and what other personal information will be presented with the photograph (i.e. first name and local town/city only). Customers will be able to withdraw their consent for any photograph of them to be used in marketing material, on the condition that they notify DriveElectric in writing before marketing material is issued for publication.

Project Partners will ask customers' permission to include agreed personal information in marketing materials (e.g. press releases). Marketing material including personal information will not be signed off for publication by EA Technology unless permission has been granted. Customers will be able to withdraw their consent for their personal information to be used in marketing material, on the condition that they notify DriveElectric in writing before marketing material is signed

off. All marketing materials must be signed off by EA Technology prior to dissemination or publication.

d) What information will be provided to the customer prior to consent being sought?

All customers seeking participation will be provided with details and purposes of the Project including:

- Future predictions for PIVs and their impact on networks and the need for the Project
- Objectives of the Project
- The identities of the Project Partners
- Funding for the Project
- A brief summary of how they can be involved in the Project, including information on the customer research subcontractor, their obligations as a trial customer, and the timescales of the Project.

The full engagement strategy is given in the Customer Engagement Plan.

e) If Priority Services Register Customers are included in the Project, how will their personal data be obtained?

If Priority service register customers volunteer for the Project and are eligible (as with any volunteer), their personal data will either be collected automatically or in a manner appropriate to their needs. For example, if the customer research subcontractor is collecting customer feedback they will use telephone calls or a face-to-face conversation if this is easier than internet.

f) Who owns the personal data? How long will the personal data be retained?

DriveElectric will be the data controller for all data for the research purposes as it will determine the purposes for which and the manner in which the personal data are processed. This also removes any need for personal data to be moved between parties unnecessarily, which could inherently weaken the protection of customer data. Project suppliers (for example Lucy Electric Gridkey) will also act as holder for non-personal information including electrical parameters which are not attributable to individual households.

The customer will own the personal data that relates to them and have rights under the Data Protection Act 1998 including, but not limited to requesting access to their personal data and request amendments (in writing or orally if they cannot make a request in writing) to inaccuracies at any time.

As part of the Project's close down procedure, all personal data will be anonymised and the original personal data will be permanently deleted. Any personal financial data necessary for the incentive scheme (held by DriveElectric in their CRM database) will be retained on a secure server for the duration of the trial and permanently destroyed afterwards.

Following the Project's close-down, Project Partners may only retain anonymised results of their analysis.

DriveElectric is the sole Project Partner who has an absolute need to access customers' financial data in order to manage the trial incentive scheme; for this reason it is appropriate that DriveElectric will also be the data controller for all personal financial data processed in relation to the Project. This eliminates any need for movement of financial data from one party to another. Personal financial data will be retained on a secure server for the duration of the trial and permanently destroyed afterwards.

g) How will data be securely transmitted?

Data transfer to and from the secure database, the research (non-DriveElectric) database and between Project Partners must use the following security:

- Wherever possible customers will be referred to via a unique ID number rather than use personal details. The CRM database will provide access via the Unique ID to personal details only by secure password access and only to the users who are defined as authorised to access this information.
- All spreadsheets will be password protected with the password transferred separately to the spreadsheet; only anonymised data will be handled in this way; they will only be passed between project partners and sub-contractors as a measure of last resort and via secure password protected online storage
- All transfer of data will be via secure password protected online storage e.g. SharePoint, Dropbox or similar
- Data will be transferred using a secure website accessed using https or transmitted using secure file transfer (either FTPS or SFTP)
- Personal data will be sent separately to other data (e.g. demand and voltage data should be sent separately to names)
- In all cases data will not be sent by email or printed from other non-protected format
- Where email of a spreadsheet is the only way data can be transferred it must be password protected and DriveElectric must be informed that this type of transfer is taking place via our compliance officer

- Passwords must be relayed via 'phone after correct checking for ID of respondent and not written down

With respect to data transmitted from substations, individuals will not be identifiable. The following checks will be taken to ensure that the data has not been tampered with:

1. An 'Open Trust' model is employed internally within the software meaning that information is able to pass freely. This type of model is secure for data and control handling of software implemented within a single micro-processor. It can also be used for when two or more micro-processors are contained within the same physical unit. Anti-tamper facilities will be added to physical units if required.
2. Encryption will be employed between physical devices if they are in different locations or are vulnerable to attack in one place. Encrypting and decrypting will be performed using fixed known keys or patterns stored in each device.
3. A 'Closed' Architecture is employed for the system. This means that each network is given a unique code and nodes are set up only to join that node. It also means that there is a unique way of identifying the devices on the network.

The following outlines the security of the equipment and how it does not compromise the secure control of the network or the data.

h) How will data be stored securely?

All personal data and non-personal data, with the exception of financial and credit rating information, will be stored on a central database. Personal details (Names, addresses, other contact details) required for the project will be held on the DriveElectric Customer Relationship Manager (CRM) database. Technical data (car usage information, electrical parameters, network information) will be stored on the DriveElectric Application Interface (API) database. Project Partners will be responsible for uploading data to the central databases which will be hosted by DriveElectric (in a data centre within the European Union) with the following security measures:

- DriveElectric will manage the databases and control access and visibility of data sets to each of the Project Partners
- DriveElectric will also manage permissions on the databases, allowing Project Partner users to have access only to fields appropriate to them. Permissions will be controlled by either assigning Windows based or SQL based authentication or a similar level of security
- The servers will reject communications from unauthorised devices
- The databases will use non-standard names (security through obscurity)

- Project partners downloading data or accessing data for analysis and modelling purposes (other than the customer research sub-contractor) will only be able to access data in an anonymised format (i.e. no personal data)

Personal data will not be stored on any portable device e.g. mobile 'phone or tablet used to gather registration detail by the PIV data control service providers. This data will be transmitted directly to the DriveElectric CM database and destroyed from the device once successfully transmitted. Identification of customers, their cars and their homes within the PIV demand control system and applications will be by code and thus anonymised.

The customer research sub-contractor will be responsible for uploading data to the DriveElectric CRM database using the security measures outlined below. This will allow the results of the customer research to be shared with relevant project partners such as CrowdCharge.

The sub-contractor who will be commissioned to carry out consumer research for the project will be suitably qualified and registered with the Information Commissioner's Office at a 'Data Controller' under the Data Protection Act 1998. It will be necessary for the customer research sub-contractor to download personal data (email addresses, first and last names, other contact details) from the DriveElectric database. It may be necessary for them to upload some of this data into a separate database provided by a specialised survey software provider. This will allow the questionnaire to be programmed appropriately as required, and administered at the correct times, to the correct participants throughout the trial period. The customer research sub-contractor will have access to this database; no other Project Partners or suppliers will be granted access. Therefore the customer research sub-contractor will be responsible for ensuring that the necessary security measures are undertaken as specified by the Data Protection Act 1998 and the Information Commissioner's Office.

As data controller of customers' financial data DriveElectric will employ the following security measures. DriveElectric is registered with the Information Commissioners Office for Data handling (Registration no. Z8537104). DriveElectric is audited annually by an industry body, the British Vehicle Rental and Leasing Association to check on procedures used to deal with customers. Procedures include the following steps to ensure security of data especially in reference to financial applications:

- Use minimal paper copies of applications and where these are generated they will be shredded once completed
- Any scanned copies are securely archived on DriveElectric's password protected server and only emailed to or directly uploaded onto secure bank systems

- All staff have data protection and anti-money laundering training as part of FCA requirements
  - No disclosure of account details unless caller can be identified
  - Appropriate checks made on identity
  - Being aware of possible fraudulent applications.

Data may be collected from customers and recorded on paper (e.g. face to face interviews or telephone conversations). For this type of information, the Project Partners must follow the security measures listed below:

- Avoid recording personal data with other recorded data as much as possible, e.g. recordings of interviews labelled by number rather than names, and records identifying names to numbers kept separately
- Keep laptops password protected and attended at all times
- Encrypt files containing personal data
- Keep paper copies of notes attended at all times
- Upload securely to the central server as soon as practically possible and destroy paper copies generated prior to the upload when no longer in use.

Network Security:

A firewall enforces access policies such as what Data Services are allowed to be accessed by the network users.

During analysis Project Partners may store information locally, and for the research element of the Project, on a separate (DriveElectric) database provided by a specialised survey software provider. The following measures will be taken:

- Avoid storing personal records with other data as much as possible (e.g. use person 1, person 2 or other non-identifiable labelling systems).
- All computers must be password protected and where relevant, software programmes will also be password protected.
- Encrypt files with personal data.
- Analysis should be only undertaken in secure premises with controlled access.

i) How will data or analysis be published?

Results, data or analysis will be published in an anonymous format and will only be published with the permission of DriveElectric and other collaborative partners. All results, data and analysis published by the Project will be aggregated. Location information will be limited to a town/district. Harm tests will be done on behavioural

data to ensure that people cannot be identified from publications unless an individual has given express permission for their details to be made available, for example in a case study or newsletter.

3. Data Collection and Storage Summary Table

The data required in the Project will be collected by:

- DriveElectric
- EA Technology
- GreenFlux
- CrowdCharge
- Lucy Electric Gridkey
- the customer survey sub-contractor

The table below gives the list of data and who will be collecting, transmitting, storing and using it. If any other Project Partner or subcontractor collects or uses data they must do so in accordance with this strategy and with permission from DriveElectric.

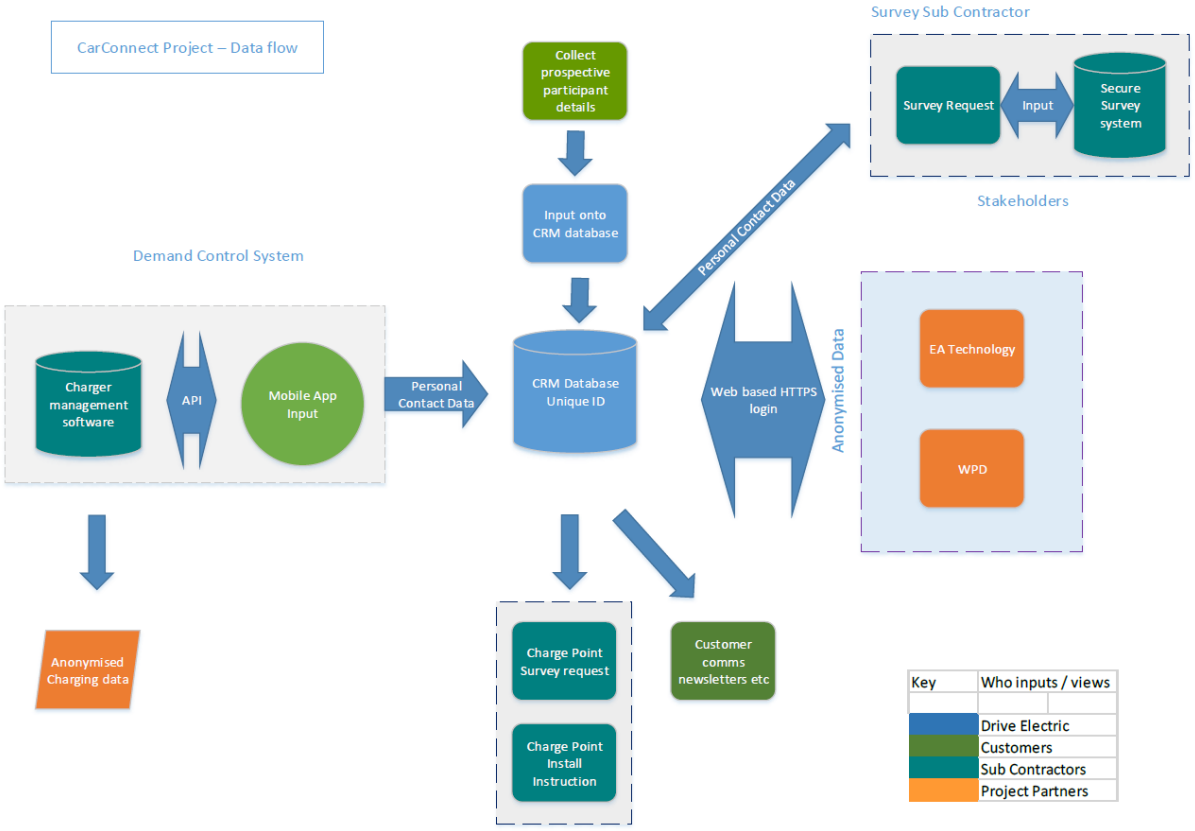
Data	Who collects the data	Where/how is data recorded	Who transmits the data	Where is the data stored	Who will use the data?
Contact details	DriveElectric	DriveElectric	DriveElectric	DriveElectric CM database	DriveElectric Customer research sub-contractor
Driving habits	Greenflux CrowdCharge	DriveElectric API database	PIV provider	DriveElectric API database	EA Technology Greenflux CrowdCharge
Socio-economic data	Customer research sub-contractor	DriveElectric database	Customer research sub-contractor	DriveElectric CM database	Customer research sub-contractor EA Technology
Project Feedback	Customer research sub-contractor	DriveElectric database	Customer research sub-contractor	DriveElectric CM database	DriveElectric EA Technology
Photos	DriveElectric EA Technology	Secure project SharePoint site	EA Technology	Secure project SharePoint site	EA Technology
Financial Data	DriveElectric	DriveElectric	Data will not be transmitted	Central DriveElectric database	DriveElectric
Monitoring data (non-personal)	Lucy Electric Gridkey	Lucy Electric Gridkey database	Lucy Electric Gridkey	Lucy Electric Gridkey database	Lucy Electric Gridkey EA Technology Greenflux CrowdCharge

Table 1: Indicative structure of data collection and use for CarConnect

4. Diagrams: CarConnect Data Flow and Management

a) Data flow

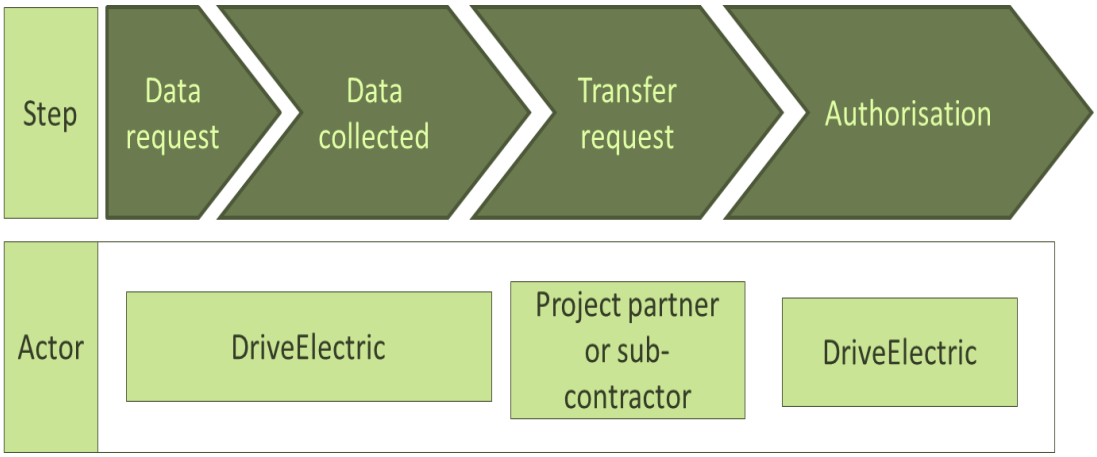
The following diagrams illustrate the data flow for this Project.



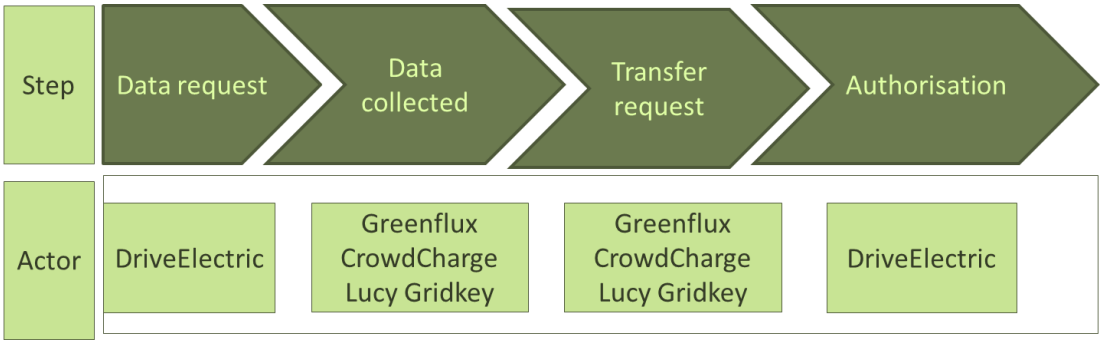
DriveElectric will hold the right to perform an audit on the data protection measures Project Partners or contractors use when collecting or handling data (essentially at any time throughout the Project).

b) Data collection and upload

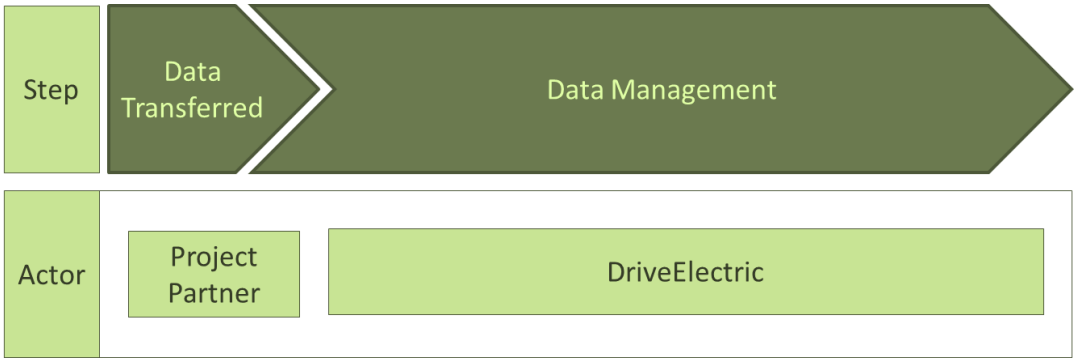
Personal Data – DriveElectric CRM database



Technical Data

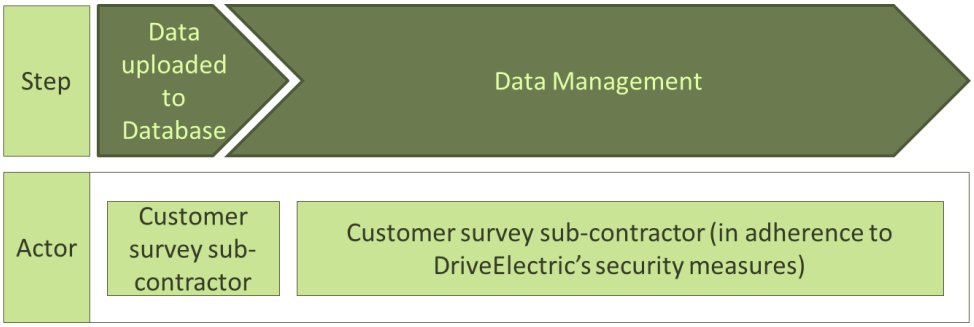


c) Data management within DriveElectric Database



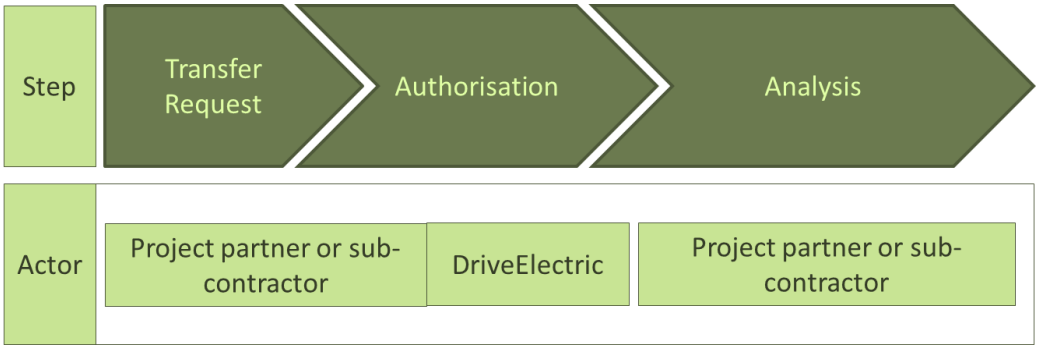
Once data is transferred to DriveElectric's secure database, DriveElectric is responsible for the security of the data shared and who has access to it.

d) Data Management within research database



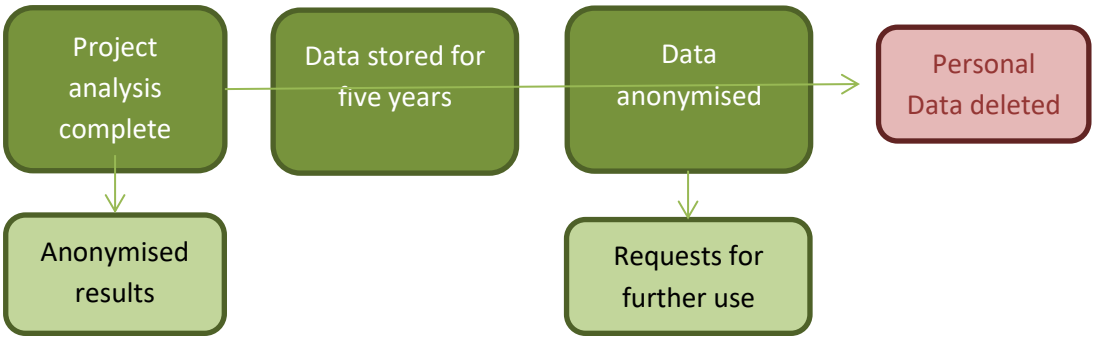
Once data is requested, and uploaded into the specialised survey software and research database, the customer survey sub-contractor will be responsible for management of this data. The customer survey sub-contractor will manage this data through adhering to DriveElectric's security measures as outlined within this document.

e) Data download / analysis



Project Partners will have access to the parts of the database relevant to the work they are undertaking within the Project and will be unable to access any area of the dataset not required for the role they hold within the Project.

f) Data anonymisation and / or destruction phase



Should any of the Project Partners or in particular the customer survey sub-contractor or participants wish to publish any of the results from this Project, they will be obliged to share the content to be published (results and accompanying analysis) with DriveElectric in advance of publication, to obtain authorisation.

Appendix A – Draft Customer Consent Form Wording

Consent form: to have a Plug-In Vehicle (PIV) charging point installed and be subject to PIV demand control, to allow your data to be gathered, and to participate in the CarConnect trial.

(Customer Copy)

As part of participating in the CarConnect project (the project) I give permission for DriveElectric, and participating companies in the project (known as the 'project team') (including Western Power Distribution (WPD) and their authorised partners and agents) to install a Plug-In Vehicle (PIV) charging point at my address to gather information about the electrical energy required to charge a PIV and what impact that has on the local electricity network in order to predict what future use of PIVs might look like. This has no impact on my energy supplier.

I agree to participate in surveys about my experience as a condition of participation.

I further acknowledge and accept that the information and data gathered from my property may be used by the project team to create statistics, validate models, and analyse customer behaviour. The project team may combine this information with other publically available information and my address to help build a network model and allow WPD to continue to deliver an electricity network for customers' needs.

The information will be collected by a vehicle charger and transmitted via secure internet connection.

I consent to my charging point being controlled remotely and understand that this may limit the ability to charge at certain times of day.

The charging points will be installed by a sub-contractor and located in an agreed place in my premises for charging my PIV. There will be a record of each monitor's serial/batch number and location. I agree to my details being passed to the subcontractor for the purpose of arranging a pre – installation survey and installation of the PIV charging equipment

To provide a good service and meeting regulatory and legal responsibilities, I acknowledge and accept that the project team may monitor and record any communications they have with me, including telephone conversations and e-mails. When they contact me, they may use any information they hold about me to do so. They may contact me by letter, e-mail, telephone, text message and other forms of electronic communications or by visiting me. They will agree a preferred method of communication with me in advance.

I am entitled to have a copy of the information DriveElectric, its partners and its agents hold on me, and to have any inaccurate information corrected.

I may have a copy of the information that is collected from me. This information is specific to me at my address and my vehicle and therefore, in the event that I sell or cease to

occupy the address which is connected to a charging point and linked to a substation monitor, as part of the project I agree to notify DriveElectric or WPD within 14 days of any sale, letting or underletting or any parting with possession of my property, or sale or cessation of use of my PIV.

By signing this consent form, I confirm that I have read, understood and agree to the terms and conditions of participating in this project, and have read, understood and agree to the processes detailed in the Customer Information pack. In addition, by signing this, I agree to receiving contact about CarConnect-related information from the project team.

Name: ……..

Signed: …….. **Date:** ……

Appendix B – Privacy Statement

Privacy Policy

We (DriveElectric), the data controller, are committed to safeguarding the privacy of our customers; this policy sets out how we will treat your personal information. Our website uses cookies. By using our website and agreeing to this policy, you consent to our use of cookies in accordance with the terms of this policy.

(1) What information do we collect?

We may collect, store and use the following kinds of personal information:
(a) information about your computer and about your visits to and use of this website (including [your IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views, and website navigation)
(b) information that you provide to us for the purpose of registering with us
(c) information that you provide to us for the purpose of subscribing to our website services, email notifications and / or newsletters
(d) any other information that you choose to send to us

(2) Cookies

A cookie consists of information sent by a web server to a web browser, and stored by the browser. The information is then sent back to the server each time the browser requests a page from the server. This enables the web server to identify and track the web browser.

We may use “session” cookies on the website. We will use the session cookies to: keep track of you whilst you navigate the website.

Session cookies will be deleted from your computer when you close your browser. We use Google Analytics to analyse the use of this website. Google Analytics generates statistical and other information about website use by means of cookies, which are stored on users' computers. The information generated relating to our website is used to create reports about the use of the website. Google will store this information. Google's privacy policy is available at:
http://www.google.com/privacypolicy.html. Most browsers allow you to reject all cookies, whilst some browsers allow you to reject just third party cookies. For example, in Internet Explorer you can refuse all cookies by clicking “Tools”, “Internet Options”, “Privacy”, and selecting “Block all cookies” using the sliding selector. Blocking all cookies will, however, have a negative impact upon the usability of many websites.

(3) Using your personal information

Personal information submitted to us via this website, e-mail, and conversations in person or telephone will be used for the purposes specified in this privacy policy or in relevant parts of the website.

We may use your personal information to:

(a) administer the website
(b) improve your browsing experience by personalising the website
(c) send you general (non-marketing) commercial communications
(d) send you email notifications which you have specifically requested
(e) deal with enquiries and complaints made by or about you relating to the website

We will not without your express consent provide your personal information to any third parties for the purpose of direct marketing.

Data stored for the purposed of the CarConnect project will be securely deleted upon project closure.

(4) Disclosures

We may disclose information about you to any of our employees or project partners insofar as reasonably necessary for the purposes as set out in this privacy policy.

In addition, we may disclose your personal information:
(a) to the extent that we are required to do so by law
(b) in connection with any legal proceedings or prospective legal proceedings
(c) in order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk)
(d) to the purchaser (or prospective purchaser) of any business or asset which we are (or are contemplating) selling; and
(e) to any person who we reasonably believe may apply to a court or other competent authority for disclosure of that personal information where, in our reasonable opinion, such court or authority would be reasonably likely to order disclosure of that personal information.

Except as provided in this privacy policy, we will not provide your information to third parties.

(5) Security of your personal information

We will take reasonable technical and organisational precautions to prevent the loss, misuse or alteration of your personal information.

We will store all the personal information you provide on our secure (password- and firewall- protected) servers. All information will be stored in an Advanced Encryption Standard (AES) encrypted database accessible by a limited number of nominated employees.

Of course, data transmission over the internet is inherently insecure, and we cannot guarantee the security of data sent over the internet.

(6) Policy amendments

We may update this privacy policy from time-to-time by posting a new version on our website. You should check this page occasionally to ensure you are happy with any changes.

We may also notify you of changes to our privacy policy by email.

(7) Your rights

You may instruct us to provide you with any personal information we hold about you. Provision of such information will be subject to:
(a) the supply of appropriate evidence of your identity (for this purpose, we will usually accept a photocopy of your passport certified by a solicitor or bank plus an original copy of a utility bill showing your current address).

We may withhold such personal information to the extent permitted by law.

You may instruct us not to process your personal information for marketing purposes by email at any time. In practice, you will usually either expressly agree in advance to our use of your personal information for marketing purposes, or we will provide you with an opportunity to opt-out of the use of your personal information for marketing purposes.

(8) Updating information

Please let us know if the personal information which we hold about you needs to be corrected or updated.

(9) Contact

If you have any questions about this privacy policy or our treatment of your personal information, please write to us by email to info@drive-electric.co.uk.