My Electric Avenue

Data Protection Strategy

Author: EA Technology

Date: 01 March 2013

Version: 4.2

The 'My Electric Avenue' project is the public identity for the Low Carbon Networks Fund Tier 2 project "I^{2}EV." The formal title "I^{2}EV" is used for contractual and Ofgem reporting purposes.

Date	Version	Author	Notes	Reference documents
28/01/2013	*2.2*	*Mary Gillie*	*Incorporating SSEPD's comments*	*Customer Engagement Plan*
28/01/2013	*2.3*	*Gill Nowell*	*Incorporating JON's comments; proofread and formatted*	*Customer Engagement Plan*
29/01/2013	*2.4*	*Nigel Bessant*	*Final review and approval*	*Customer Engagement Plan*
05/02/2013	*3.1*	*Mary Gillie*	*Updated after Ofgem's comments*	*Customer Engagement Plan*
06/02/2013	*3.2*	*Gill Nowell*	*Proofread after update*	*Customer Engagement Plan*
13/02/2013	*3.3*	*Richard Hartshorn*	*Review and formatted*	*Customer Engagement Plan*
28/02/2013	*4.1*	*Gill Nowell*	*Updated after Ofgem's comments*	*Customer Engagement Plan*
01/03/2013	*4.2*	*Richard Hartshorn*	*Updated after Ofgem's comments*	*Customer Engagement Plan*

Final Approval

Date	Version	EA Technology authorisation by	SSEPD authorisation by
28/01/2013	*2.4*	*James O'Neill*	
29/01/2013	*2.4*		*Nigel Bessant*
06/02/2013	*3.2*	*Dave A. Roberts*	
13/02/2013	*3.4*		*Nigel Bessant*
28/02/2013	*4.1*	*Dr Dave Roberts*	*Nigel Bessant*
01/03/2013	*4.2*		*Nigel Bessant*

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.*

1 Introduction

The My Electric Avenue project is a Low Carbon Networks Fund (LCNF) research and development project. The uptake of Electric Vehicles (EVs) is predicted to increase rapidly in the next 10 years, and therefore demand on LV networks is also predicted to rise. The aim of the project is to inform the development of equipment to manage demand from EV chargers to avoid this predicted strain on the distribution network. The trials will be held primarily in SSEPD's and Northern Powergrid's licence areas.

From a data protection perspective, a key aspect of the project is the collection of customer EV charging habits, feedback and driving habits from a sample of up to 100 participants in clusters. A second initiative is a wider data collection exercise of customer driving and charging habits and demographics (outside of local clusters). Access to the data will be given to University of Manchester to categorise customers, model their usage of their EV charger, enable network modelling and to analyse the impact of the control equipment on the demand on the LV Network. De Montfort University will collect behavioural data and personal feedback to allow an analysis of human response and provide a statistical comparison of the behaviour in the trials to be compared with a larger population.

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

If any aspects of the data protection strategy change during the project 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 and project feedback as well as electrical usage for EV charging and network information acquired through substation monitors and intelligent control boxes connected in series with charging points (installed into participating customers' homes/businesses). This document describes the data protection measures for customer data to be undertaken by EA Technology and project partners or subcontractors contracted to collect, or to perform analytics and modelling using the data. Diagram a) in section 4 illustrates the data flow overall for the project.

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

For the rental agreements of EVs, customers will be asked for their bank details and credit history. Customers' bank details and credit rating are only required by Fleetdrive Electric (the project partner managing the EV rental programme) to process the rental agreement. Therefore they will be responsible for the collection and storage of this data. At no point will this financial data be available to other project partners (see Table 1 in section 3).

The project will collect name, address, telephone number, and email address during recruitment as well as behavioural information (this will include driving and charging habits, opinion on the control technology, and satisfaction levels with the technology). Those participating in the technical trials will also be required to provide information about their home or business to determine whether their home is suitable for the charging point. Note that at no point will sensitive personal data[1] (as defined by the Information Commissioners Office) be collected or recorded as part of this project.

The project will also collect a number of electrical parameters such as voltage (at the substation and at customer charging points), current drawn by individual chargers and LV feeders, and charging point switching information.

For marketing purposes, customers may be asked to be photographed with their EVs in their local area or street, by project partners (i.e. Automotive Comms). 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 My Electric Avenue 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 online or written weekly surveys, face-to-face, telephone or email interviews, and focus groups. Residential information will be collected using simple questionnaires. Financial information collected by Fleetdrive Electric will be collected by a questionnaire.

Electrical data and charging points switches will be collected in 10 minute or 30 minute intervals from the intelligent control boxes and collated at the local LV substations or

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

recorded at the LV substation by the monitor/controller. Individuals will not be identifiable from this data. Each charging point will be assigned a code.

The personal non-financial data required in the My Electric Avenue project will be collected by Nissan, Zero Carbon Futures, Fleetdrive Electric, De Montfort University, and EA Technology.

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.

The address and details of where each intelligent control box and charging point is installed will be kept for use within an asset management plan. This asset management plan will be provided to the relevant DNOs and used by them to enable a quick response to any faults. Information from the asset management plan, such as the location of the monitor control units in substations and the LV feeders controlled by these devices may be held in the DNOs supply interruption management system. Participating customers' details may be recorded in this supply interruption management system, to assist the DNO in quickly responding to reports of a problem with the equipment installed.

During the recruitment process for clusters, the location of potential participants will be used to assess the network and determine where other participants need to be located to form a cluster.

In the instance that customers approach EA Technology with a request to take part in the technical/cluster trials, EA Technology will firstly ensure that they are eligible, and then encourage them to recruit another nine neighbours or people from their local area to take part. However, in the instance that customers request to know how many other customers (if any) have volunteered in their area, EA Technology will respond in one of two ways:

- Reply by stating the number of people in their area who have registered interest (without divulging any identifiable information), and therefore highlight how many the customer still needs to recruit to take part.
- Ask those customers already registered if they are happy for EA Technology to pass their name and email address or telephone number to the customer making an enquiry, for them to liaise with each other regarding recruitment. The request will only be made if another interested customer ask for contact details and details will be passed on only if permission is given to the customer who requests it. They will be asked not to pass the contact on to anyone else.

Providing contact details should help interested customers work together to recruit others.

The data collected by the substation monitors will not be personal data; however, EA Technology will still take the responsibility to process this data securely in accordance with the Data Protection Act 1998. Data will be collected from the substation monitors and transferred in a safe and secure manner. Data will be stored in a secure electronic database. Data will also be collected from data loggers in the EVs, installed by Nissan. This data is

collected from all customers using Nissan Leafs, (with their permission) regardless of their participation in the trials and is collected via a GPRS connection direct to a Nissan server. Individuals could not identified from the data so it is non-personal EA Technology will access this data via Nissan's servers. The data will be stored in accordance with Nissan data protection procedures to which the customers have 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 Nissan. Data will be transferred in accordance with the protection measures outlined in this document. Data from the monitor controllers will either be downloaded via the DNOs SCADA system and/or GPRS in accordance with the data protection measures outlined in this document.

The non-personal data required in the My Electric Avenue project will be collected by Nissan, Zero Carbon Futures, De Montfort University, EA Technology and ANDTR.

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 be included with the rental agreement for the electric vehicle and the conditions on which participants will receive the discounted lease. The project's Customer Engagement Plan details the full engagement strategy.

EA Technology will write into contracts with partners and contractors that data shared with project partners as part of the My Electric Avenue project 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. EA Technology will control access to non-financial data and only allow 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 (e.g. Automotive Comms) 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 EA Technology in writing before marketing material is signed off.

Customers will also be asked for permission to share their first name and email address with other interested customers in their area. This permission will only be sought in the instance of the situation described in Section 2d. Customers will be asked to provide an email or letter to EA Technology confirming their consent for their contact details to be shared.

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

All customers seeking participation will be provided with details of the project including:

- Future predictions for EVs and their impact on networks and the need for the project
- Objectives of My Electric Avenue

- Project partners
- Funding for My Electric Avenue
- A brief summary of how they can be involved in the project, including information on the monitors, 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 customers volunteer for the project and are eligible (as with any volunteer), their personal data will be either collected automatically or in a manner appropriate to their needs. For example, if De Montfort University 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?

As third party delivery body and project lead, EA Technology takes responsibility for the initiation, development and maintenance of relationships with all customers. Given their role and tasks within the project EA Technology will need to carry out a significant amount of work using the data, notably analysing it and coordinating activities. Their sub-contractors will also be required to carry out analysis, with EA Technology releasing data as required to facilitate this. It is therefore appropriate that EA Technology will be the data controller for storing all data with the exception of customer financial data. This also removes any need for personal data to be moved between parties unnecessarily, which could inherently weaken the protection of customer data. EA Technology will also act as holder for all non-personal information including electrical parameters which are not attributable to individual households. However, the customer will own the personal data that relates to them and will be able to request access to their personal data and request amendments (in writing) to inaccuracies at any time.

As part of the project close down procedure, all personal data will be anonymised and the original personal data will be permanently deleted. Personal financial data (held by Fleetdrive Electric) will be retained on a secure server for the duration of the lease contract and permanently destroyed afterwards.

Partners may only retain anonymised results of their analysis. They must return all non-personal and personal data to EA Technology and delete all records from their local servers. If the data is required again at a later date a new data request must be submitted to EA Technology.

Fleetdrive Electric is the sole project partner who has an absolute need to access customers' financial data in order to undertake credit checks; for this reason it is appropriate that Fleetdrive Electric will 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 lease contract and permanently destroyed afterwards.

g) How will data be securely transmitted?

Data transfer to and from the secure database must use the following security:

- All spreadsheets will be password protected with the password transferred separately to the spreadsheet
- Data will be transferred using a secure website (i.e. https) or secure FTTP
- Personal data will be sent separately to other data (e.g. demand and voltage data should be sent separately to names).

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.

4. The monitor/controller unit is accessible externally by an RS232 communications system. This will ensure that access to this unit is restricted as it is located within a substation or cabinet. Further passwords or encryption will be added.

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

There is a small possibility that the control of the network or data could be adversely affected by hacking into the monitor/controller. The operation of the monitor/controller unit is hard coded within the microprocessor. Commands to control the unit are sent using a RS232 link from a PC. This link is vulnerable, however to pose a threat, physical access to the monitor/controller units would be required and in addition knowledge of the internal workings of the unit would be needed.

Control of the network could be compromised by hacking into an intelligent control unit but it is considered difficult to achieve. This is because there are no external port connections to the intelligent control boxes as the commands and data transmissions operate solely over the Power Line Carrier (PLC) link. The intelligent socket is only configured to receive commands and will not initiate commands to other units. Commands can only be accepted from the monitor/controller unit set as the co-ordinator for the system (i.e. it is a Closed Architecture). The Message Handling software checks the validity of messages and the

messages are encrypted. Furthermore individuals could only be identified if the meaning of the numerical data was known and together with the address from which the data was sent. Further security can be added by introducing the concept of Trust Centres through which authentication of the messages senders can be implemented. Certificates passed between the trust centre and other nodes on the network can be used to authenticate the source of a message. This will be investigated during the project as it is not an issue for protecting personal data.

Because malicious data and control commands onto the wires would need firstly to be encrypted in the correct manner, it is considered very difficult to inject. A further precaution is that, the protocol relies on a sequence of messages, rather than one packet, to cause a particular action to occur. Message data and unit states are checked before the unit will act on a command. Sequencing and network identities are used to check whether or not a message is valid or from a valid source. Signals that appear to look like messages would be rejected as noise. The software operates 'Open Trust' sequences, so messages are freely transmitted within the device which means that any data that was received but found to be invalid later could be filtered and possibly tampering could be detected. This will be investigated during the trial.

As the Network is a closed architecture, the system can be configured to allow only pre-set or pre-known nodes to join. If as part of the project it is found that a more open architecture is needed, i.e. one where devices from different sources can be added to the network, additional Device Authorisation can be added to the network. Attempts for units other than those expected to join the network could be recognised as attempts at tampering.

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. A log of data requests will be kept and maintained by EA Technology. Project partners will be responsible for uploading data to the central database which will be hosted by EA Technology with the following security measures:

- EA Technology will manage the database and control access and visibility of data sets to each of the project partners
- EA Technology will also manage permissions on the database, allowing partner users to have access 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 server will reject communications from unauthorised devices
- The database is capable of disabling the SQL browser service
- The database will use non-standard names (security through obscurity)
- Information will be held on the database anonymously with a code to link it to personal data.

As owners and handlers of customers' financial data, Fleetdrive Electric will use the following security measures. Fleetdrive Electric is registered with the Information Commissioners Office for Data handling (Registration no. Z8537104). Fleetdrive Electric 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 Fleetdrive Electric's onsite 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 FSA 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 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.

Data downloaded from the cars will be collated on Nissan's Global Data Centre (GDC) which has the following security measures:

Application Security:

1. Authentication: GDC authenticates Data Services requests using dedicated user ID (tecid) and password (tecpw). Only the authenticated requests will be able to utilize Data Services.

2. Authorization: GDC authorizes Data Services requests of Ofgem based on the contract ID which is assigned to the user and VIN which is registered in GDC prior to the requests.

3. Session Management: Token which allows the user to utilize Data Services for a particular VIN will be generated by GDC after authentication and authorization succeed. The token expires in 90 days or when a new token is generated by another request for a particular VIN.

4. Encryption of Communications: Hypertext Transfer Protocol Secure (HTTPS) is used with deployment on the Internet for Data Services.

Network Security:

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

During analysis partners may store information locally. 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 software programmes and computers must 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 EA Technology and SSEPD. All results, data and analysis published by the project will be aggregated to feeder level. 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 My Electric Avenue project will be collected by:

- Zero Carbon Futures
- Fleetdrive Electric
- De Montfort University
- EA Technology
- ANDTR
- Automotive Comms
- Nissan

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

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	EA Technology Zero Carbon Futures Fleetdrive Electric	From feedback forms when establishing cluster	Fleetdrive Electric	On Fleetdrive Electric 's secure system and EA Technology's secure server (names and addresses of participants may be stored on the relevant DNOs trouble call systems)	Fleetdrive Electric De Montfort University EA Technology Zero Carbon Futures The relevant DNO
Credit rating and financial details	Fleetdrive Electric	Requested by Fleetdrive Electric when customers have given permission	Fleetdrive Electric	On Fleetdrive Electric 's secure system	Fleetdrive Electric
Driving habits	Nissan EA Technology	Recorded in the EV	Nissan, EA Technology	EA Technology's secure server	De Montfort University EA Technology
Socio-economic data	De Montfort University	Face to face, internet, phone, workshops, paper based surveys	De Montfort University/ Zero Carbon Futures	EA Technology's secure server	De Montfort University EA Technology University of Manchester
Project Feedback	De Montfort University	Face to face, internet, phone, workshops, paper based surveys	De Montfort University	EA Technology's secure server	De Montfort University EA Technology University of Manchester

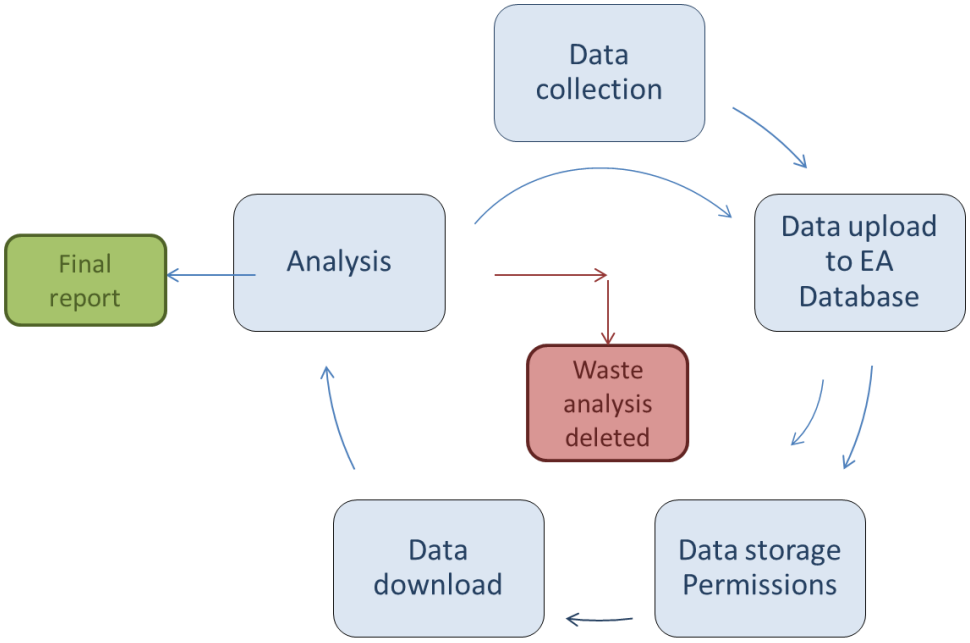
Data	Who collects the data	Where/how is data recorded	Who transmits the data	Where is the data stored	Who will use the data?
Charging current, voltage at charging point	EA Technology DNO	Intelligent socket, sent to the substation	ANDTR or EA Technology	EA Technology's secure server and temporarily at the substation	EA Technology University of Manchester
Network data from the substation	EA Technology DNO	Monitor controller will record data, SCADA or GPS or PLC	ANDTR or EA Technology	EA Technology's secure server	EA Technology University of Manchester
Photos	Automotive Comms or subcontractor	On site with customers	Automotive Comms or subcontractors	EA Technology's secure server	Automotive Comms or subcontractors

Table 1: Indicative structure of data collection and use for My Electric Avenue

4 Diagrams: My Electric Avenue Data Flow and Management

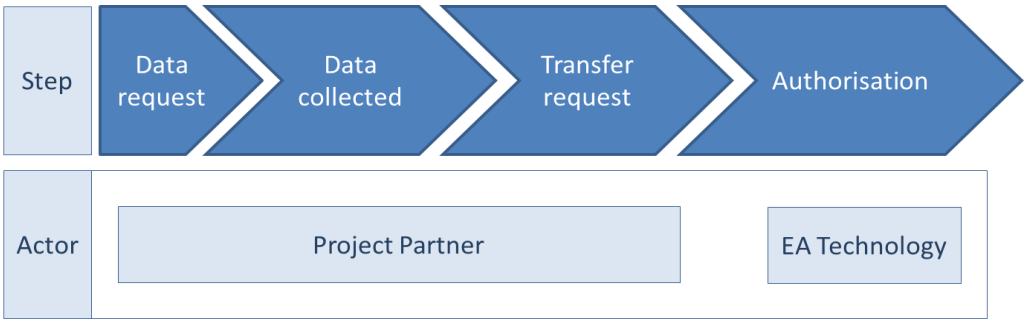
a) Data flow

The following diagrams illustrate the data flow for this project.

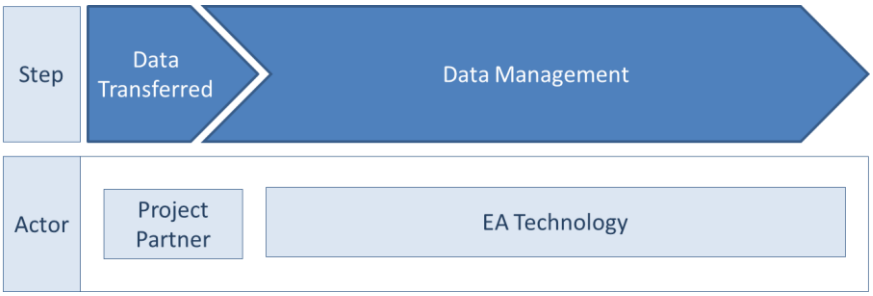


EA Technology will hold the right to perform an audit on the data protection measures partners or contractors use when collecting or handling data (essentially at any time throughout the project).

b) Data collection and upload

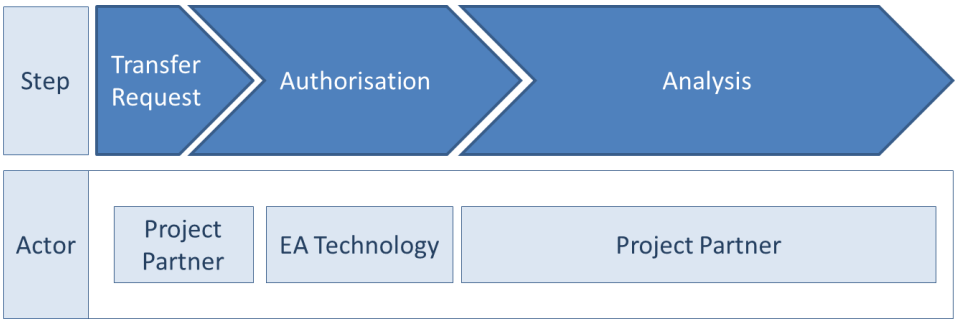


c) Data management



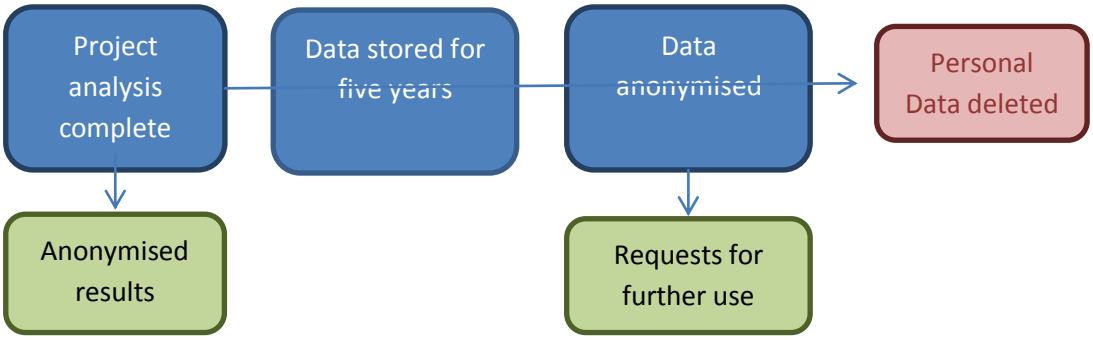
Once data is transferred to EA Technology's secure database, EA Technology is responsible for the security of the data shared and who has access to it.

d) Data download / analysis



Precise requests are essential to facilitate the access to data. All requests for data will be made through the assigned EA Technology team member.

e) Data anonymisation and / or destruction phase



Should any of the project partners (notably De Montfort University and University of Manchester) 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 EA Technology in advance of publication, to obtain authorisation.

Appendix A – Draft Customer Consent Form Wording

Consent form: to have an Electric Vehicle charging point and control technology installed, to allow your data to be gathered, and to participate in the My Electric Avenue trial.

(Customer Copy)

As part of participating in the My Electric Avenue project (the project) I give permission for EA Technology Ltd, and participating companies in the project (known as the 'project team') (including Scottish and Southern Energy Power Distribution and their authorised partners and agents) to install an electric vehicle (EV) charging point at my address to gather information about the electrical energy required to charge an EV and what impact that has on the local electricity network in order to predict what future use of EVs 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 SSEPD to continue to deliver an electricity network for customers' needs.

The information will be collected by a control box installed in my home and sent by Power Line Carrier (PLC) to my local substation. Substation monitors installed in the electricity substation that supplies my premises will automatically collect this information and communicate it remotely to a central server.

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 Zero Carbon Futures and located in an agreed place in my premises for charging my EV. There will be a record of each monitor's serial/batch number and location.

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 phone 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, phone, 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 EA Technology, 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 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 EA

Technology or SSEPD within 14 days of any sale, letting or underletting or any parting with possession of my property.

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 My Electric Avenue related information from the project team.

Name: ……..

Signed: …… **Date:** ……

Consent form: to have an electric vehicle charging point and control technology installed, to allow your data to be gathered, and to participate in the My Electric Avenue trial.

(EA Technology Copy)

As part of participating in the My Electric Avenue project (the project) I give permission for EA Technology Ltd, and participating companies in the project (known as the 'project team') (including Scottish and Southern Energy Power Distribution and their authorised partners and agents) to install an electric vehicle (EV) charging point at my address to gather information about the electrical energy required to charge an EV and what impact that has on the local electricity network in order to predict what future use of EVs 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 SSEPD to continue to deliver an electricity network for customers' needs.

The information will be collected by a control box installed in my home and sent by Power Line Carrier (PLC) to my local substation. Substation monitors installed in the electricity substation that supplies my premises will automatically collect this information and communicate it remotely to a central server.

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 Zero Carbon Futures and located in an agreed place in my premises for charging my EV. There will be a record of each monitor's serial/batch number and location.

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 phone 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, phone, 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 that the project team holds 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 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 EA Technology or SSEPD within 14 days of any sale, letting or underletting or any parting with possession of my property.

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 My Electric Avenue related information from the project team.

Name: ……..

Signed: …….. **Date:** ……..