Guidance for EVCC Members on the General Data Protection Regulations (GDPR)

The General Data Protection Regulations (GDPR) came into force on 25 May 2018. It is important that you familiarise yourself and those in your organisation with its provisions and requirements. The best place to start is on the Information Commissioner's Office (ICO) website on which this guidance is closely based:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Many of the GDPR's main concepts and principles are much the same as those in the previous Data Protection Act (DPA). However, there are new elements and significant enhancements. For example, the GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. This means that you need to ensure that your approach to governance and the way you manage data protection as a corporate issue meets the requirements.

As a starting point you need to map out which parts of the GDPR are likely to have the greatest impact on your business model. That way you can give those areas the necessary prominence in your planning process. Any information you are holding on your customers is likely to be a key part of this process. The ICO has published two very helpful documents which you should read carefully:

- Twelve steps to take now:
  https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
- Data protection self-assessment toolkit:
  https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/ .

The ICO advises businesses to take 12 steps to ensure that they are complying with GDPR. The ICO has summarised these steps as follows:

1. Awareness
2. Information you hold
3. Communicating privacy information
4. Individuals' rights
5. Subject access requests
6. Lawful basis for processing personal data
7. Consent
8. Children
9. Data breaches
10. Data Protection by Design and Data Protection Impact Assessments
11. Data Protection Officers
12. International.

Make all your Directors, senior managers and staff aware of GDPR

It is important that you make all the Directors and senior managers in your company are aware of their obligations under GDPR. It is a good idea to draft an internal communication for your staff setting out the key points. In particular, it is important that all the Directors and senior managers are aware that there are restrictions on sharing and communicating information about individuals including your customers.

Document the information (data) about individuals you hold

Once you have made everyone in your company aware of GDPR, the next step you need to take is to examine and document:

- all the types of personal data you hold,
- how you obtain the data
- what you do with the data.

Personal data about your past, present and future customers will be a very important element of this process. You may obtain data by telephone, email, post or in person, for example. Remember to include personal data you receive as a result of any leads you may have generated or purchased. Data about your employees and any self-employed individuals you subcontract work to are also covered and so be sure to include this in the document you produce. It is also a good idea to list where you hold the data, for example in your CRM database, and the steps you have taken to ensure that this is secure.

Update your Privacy Policy Statement or Notice

If you do not already have a Privacy Policy Statement or Notice on your website and in hard copy you should draft one as soon as possible. If you already have one, you should take steps to amend it to bring it into line with GDPR. (You can find EVCC's Privacy Policy Statement at www.electric-vehicle.org.uk) Your Statement or Notice should explain clearly:

- who you are
- what you do
- the kinds of personal information (data) you hold
- the purposes for which you hold it, the use you make of it
- the rights of any data subjects
- the circumstances in which you transfer or share the information, and
- how you will communicate any changes to your privacy policy.

Make sure you inform individuals (data subjects) of their rights

The ICO lists individuals' rights as follows:

- the right to be informed
- the right of access
- the right to rectification
- the right of erasure

- the right to restrict processing
- the right to data portability
- the right to object
- the right not to be subject to automated decision-making including profiling.

You should spell out all these rights in your Statement or Notice. You must also have procedures in place to deliver these to the individuals concerned. You should be able to demonstrate that you are in a position to do this.

Explain the procedure you follow when you receive a subject access request

All individuals have the right to request to see the data you hold on them. In line with the previous section you must publish the procedure you will follow should you receive a subject access request. This should include the timescales within which you will respond, the format in which you will provide the data, the ways in which individuals can contact you to make a subject access request and the name of the person in your organisation responsible for dealing with this.

Make sure any data processing you do is lawful

You must be very careful with any personal data you hold. If you hold customers' details, for example, you must be very careful about how you store these details and how you use them. In particular you must be very careful if you use individuals' data for any purpose other than that for which you obtained them.

So, for example, you must not pass your customers' details to a third party agency to carry out marketing or to sell them ancillary services without their explicit consent. If you do have any data sharing agreements you need to examine them to ensure that they are compliant, and that any data is well protected.

Make sure you seek consent to hold and share the data

Any individuals about whom you hold data must have consented for you to hold it. This might have been by contacting you in the first place and asking you to provide them with information or a quotation, for example. In your standard documentation, such as your terms and conditions and your quotations, you should include a section informing customers about how you will store the data they have provided you. You must seek their consent should you want to use this data for any purpose other than that for which they have provided it to you.

Make sure you are aware of any data you are holding that relate to children

If, for any reason, you hold data about children, there are specific requirements that relate to them. In particular, you will require parental consent to process such data in any way. It is your responsibility to be aware of the age of children whose data you are holding.

Make sure you have procedures in place to deal with any data breaches

You need to have procedures in place to detect any data breaches. If you suspect that there have been any data breaches, for example as a result of your CRM system being compromised, you must investigate them fully and also report them in line with the regulations.

Decide whether you need to carry out a Data Protection Impact Assessment

The ICO has published a guide to help you to decide whether your company would benefit from a formal Data Protection Impact Assessment. You should follow the ICO's self-assessment to see whether your company would benefit from an assessment:
https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/

Appoint some-one in your organisation to be your Data Protection Officer

You need a single, designated individual in your company to be responsible for data protection compliance. You should explain who this person is in your Privacy Policy Statement or Notice, and provide their contact details. In some cases a Data Protection Officer is required, but this is in cases where large amounts of data are being processed, or in the case of very sensitive categories of data, such as health records for example.

Be aware that there are specific requirements if your company operates in more than one country

If your company operates in more than one EU Member State, and if you process data between Member States, you will need to decide which is to be your lead data protection supervisory authority, and include this in all your documentation. This should be the Member State in which your company makes its most significant decisions about any data processing activities. A European Commission Working Group (Number 29) has prepared further guidance on this. You should read it carefully if this could apply to your company:
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080 .

24 January 2020

Document Version Control

Date of issue	24.01.2020

Author	V Graham
Document number	EVCC 009
Version number	1.0
Version date	24.01.2020
Rationale for amendments	N/A