General Data Protection Regulations (GDPR)

Originally published 25 May 2018, updated 3 May 2022

Introduction:

From 25 May 2018, the General Data Protection Regulations (GDPR) will require all organisations that process data to comply with new legislation regarding use of personal data. This is the first change to data regulation since the implementation of the Data Protection Act 1998.

GDPR seeks to address concerns over abuse of personal data by social media platforms and digital marketing and advertising companies. It will address how data is collected and stored and seek to protect the rights of consumers regarding how companies use their personal data. It will put the power in the hands of individuals by allowing them to specify what data is stored on them, what it is used for and when and how it is removed. Businesses that collect and store individual data must be prepared to state exactly what it is going to be used for and where they obtained it. Consumers will also be able to request that incorrect information be amended, deleted and removed from a company's database.

The primary purpose of GDPR is to ensure personal data is gathered legally, under strict conditions, for a legitimate purpose. Failure to comply can lead to huge financial penalties. The enforcing body for GDPR is the ICO – Information Commissioner's Office.
GDPR has established six lawful reasons for processing data. At least one of these justifications must apply for an organisation to legally process data. The six justifications are where the subject has explicitly consented (through an 'opt-in') to their data being processed; to comply with a contract; or legal obligation; or to protect an interest that is essential for the life of the subject; if processing the data is in the public interest; or if doing so is in the controller's legitimate interest.

General Data Protection Regulation also imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. As a non-profit corporate membership association holding primarily business-related personal data (i.e. work e mail addresses not personal e mail addresses etc), the risks of abuse of data that GDPR is seeking to prevent are less direct for EIC than for say a mobile phone company, nonetheless we must ensure that EIC is compliant with GDPR and that staff and members are confident that we handle data in the right way.

Also, while this note is about EIC specifically, the other companies in the wider group must also be compliant. Sister organisation the **Association for Consultancy and Engineering** (ACE) is taking much the same steps as EIC, while **Infrastructure Intelligence**, which operates in a more commercial manner, will put additional steps in place.

1. Getting ready – a few key actions:

- **Audit the information you hold:** Organisations must create a list of the personal data held and identify it by type, i.e. names, addresses, phone numbers etc.

  Action: EIC has carried out a data mapping exercise and established what information is held including member, group and stakeholder details.

- **Determine why you hold the information**: GDPR requires organisations to establish a legal basis for collecting data, to be outlined in the privacy policy.

  Action: EIC has carried out a data audit including establishing the legal basis for holding members and stakeholder's personal data under GDPR's 'legitimate interests' proviso.

  We will hold member and stakeholder data where it is necessary to perform a contract, or where it is necessary for our legitimate interests and it would be reasonable to expect EIC to process the personal data for the purposes of providing and enhancing EIC's products and services. We will include unsubscribe options on all our generic emails, and if a member company resigns we will delete the personal data we hold after three months unless we have an agreement with the individuals not to do so. Establish how you store data, and who it is shared with: This could be a list of internal databases, and third-party storage providers.

  Action: Included in the above is the sharing of personal data with EIC volunteers, acting on our behalf, who use it to support the activity of the groups or committees in which they operate.

- **Document how data is processed:** Organisations will need to outline all processing activities, including keeping the name and contact details of the data processors, as well as the categories of processing carried out - and the transfers of personal data to an 'adequate' third country (one that is outside the European Economic Area, but whose data protection measures are deemed adequate for data transfers) or international organisation.

  Action: EIC has done this as part of the Data Mapping Exercise.

- **Revamp your privacy policy:** Organisations must write a clear and understandable privacy policy that is publicly accessible on their websites. This must clearly stipulate the lawful basis for data collection and processing in concise, easy to understand and clear language. Customers and users need to be informed of the use of any third-party data processors or controllers, to which they should consent by accepting your privacy policy.

  Action: EIC has updated its website privacy policy. See: www.eic-uk.co.uk/privacy-policy/

- **Refresh existing consents if necessary:** Consent must be given freely, as well as being specific, informed and unambiguous; hinging on a positive opt-in. Organisations must explain clearly and specifically why you're collecting certain data and what that data will be used for, plus which third-party controllers will be able to use that consent. As well as make clear that users can withdraw their consent and make it easy for them to do so.

  Action: EIC has a 'legitimate interest' as defined by GDPR in processing our members and stakeholders' data, we have chosen not to explicitly seek new opt-in consent from the individuals we hold data on. Instead, we have updated the privacy policy and are communicating this, the ability to unsubscribe and our intention to process data under 'legitimate interest' in a series of e-mails to members and Infrastructure Intelligence subscribers.

- **Implement internal awareness:** Many data breaches involve a degree of human error. Training staff to be aware of how GDPR affects their daily work maximises chances of compliance and minimises risk of suffering data loss or theft.

Action: EIC rolled out training for staff in Feb 2018 which can be extended to volunteers.

- **Appoint a Data Protection Officer (DPO)**: Especially important if your organisation is a public authority, or if you carry out certain types of processing activities.

  Action: Although not legally obliged to do so, EIC has appointed a Data Privacy Manager – EIC CEO, **Stephen Marcos Jones**, with the responsibility for data protection compliance and monitoring.

2. Employees and GDPR

GDPR will affect employees in two ways. Firstly, in their employment capacity with their organisation where they process personal data as part of their everyday roles and responsibilities. Secondly, as data subjects where their organisation collects and processes personal data specific to the employee themselves.

Handling data in an employment capacity:
Employees/Volunteers who process personal data as part of their role, should be fully abreast of their organisation's GDPR policies and how these will affect how they collect, process and store data. Employees/Volunteers should ensure the following:

- Their roles and responsibilities are clearly defined;
- They are aware of who the responsible data protection person is; They only process personal data in line with their defined responsibilities;
- They have a clear overview and understanding of the organisation's data protection policies;
- They are provided with training specific to the processing of personal data.

3. A few practical tips

- Employees must ensure that personal data is maintained in a secure environment and transmitted through secure methods;
- They must protect keys, passwords and codes that that would facilitate unauthorised access;
- They must protect mobile devices and storage media from loss and theft; They must get into the habit of sending blanket emails using 'Bcc' rather than 'To';
- It is good practice to include a line at the end of blanket emails informing recipients that they have a right to inform you that they no longer wish to receive emails from you;
- They must engage in regular data cleaning i.e. reducing email lists when some recipients haven't engaged for a defined period - no matter how unpalatable it may seem;
- New personal data: Employees and Volunteers may acquire new business cards; however, this should be securely stored for example on the CRM/IMS system.

4. Reporting data breaches

Under GDPR, any breaches involving personal data must be reported to the Information Commissioner's Office within 72 hours - including what data has been lost, any consequences, and what countermeasures have been taken.

Any loss in non-encrypted personal data must also be communicated to the data subjects involved.

In the event of a breach, EIC employees must contact **Stephen Marcos Jones** without delay on: smjones@acenet.co.uk or 020 7202 4148.

Any queries regarding any of the above should be addressed to EIC:

Claire Clifford,
Director of People, Culture and Skills,
3 Hanbury Drive,
Leytonstone House,
London, E11 1GA.

E: cclifford@acenet.co.uk T: 020 7202 4148.

For further information, please see: https://ico.org.uk