GDPR BRIEFING

The General Data Protection Regulation comes into effect on 25 May 2018. It applies to any organisation that handles the personal information of any resident in the European Union. GDPR requires organisations to maintain the privacy and security of any European Union resident's personal information. To ensure compliance with GDPR, some key principles need to be understood and implemented.

People have a right to privacy. Organisations need to respect their privacy by restricting what personal data they collect and process and by safeguarding that data. Privacy obligations apply to any information, either by itself or when used with other pieces of information, which could identify an individual person living in the European Union. This information could be personal data such as names, addresses, passport numbers, driver's license numbers, ID numbers, financial details, location data, or sensitive personal data such as biometrics, union memberships, medical history or a person's sexual, religious, or political orientation. The regulation applies to a 'natural person,' meaning a living individual. Here are some of the key tenants of GDPR that should be followed:

Personal data for individuals shall be processed lawfully, fairly, and in a transparent manner. People need to be told what is being collected and for what purpose.

Personal data shall be collected for specified, explicit, and legitimate purposes. It shall not be used for any other reasons that conflict with these purposes.

Personal data shall only be kept and processed for as long as it is required for that purpose and for no longer than that. Personal data must be kept up-to-date and accurate.

People have the right to receive a copy of their data or can request that their personal data no longer be used. In some cases, they can have it deleted entirely.

Organisations must implement appropriate security measures to protect personal data against accidental or unlawful destruction, loss, alteration, or disclosure.

In addition, organisations need to ensure all staff members who handle personal data are properly trained in how to secure and protect that data.

Protection measures that are in place to secure personal data must ensure an appropriate level of protection to the sensitive nature of the data. As the risk associated with data becomes greater, so should the effort and measures to protect the data. Measures taken should be regularly reviewed and updated. Records about privacy, security decisions and measures which help to show compliance with the requirements must be documented. Also organisations are legally bound to employ measures, such as contracts and due diligence reviews, to protect personal data when transferring it to external third parties or parties outside the EU.

Finally, in the case of a personal data breach, organisations shall report the breach within 72 hours after becoming aware of it. Failure for organisations to comply with GDPR can result in fines up to €20m or 4% of their global revenue whichever is greater.

Key Data Protection terms:

- **The Information Commissioner:** this is the UK regulatory body which is responsible for promoting the good data protection practice undertaken by data controllers. The ICO publishes data protection guidance and also has the power to fine companies who breach the rules.

- **The Data Controller:** will usually be organisations, i.e. The IED. They are responsible for deciding what information will be collected, how it will be used and why it is needed

- **The Data Processor:** often third-party companies or Individuals who are used to process data on behalf of the Data Controller; e.g. an outside company used to administer payroll or pensions.

- **The Data Subject:** the person whose data is being processed.

- **Legal Basis for Processing Data:** The IED will use the 'Legitimate Interest' as the basis for processing members, and prospective member's personal data, as without this data we will be unable to assess competence against defined standards or award membership or registration. Likewise, volunteers must have limited access to the personal data of applicants/members in order to fulfil our commitments under our Royal Charter or as a licensed body on behalf of the Engineering Council (ECUK) or Society for the Environment (SocEnv).

Managing your Data:

Members can manage their data at anytime via the Members area of the IED website or by calling the IED headquarters during office hours 01373 822801.

As a volunteer what should I do?

Here are some steps that you should take today:

1. Treat all personal data with respect and security (treat the data as if it was personal and private information about you).

2. You must only process, collect or share personal data on behalf of the Institution and only for the purposes of your current volunteer role; i.e. processing membership application details, Professional Review Reports (PRR) and Professional Review Assessment Reports as a Membership Assessor and/or as a member of the Membership Committee. Likewise, for other committees or roles such the Education and Training Committee or as a Member of Council.

3. Be aware of your working environment when accessing documents which contain personal data. Be careful of processing data in public areas such as trains or cafés in case you may be overlooked.

4. Lock your screen when away from a computer or device that is being used to process personal data and keep hard copy documents in a secured place, especially when travelling or out and about.

5. Delete information you don't need anymore. Securely destroy or return information shared with you in your role as a volunteer for the Institution once it has been processed and is no longer required.
6. Be extra careful when sending personal data - check you are sending it to the right people. Be careful of the use of To, Cc and Bcc fields – where possible send links to documents rather than sending documents as attachments. If you have personal data in your mailbox, have a cleanout - move what you need to a relevant, separate and protected filing area and delete the rest.

7. Give files and documents meaningful titles that make it clear if a file contains personal data.

8. Store personal data in an appropriate filing system with the right security and access controls applied. Consider who has access to the data and keep it out of shared storage.

9. Try to reduce the amount of personal data you hold. Ask yourself – do you really need it? Consider why you are keeping it and how long it is likely to remain current. Take steps to update or delete accordingly.

10. Safeguard documents shared with you, and if you suffer a data breach or lose documents controlled under the GDPR ensure you notify the IED HQ staff within one working day of becoming aware of the loss of control.

11. Please acknowledge your responsibilities under GDPR.

    a. Click below to send an email to the IED confirming you have read this briefing and will act to help the Institution to be GDPR compliant.

    b. Acknowledgement of Volunteer GDPR Briefing email

Resources

The GDPR Regulation:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R067

Information Commissioners Office:

https://ico.org.uk/

ICO GDPR Guide:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/:

EU GDPR Portal:

https://www.eugdpr.org/

Information management and associated risk:

http://www.nationalarchives.gov.uk/documents/information-management/rfi-sme-2017.ppt