General Data Protection Regulation - Information for Volunteers

Background

The General Data Protection Regulation (GDPR) came into being on 14th April 2016 and became law in the United Kingdom on 25th May 2018. The regulation gives individuals rights over any data about them held by organisations. It contains provisions and requirements for the acquiring, keeping and processing of personally identifiable information of individuals inside the European Union. It applies to any enterprise that holds or processes the personal data of people inside the EU, regardless of the organisation's location or the citizenship of the persons.

The GDPR is designed to update data protection legislation to reflect advances in technology and the way personal data is used, so that it is fit for purpose in the digital age. Whilst many of the GDPR's requirements are similar to the existing ones there are some key changes in the legislation that affect how we manage data in PMI UK as we carry out our activities.

Some unofficial definitions:

Personal Data is personally identifiable information (see below for examples)

Data Subject is the individual whose personally identifiable information is held

Data Controller is the organisation that decides what is done with the data

Data Processor is the organisation that uses or processes the data

Data Breach is an action contrary to PMI UK's Data Protection Policy such as use of data in a manner not approved or release of information to an unapproved third party.

Aims

The aims of this document are that PMI UK Chapter volunteers: recognise what 'personal data' is; recall the key points of the GDPR; make use of personal data only for acceptable processes; are able to decide if a Data Breach has taken place; and are able to apply the Data Breach Policy if they need to.

What is Personal Data?

	Personal Data	Sensitive Personal Data	Personal Data for Special Categories of Person
Definition	Any information relating to an individual person which enables that individual to be identified(whether directly or indirectly)	Personal Data revealing and/or concerning an individual's: • Racial or ethnic origin • Trade union membership • Sex life • Sexual orientation	Personal Data directly relating to a child or vulnerable individual. The definition of personal data is the same.
Relevant Examples	Personal data can include any of the following or combination thereof which enable an individual to be identified: • Name • Address (including an IP address) • Identification number • E-mail address • Bank account details • Factors that are specific to that individual (physical, mental, economic, cultural such as • Photographs or recordings	As with personal data to the extent that it concerns sensitive information such as: • Medical records • Spouse/child • Marital status • Marriage or death certificate	As with personal data to the extent that it concerns a child or vulnerable individual such as: • Medical records • Information about a child

Principles of Personal Data Processing

The GDPR requires that personal data shall be:

- Collected only if the Data Subject gives explicit permission for the purpose and the data to be collected
- Processed fairly and transparently
- Collected only for specified, explicit and lawful purpose/s
- Collected only as required for the purpose/s and no other data
- Accurate and up to date
- Managed securely
- Retained only for as long as is necessary and then erased

- Not shared with other organisations unless a contract is in place, including for the protection and use of the data

What's New?

Individuals now have additional rights under the GDPR. This includes:

Right of Access – Individuals have the right of access: to know what information is held and for what processes or uses. This is similar to the Data Protection Act.

Right of Rectification – Individuals have the right to have any information held rectified if inaccurate or incomplete. If passed to a 3rd Party that party must also be informed.

Right to Object – Individuals have the right to object to their data being processed for direct marketing, research and a task in the public interest.

Right to restrict Processing – This is similar to the DPA. When a restriction is received/applied the data can be stored but not used/processed.

Right to Data Portability – Individuals are allowed to obtain and reuse their data across different services. They are allowed to move, copy or transfer the data across different IT environments.

Right to Erasure – Also known as the "Right to be Forgotten." Individuals have the right to have their personal data removed or deleted unless there is a compelling reason not to do so.

Data Breach Notification – GDPR requires that any data breach must be reported to the relevant authority within 72 hours of learning of the breach and the individual concerned by the breach must be contacted without undue delay. The only exception is where the breach may not cause harm e.g. the data is securely encrypted. The penalties for data breaches have been reviewed and significantly increased from the £500k in the DPA. The maximum penalty is now €20m or 4% of the organisation's annual turnover.

Data Breach – The GDPR definition: 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

Data Breach Policy – Every organisation that is a data controller or data processor shall have a Data Breach Policy.

What does this mean for us?

As volunteers regardless of the level of involvement we must be aware of the above and ensure that we comply with the regulation. There are some basic do's and don'ts that we must all observe when we are working on behalf of PMI UK Chapter:

DO be sure that all personal data is necessary. Always ask – do I need this?

DO be sure to confirm you have the owner's explicit consent to the data being collected and the specific use of it. This is especially relevant at events.

DO be sure you can demonstrate this consent if asked.

DO be sure that the data collected is the minimum necessary required.

DO be sure that when data is being collected the mandatory information is provided to data subjects AND it is for an approved purpose. If in doubt contact the Director of Operations BEFORE collecting any data. Each branch of UK Chapter has completed a list of approved purposes which can be seen at Project Place.

DO be sure that the data collected is safely stored. Be sure to use only the relevant location in Project Place.

DO ensure only the volunteers who really need it have access to the data. And each volunteer has signed the UK Chapter Confidentiality Agreement. You may check this with Director of Operations.

DO be sure to delete any data once its purpose for collection has expired.

DO report any data breach (even suspected breach) to the Director of Operations immediately you become aware of it.

DO respond to a data enquiry made under GDPR by referring the enquiry to the Director of Operations within 24 hours and informing the enquirer that you have done so. Please **DON'T** respond yourself.

DO review every couple of months any personal data you control and delete it unless there is good purpose to keep it.

DO Review the UK Chapter Data Protection Policy and find out who is the contact for data protection issues at our web site

DON'T allow persons under 13 years of age to participate in UK Chapter activities until you have the approval of Director of Operations.

DON'T share personal data without the owner's consent.

DON'T hold personal data (including photographs) in personal folders or on personal devices.

DON'T share event attendance records with 3rd parties such as sponsors without PMI UK's formal approval from the Director of Operations. For example if holding an event at a company premises, don't share the attendee list with Security.

DON'T collect any sensitive personal data, as defined in the table above.