

1. This policy sets out the procedure to be followed by the Expert Witness Institute, its Governors and employees, to ensure it complies with its obligations under data protection law. It is designed to ensure that we take a clear and consistent approach to data subject rights requests. Such requests were previously referred to as 'subject access requests'.

Definitions

2. **Personal data** is defined by article 4(1) General Data Protection Regulation (GDPR). It means *'any information relating to an identified or identifiable natural person ('data subject'); an identifiable [living] natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'*.

3. **Special category personal data** is defined by article 9(1) GDPR. It means any personal data that reveals a living individual's

'racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.

Data Subject rights and obligations

4. The GDPR provides individuals whose personal data has been processed, i.e., data subjects with rights concerning their personal and specific category personal data. Those rights are:
 - the right to receive information concerning personal data collected by the data controller: EWI is the data controller for their information. This is the right to be informed of how we are going to process their data before we do so. This information is contained in our Privacy Notice;
 - the right to receive information by the data subject concerning personal data otherwise obtained by the data controller. This is the right to be informed of how we are processing their data when it was given to us by someone other than the data subject;
 - the right of access to data and related information by the data subject .This is generally known as the **subject access right**;
 - right to rectification of data held i.e., the right to require us to correct any mistakes made in respect of their data;

- the right to erasure of data held we hold;
 - the right to stop us processing their data;
 - the right to have their data transferred to someone or some organisation of their choice. This right only applies where we have processed a data subject's rights based on their consent and processed their data by automated means;
 - the right to object to processing; and
 - the right not to be subject to automated decision-making or profiling.
5. Where a data subject seeks to exercise any of these they will do so via a '**data subject request**' or DSR. This policy sets out the process we must follow when such a request is made.
6. There are a number of exemptions to the various data subject rights which may apply to personal data which it holds or which it holds on behalf of the judiciary. The exemptions are set out in the GDPR and the Data Protection Act 2018. Further details are set out below.

Dealing with a DSR

7. A DSR must be submitted in writing, either by letter, email to the Chief Executive at info@ewi.org.uk. They should include:
- Name of individual;
 - Correspondence address;
 - Contact number and email address;
 - Details of the information requested.
8. If a DSR is received it must be reviewed by our Data Privacy Officer immediately. The Data Privacy Officer must log the date and time it was received in our Data Subject Request Log. In order to ensure that we can respond within a calendar month of receipt of the DSR, the deadline for responding must be recorded at this time in the Log.
9. The Data Privacy Officer will then consider the response, undertake such investigation as necessary to determine what, if any, personal or special category personal data we hold on the individual making the DSR. In determining our response the Data Privacy Officer will consider the following questions:
- Should we provide a response to the DSR?
 - Do we hold any information relating to the subject of this request?
 - If so, does any of that information qualify as personal data or 'special category personal data' as set out in the GDPR?

- Do the GDPR and DPA 2018 contain any exemptions which may be used so as to prevent the disclosure of personal data or special category personal data to the requestor? In particular, does the request concern personal data to which the absolute exemption from the subject access rights apply or does it concern personal data to which the partial exemption applies.

10. Where personal data is held and ought to be supplied to the person making the request only the personal information concerning that individual will be provided. There is no right to receive specific documents. The right is to receive information only.

11. It is important to remember that although personal data often forms part of a document, the data subject rights concern the individual's personal data, and not necessarily to a document or any third party's personal data.

12. Information will not be provided if an exemption from the subject access right applies.

Should we respond?

13. We must confirm the identity of the person making the DSR. This is necessary to ensure that we do not inadvertently breach our duty to keep personal data secure by disclosing it to someone other than to the individual whose personal data it is.

14. To confirm identity:

- may ask the individual to provide two forms of identification;
- may contact the individual via the telephone to confirm the request was made.

15. If the person making the DSR is not the person whose personal data is sought but they seek it on behalf of that person we must ensure that we receive proof of their right to ask for the information on behalf of the individual whose data it is.

16. Where an individual has made a number of similar requests for information we may either refuse to provide the information or we may charge a reasonable fee for providing it. We may do this where an individual has made a number of requests and the immediate one is therefore 'manifestly unfounded or excessive'.

17. We also do not need to comply with the request if it is so unclear that we are unable to ascertain what information is being requested. Where this happens we must ask the requester to provide further information before then considering our response.

Do we have any personal information?

18. We must bear in mind that personal data may take a number of forms and be contained in a number of different documents. It may be contained in a number of different files, paper-

based, and electronic, including e-mail. It may be contained on computers, mobile phones, tablets.

19. Consideration must be given to all the different ways in which we hold personal data by the Data Privacy Officer. In doing so they must ensure that they consider what information we hold by reference to the definitions of personal and special category personal data set out in article 4(1) and article 9(1) GDPR.

Are there any applicable exemptions to complying with the DSR?

20. The GDPR and 2018 Act set out a number of exemptions to the various subject access rights. If an exemption applies EWI can properly refuse to provide personal or special category personal data that we hold.

21. The Data Privacy Officer will consider if any exemptions apply. In particular there is a right to withhold information where to comply with a request would infringe the rights of third parties or where information is subject to legal professional privilege. Reference should be made to the Schedules in the 2018 Act to determine if an exemption applies.

The response

22. Having determined whether we hold any information and whether that information can properly be provided to the person making a DSR, the Data Privacy Officer will ensure an appropriate response is provided within the calendar month deadline. That response must set out how further information concerning subject access requests can be obtained from the Information Commissioner's Office (the ICO), the right to complain to the ICO and the ICO's contact details.

23. Where the DSR concerns the **subject access right**, the following information must be provided to the data subject:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling (see article 22(1) and (4) GDPR) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and

- where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 GDPR relating to the transfer.
24. Copies of the data subject's information must be provided, unless an exemption applies.
 25. There is no right to receive a copy of documents in which information is processed. No fee may be charged for the information.
 26. If the data subject requests further copies of data having been provided with information, a reasonable fee may be charged for the provision of further copies. The reasonable fee should be no more than the administrative cost of providing the additional copies.
 27. The response must provide information on how the person making the request can ask to have it subject to an internal review if they are not satisfied with it. They may ask for such a review to be carried out within 21 days of the date of the response. If they ask for an internal review of the response, it will be conducted by the EWI Governor nominated to deal with Data Protection issues. The review must be completed within 14 days of receipt of the request for a review. The review response must also set out how further information concerning subject access requests can be obtained from the Information Commissioner's Office (the ICO), the right to complain to the ICO and the ICO's contact details.

Review

28. This Policy will be reviewed annually by the EWI Governors.