The General Data Protection Regulation (GDPR): IAH Policy

Introduction

The General Data Protection Regulation (GDPR) is an EU regulation (EU 2016/679) on data protection and privacy for all individuals within the European Union. It also addresses the export of personal data outside the EU. It aims to give control to people over their personal data and harmonise regulation across the EU. It comes into force on 25 May 2018.

The GDPR applies to 'processing', or simply keeping or using, 'personal data', including electronic and hard copy information. This is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier.

A 'data controller' is an organisation that determines the purposes and means of processing personal data. A 'data processor' is an organisation that processes personal data on behalf of a controller. We have a small Secretariat, with part-time staff, that acts as both controller and processor, with the roles undertaken by different members of staff. Organisations that process certain data on a large scale must have a 'data protection officer'. We consider that we are not required to have a data protection officer.

In preparing this policy we have referred extensively to the 'Guide to the General Data Protection Regulation' published by the Information Commissioner's Office (see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/).

Data protection impact assessment (DPIA)

We have carried out an assessment of our data processing activities to help to identify and minimise data protection risks. This review included:

- the data we gather
- how and why we use this data
- why it is necessary for us to process data, the rights of data providers and considerations of proportionality
- what the risks may be to individuals and how significant they may be
- our approach to mitigating risks and protecting data.

We consider that our use of data will not result in high risk to individuals' interests. We will review this assessment periodically.

Lawful basis for processing data

A valid lawful basis is required for processing personal data. If this basis is not necessary for the data-processing, then it is not a lawful basis.

We aim to give people as much control and responsibility for their data as possible (including the ability to change their mind as to whether it can continue to be processed) and so where

possible we rely on consent as our legal basis for using data. We also use legitimate interests, contracts and legal obligation as the legal basis where appropriate:

- **Consent:** the individual has given clear consent to process their personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract with the individual, or because they have asked that we take specific steps before entering into a contract.
- **Legitimate interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.
- **Legal obligation:** the processing is necessary to comply with the law (not including contractual obligations).

We inform data providers of the legal basis that we rely on for using their data and how we intend to make use of their data. We inform them of any third party who will also act as controllers or as data processors.

Where we act on the basis of consent, we ask people actively to opt in (rather than opt out) and inform them that they can withdraw consent at any time. We keep records to show who gave consent, when, how, and what they were told.

Data we use

We collect personal data for various purposes:

Who	What	Why	Who uses	Legal basis
Members	Name, address, email, phone Occupation and professional interests	• Process membership applications and renewals • Send hard copy and digital communications - Hydrogeology Journal, newsletters, updates • Share contact details with national chapters (including for membership renewals), commissions and networks, for group-specific communications • Sponsored members • Share details with website host for processing	Secretariat Secretariat, Springer NCs, C&Ns Website host	Legitimate interest and consent
Non-members	Email	Send digital communications – newsletters, updates	Secretariat Campaign Monitor	Consent
Staff	Name, address, email, phone Bank details	General management, H&S, payroll Contact and pay data shared with payroll contractor;	Secretariat Payroll contractor Bookkeeper	Contract

		and with our Bookkeeper for processing payments Details relating to pay and tax	HMRC	Legal obligation
Contractors	Name, address, email, phone, payment details	Management of contracts	Secretariat Bookkeeper	Contract
Other corporate contacts	Name, address, email, phone	Marketing	Secretariat	Legitimate interest
HJ Authors	Name, address, email, phone	Management of submitted papers	TEA Editors Associate Editors	Consent
Others providing income	Contact details, details of income and source/reason	Processing data for financial statements and accounts Provision of data required for accounts	Secretariat Bookkeeper HMRC	Legitimate interest Legal obligation

We receive data via online forms and also in other electronic formats (email, spreadsheets, documents, scans, digital photos, fax) as well as hard copy documents by post.

Information to data providers and rights

GDPR provides certain rights to those who provide us with data dependent on the legal basis we use. Nonetheless, we aim to apply the range of rights to all data providers where this is reasonable and possible.

Legal basis	Erasure of data	Digital portability	Objection to use
Consent	√	√	× (though consent can be withdrawn)
Contract	√	√	×
Legitimate interest	√	×	√
Legal obligation	×	×	×

If data is considered to be incomplete or inaccurate then individuals have the right to ask for this to be rectified. We aim to make the rectifications as quickly as possible unless there is a valid reason for not doing so, on which case will notify the person concerned.

We accept that an individual always has the right to object to processing for the purposes of direct marketing, whichever lawful basis applies.

We accept that individuals are not obliged to provide personal data to us. However, without the requisite information we will not be able to offer some of our services.

Individuals have the right to make a complaint to us and to the supervisory authority regarding processing of their personal data if they are unsatisfied with how we have handled their

information. The supervisory authority in the UK is the Information Commissioner (contact https://ico.org.uk/global/contact-us/).

Documentation

We have fewer than 250 employees and process personal data occasionally. We do not consider that our use of data could result in a risk to the rights and freedoms of individuals. In accordance with the GDPR, we therefore document the following information.

Our controllers

- name and contact details
- the names and contact details for national chapters, commissions and networks (including those based outside the EU) where they act as joint controllers
- why we use personal data
- the types of people whose personal data is processed
- the types of information we process about people
- who we share data with
- how long we will keep the data for
- our technical and organisational security measures for protecting personal data

Our processors

We record details of those who process data on our behalf and issue them with written instructions (in effect a contract). These include:

- the types of data use e.g. membership renewals, providing news updates.
- ensuring technical and organisational security measures for protecting data
- notification of personal data breaches
- a duty of confidence
- delete or return all personal data to the controller at the end of the contract
- use of a sub-processor only with the prior written authorisation of the controller
- co-operation with supervisory authorities (such as the ICO)
- record keeping for processing activities

Data retention

We retain data for as long as is necessary. We are required under UK tax law to keep relevant basic personal data (name, address, contact details) for a minimum of 6 years after, which time it will be destroyed. Where individuals have given their consent for us to use their details for direct contact, including marketing, we will keep this data until they inform us of their withdrawal of consent. We will review other data at least every 3 years and consider whether it is necessary to retain this.

Data Security

GDPR requires us to have a level of security that is 'appropriate' to the risks presented by your processing. We must ensure the 'confidentiality, integrity and availability' of our systems and services and the personal data we process within them.

In line with these requirements, our security measures aim to ensure that:

- the data can be accessed, altered, disclosed or deleted only by those we have authorised to do so (and that those people only act within the scope of the authority you give them);
- the data we hold is accurate and complete in relation to why we are processing it; and
- the data remains accessible and usable, i.e., if personal data is accidentally lost, altered or destroyed, we are able to recover it and therefore prevent any damage or distress to the individuals concerned.

In applying our data security provisions we take account of data that may be accessible by others e.g. processors and their security arrangements, during computer maintenance, theft or loss of equipment, the abandonment of old computers or hard-copy records being lost, stolen or incorrectly disposed of.

International transfers

The GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations. We transfer data where this is

- made with the individual's informed consent;
- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- in the case of legitimate interest, provided such interests are not overridden by the interests of the individual.

In all cases we seek to ensure that the organisation receiving the personal data has adequate safeguards for data security.

Our privacy notice

We include the following in our privacy notice:

- The lawful basis for the processing.
- Where we cite 'legitimate interests' as the basis for the processing we state these interests, with the appropriate justification.
- The rights available to individuals regarding the processing.
- The source of personal data if this was not obtained directly from an individual.

Marketing

We acknowledge that when we provide information in our newsletters and email updates that includes encouragement to join the IAH and to support us in other ways, then this constitutes marketing. We seek opt-in consent from individuals so that we can provide this information and accept that consent may be withdrawn at any time.

We will proactively contact companies and organisations as part of our marketing activities. In doing so we will contact personnel in the departments that would reasonably expect to receive such marketing contact and we do this as part of our legitimate interest. When we contact companies and individuals in this way we will inform them that they have the right to opt out of such contact.

We will also speak with people at conferences and meetings and seek their consent to receiving marketing information. In such cases individuals will have the right to withhold consent or subsequently withdraw it once it has been given.

Personal data breaches

An occurrence of the following will be considered to be a personal data breach: should any personal data be lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

We will ensure that we quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

Data protection fee

We process personal data only for the following purposes to support our core business purpose:

- Staff administration
- Advertising, marketing and public relations
- Accounts and records
- Not-for-profit purposes

On this basis we consider we do not need to pay a data protection fee.

Review of this policy

We will review this policy periodically, at least every 3 years or sooner where our attention is drawn to particular issues, and make any additions needed to ensure that it continues to accord with the GDPR.

Ian Davey, IAH Executive Manager

May 2018