

	Document Name	
	Data Protection Policy	
	Document No.	HR/PD/24
	Revision No.	02
	Authorised by:	SAI
	Date	Oct 2022
	Pages	1 of 5

DATA PROTECTION POLICY

1. POLICY STATEMENT

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process data about our employees, members, Committees/Groups/Special Interest Groups, customers, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful activities in our operations.

All Data users are obliged to comply with this policy when processing data on our behalf.

2. SCOPE

The types of data that ASME may be required to handle includes information about current, past and prospective members, Directors, Committees/Groups/Special Interest Groups committees, employees, suppliers, customers and others that we communicate with.

The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the amended UK Data Protection Act 2018 and the UK GDPR (General Data Protection Regulations) 2018 (the Acts) and other relevant regulations.

On 28 June 2021 the EU Commission adopted decisions on the UK's adequacy under the EU's General Data Protection Regulation (EU GDPR) and Law Enforcement Directive (LED). In both cases, the European Commission has found the UK to be adequate. This means that most data can continue to flow from the EU and the EEA without the need for additional safeguards. From 1 January 2021, the UK is a 'third country' for EU General Data Protection Regulations (GDPR) purposes.

The UK GDPR imposes restrictions on the transfer of personal data to a 'third country' unless that country benefits from an adequacy decision. The EU Exit Regulations effectively grant interim adequacy decisions in favour of all the EEA member states. Therefore, UK organisations may continue to be able to send personal data to organisations in the EEA and will allow organisations to continue to rely on the 13 existing adequacy decisions adopted by the EU. Whilst the adequacy decisions remain in place, the UK GDPR applies.

Both decisions are expected to last until 27 June 2025.

ASME only transfer personal data outside the UK to consumers (ie our members) or only receive personal data from outside the UK directly from consumers.


This policy and any other documents referred to in it, sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

We will ensure that all relevant personnel are trained in their GDPR responsibilities and that the data we hold is processed correctly and kept safe.

3. DEFINITIONS

Data: is recorded information whether stored electronically on a computer, or in certain paper-based filing systems.

Data: means personal data relating to a living individual who can be identified from that data (even if pseudonymised). Personal data can be both factual (such as name, address or occupation), or an opinion such as a performance appraisal. It is important that the information has the data subject as its focus as it

	Document Name	
	Data Protection Policy	
	Document No.	HR/PD/24
	Revision No.	02
	Authorised by:	SAI
	Date	Oct 2022
	Pages	2 of 5

affects the individual's privacy in some way. Mention of a person's name in a document does not constitute personal data, but personal details such as someone's contact details or salary would fall within the scope of the Acts.

Data controllers are the people or organisations who determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Acts. ASME is the data controller of all data used in our business for our own organisational purposes.

Data Users: includes employees whose work involves using data and ASME's Committees/Groups/Special Interest Group committees.. Data users have a duty to protect the information they handle by following this data protection policy at all times.

Data Subjects: for the purposes of this policy, this includes all individuals about whom the Company holds personal data. All data subjects have legal rights in relation to their personal information. This is detailed in our **Privacy Policy**.

Processing: is any activity that involves the use of data. It includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Special personal data: includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life/orientation, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Special personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.


4. GDPR PRINCIPLES

Anyone processing personal data must comply with the UK GDPR seven principles of good practice. These are:-

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

4.1. LAWFULNESS, FAIRNESS AND TRANSPARENCY

For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Acts. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When special personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that these requirements are met.

	Document Name	
	Data Protection Policy	
	Document No.	HR/PD/24
	Revision No.	02
	Authorised by:	SAI
	Date	Oct 2022
	Pages	3 of 5

There are 6 Lawful Bases for collecting and processing data.

- Consent
- Contract
- Legal Obligation
- Vital Interest
- Public Task
- Legitimate Interests

ASME details which are used and for what purpose in our Privacy Policy, which can be either requested in writing or accessed on our website at www.asme.org.uk

If we collect personal data directly from data subjects, we will inform them about:

- The purpose or purposes for which we intend to process that personal data.
- The types of third parties, if any, with which we will share or to which we will disclose that personal data.
- The means, if any, with which data subjects can limit our use and disclosure of their personal data.

If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

We will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

If there has been a breach in our data protection which could have a detrimental effect on the data subject, we will inform them (and the Information Commissioners Office - ICO) within 72 hours.

4.2. PURPOSE LIMITATION

In the course of our business, we may collect and process personal data. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, and others).


We will only process personal data for purposes specifically permitted by the Acts. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

4.3. DATA MINIMISATION

We will only collect personal data to the extent that it is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

4.4. ACCURACY

Any Personal data kept will be accurate and, where necessary, kept up to date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. The Data Subject has the right to request that any incorrect data is corrected, to be deleted (other than data ASME is legally obliged to process, eg for HMRC).

	Document Name	
	Data Protection Policy	
	Document No.	HR/PD/24
	Revision No.	02
	Authorised by:	SAI
	Date	Oct 2022
	Pages	4 of 5

4.5. STORAGE LIMITATION

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

4.6. INTEGRITY AND CONFIDENTIALITY

4.6.1. We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

4.6.2. We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies or if they put in place adequate measures themselves and can confirm their compliance to UK GDPR 2021.

4.6.3. We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it.
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored in a common filing system rather than in individuals' own systems or own PCs.
- Security procedures include:
 - Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind (Personal information is always considered confidential.)
 - Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
 - Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
 - IT systems are all password protected and have sufficient protection against cyber attacks. This is subject to regular testing.

4.7. ACCOUNTABILITY

ASME is responsible for complying with the UK GDPR 2021 and we have put in place appropriate technical and organisational measures to meet the requirements of accountability.

5. TRANSFERRING PERSONAL DATA TO/FROM AN EEA COUNTRY

5.1 Data transfers from ASME to EEA countries

We can still send personal data to the EU/EEA, Gibraltar and other countries deemed "adequate" by the EU. They have adequate protection by the UK Government under the new arrangements. We will always do so securely in accordance with the UK GDPR principles.

	Document Name	
	Data Protection Policy	
	Document No.	HR/PD/24
	Revision No.	02
	Authorised by:	SAI
	Date	Oct 2022
	Pages	5 of 5

5.2 Data transfers to ASME from EEA countries

Because the UK is currently deemed a 'third country', the EU require additional protection when transferring personal data to the UK. We use the Standard Contractual Clauses to make sure that data transfers are secure and lawful. These are EU approved terms to facilitate the continued exchange of personal data. This is the most appropriate safeguarding available to ASME and ensures that we continue to protect personal data flowing into the UK from the EEA.

6. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

6.1 We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- The Third Party has confirmed its compliance to UK GDPR 2021
- The data subject has given their consent.
- The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
- The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

6.2 Subject to the requirements in clause 5.1 above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

7. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

We may also disclose personal data we hold to third parties if we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction, where they have confirmed their compliance to UK GDPR requirements.

8. DEALING WITH SUBJECT ACCESS REQUESTS

Data subjects must make a written *formal* request for information we hold about them. This will be responded to within one month of receipt.

ASME employees who receive a written or verbal request from another individual should forward it to the Operations Manager/Data Controller immediately.

9. CHANGES TO THIS POLICY

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.