Policy	IEMA Transforming the world to sustainability

DATA PROTECTION 2018 & UK GDPR 2021

A. Introduction

IEMA is committed to complying fully with the Data Protection Act 2018. We are required to maintain certain personal data about individuals for the purposes of satisfying our operational and legal obligations. This policy has been written to assist our employees in understanding our obligations under the Act in the processing of information relating to current, past, and prospective employees and members; clients; suppliers and other organisations with whom we have dealings. The policy relates to information provided to us online, via phone or text, by email, in letters or correspondence.

B. Scope and aims of this policy

The aim of the policy is to assist an employee to comply with the legal requirements of the Data Protection Act 2018 and to minimise any risk to IEMA by setting out clear guidelines relating to the processing, storage, and disposal of data.

C. Legal considerations

The following legislation applies to this policy:

- the Data Protection Act 2018
- any Codes of Practice issued by the Information Commissioner's Office (ICO)

D. Definitions

The Data Protection Act lays down conditions for the processing of any personal data and makes a distinction between personal and sensitive personal data.

Personal data is defined as data relating to a living individual who can be identified from that data; or from that data and other information, which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information regarding an individual's racial or ethnic origin, political opinion, religious or other beliefs, trade union membership, physical or mental health or condition, sexual life, or criminal proceedings or convictions.

E. Principles

IEMA adhere to the 8 principles of the Data Protection Act:

1. Personal information must be fairly and lawfully processed
2. Personal information must be processed for limited purposes
3. Personal information must be adequate, relevant, and not excessive
4. Personal information must be accurate and up to date
5. Personal information must not be kept longer than is necessary
6. Personal information must be processed in line with the data subjects' rights
7. Personal information must be secure
8. Personal information must not be transferred to other countries without adequate protection

These principles apply to obtaining, handling, processing, transportation, and storage of personal data and applies to employees and associates of IEMA who must always adhere to these principles. Please also refer to our IT Systems, Internet, and Email Policy.

F. Responsibilities

Not complying with these requirements could lead to legal implications for you and the organisation and may also lead to disciplinary action, including dismissal as a possible outcome.

G. Database

The database contains confidential information about our members, clients, and suppliers and as such, this information must not be removed from its static location in any format, unless the removal or transfer is authorised by a member of the Leadership Team. Please also refer to IT Systems, Internet, and Email Policy.

H. Subject access request (GDPR)

This procedure sets out the key features regarding handling or responding to requests for access to personal data made by data subjects, their representatives, or other interested parties. This procedure will enable IEMA to comply with legal obligations, provide better customer service, improve transparency, enable individuals to verify that information held about them is accurate, and increase the level of trust by being open with individuals about the information that is held about them.

This procedure applies to employees that handle data subject access requests such as the Data Protection Officer and Head of Operations.

I. Reference documents

1. UK GDPR 2021
2. Data Protection Act 2018

J. Subject access requests

- A Subject Access Request (SAR) is any request made by an individual or an individual's legal representative for information held by IEMA about that individual. The Subject Access Request provides the right for data subjects to see or view their own personal data as well as to request copies of the data.

- A Data Subject Access Request must be made in writing. In general, verbal requests for information held about an individual are not valid DSARs. In the event a formal Data Subject Access Request is made verbally to a staff member of IEMA, further guidance should be sought from the Data Protection Officer, who will consider and approve all Data Subject Access Request applications.

- A Subject Access Request can be made via any of the following methods: email, post, corporate website, or any other method. SARs made online must be treated like any other Subject Access Requests when they are received, though IEMA will not provide personal information via social media channels.

K. The rights of the data subject

- To know whether a data controller holds any personal data about them.
- Receive a description of the data held about them and, if permissible and practical, a copy of the data.
- Be informed of the purpose(s) for which that data is being processed, and from where it was received.
- Be informed whether the information is being disclosed to anyone apart from the original recipient of the data; and if so, the identity of those recipients.
- How long IEMA will store the data, and how we made that decision.
- Information on the data subjects' rights to challenge the accuracy of their data, to have it deleted, or to object to its use.
- The right of data portability. Data subjects can ask that their personal data be transferred to them or a third party in machine readable format (Word, PDF, etc.). However, such requests can only be fulfilled if the data in question is:
    - Provided by the data subject to IEMA
    - Is processed automatically and is processed based on consent or fulfilment of a contract

- If the data is being used to make automated decisions about the data subject, to be told what logic the system uses to make those decisions and to be able to request human intervention
- Their right to complain to the ICO
- Whether their data is used for profiling or automated decision making and how it is doing this.
- IEMA must provide a response to data subjects requesting access to their data within 30 calendar days of receiving the Subject Access Request
- A copy of the requested data should be provided free of charge

L. Requirements for a valid SAR

To be able to respond to the Subject Access Requests in a timely manner, the data subject should:

- Provide IEMA with enough information to validate his/her identity (to ensure that the person requesting the information is the data subject or his/her authorised person)

IEMA will provide information to data subjects whose requests are in writing and are received from an individual whose identity can be validated by IEMA. However, IEMA will not provide data where the resources required to identify and retrieve it would be excessively difficult or time-consuming. Requests are more likely to be successful where they are specific and targeted at information.

Factors that can assist in narrowing the scope of a search include identifying the likely holder of the information (e.g. by making reference to a specific department), the time period in which the information was generated or processed (the narrower the time frame, the more likely a request is to succeed) and being specific about the nature of the data sought (e.g. a copy of a particular form or email records from within a particular department).

M. SAR process

F.1 Requests

Upon receipt of a SAR, the Data Protection Officer will acknowledge the request.

F.2 Identity Verification

The Data Protection Officer needs to check the identity of anyone making a SAR to ensure information is only given to the person who is entitled to it. If the identity of a SAR requestor has not already been provided, the person receiving the request will ask the requestor to provide two forms of identification, one of which must be a photo identity and the other confirmation of address.

If the requestor is not the data subject, written confirmation that the requestor is authorised to act on behalf of the data subject is required.

F.3 Information for Subject Access Request

Upon receipt of the required documents, the person receiving the request will provide the Data Protection Officer with all relevant information in support of the SAR. Where the Data Protection Officer is reasonably satisfied with the information presented by the person who received the request, the Data Protection Officer will notify the requestor that his/her SAR will be responded to within 30 calendar days. The 30-day period begins from the date that the required documents are received. The requestor will be informed by the Data Protection Officer in writing if there will be any deviation from the 30-day timeframe due to other intervening events.

F.4 Review of information

The Data Protection Officer will contact and ask the relevant department(s) for the required information as requested in the SAR. This may also involve an initial meeting with the relevant department to go through the request, if required. The department which holds the information must return the required information by the deadline imposed by the Data Protection Officer and/or a further meeting is arranged with the department to review the information. The Data Protection Officer will determine whether there is any information which may be subject to an exemption and/or if consent is required to be provided from a third party.

The Data Protection Officer must ensure that the information is reviewed/received by the imposed deadline to ensure the 30-calendar day timeframe is not breached. The Data Protection Officer will ask the relevant department to complete a “Data Subject Disclosure Form” to document compliance with the 30-day requirement.

F.5 Response to Access Requests

The Data Protection Officer will provide the finalised response together with the information retrieved from the department(s) and/or a statement that IEMA does not hold the information requested, or that an exemption applies. The Data Protection Officer will ensure that a written response will be sent back to the requestor. This will be via email, unless the requestor has specified another method by which they wish to receive the response (e.g., post). IEMA will only provide information via channels that are secure. When hard copies of information are posted, they will be sealed securely and sent by recorded delivery.

F.6 Archiving

After the response has been sent to the requestor, the SAR will be considered closed and archived by the Data Protection Officer.

F.7 Exemptions

An individual does not have the right to access information recorded about someone else, unless they are an authorised representative, or have parental responsibility.

IEMA is not required to respond to requests for information unless it is provided with enough details to enable the location of the information to be identified, and to satisfy itself as to identity of the data subject making the request.

In principle, IEMA will not normally disclose the following types of information in response to a Subject Access Request:

- Information about other people – A SAR may cover information which relates to an individual or individuals other than the data subject. Access to such data will not be granted unless the individuals involved consent to the disclosure of their data.
- Repeat requests – Where a similar or identical request in relation to the same data subject has previously been compiled within a reasonable time period, and where there is no significant change in personal data held in relation to that data subject, any further request made within a six-month period of the original request will be considered a repeat request, and IEMA will not normally provide a further copy of the same data.
- Publicly available information – IEMA is not required to provide copies of documents which are already in the public domain.
- Opinions given in confidence or protected by copyright law – IEMA does not have to disclose personal data held in relation to a data subject that is in the form of an opinion given in confidence or protected by copyright law.
- Privileged documents – Any privileged information held by IEMA need not be disclosed in response to a SAR. In general, privileged information includes any document which is confidential (e.g., a direct communication between a client and his/her solicitor) and is created for the purpose of obtaining or giving legal advice.

N. SAR refusal

There are situations where individuals do not have the right to see information relating to them. For instance:

- If the information is kept only for the purpose of statistics or research, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved.
- Requests made for other, non-data protection purposes can be rejected.

If the responsible person refuses a SAR on behalf of IEMA, the reasons for the rejection must be clearly set out in writing. Any individual dissatisfied with the outcome of his/her SAR is entitled to make a request to the Data Protection Officer to review the outcome or raise their concerns with the ICO.

O. Related policies

- Security Incident Response Plan
- Mobile Device Usage and Security Policy
- IT Systems, Internet and Email Policy

P. Updates

Any changes or amendments to this policy will be communicated to all staff.

Document History

Version	Date	Reason for Change
1.0	January 2019	Original Version
2.0	November 2021	DPA 2018 & SAR requests merged under the policy header Data Protection Act 2018 & UK GDPR 2021. New Template with Version Control and Document History Added.