IMC WORLDWIDE GROUP.

PERSONAL DATA RETENTION POLICY

The IMC Worldwide Group (IMC) is committed to protecting and respecting individuals' privacy.

This policy sets out our retention policy for personal data as well as the minimum standards to be applied when destroying certain information within IMC.

PURPOSE, SCOPE AND USERS

Personal Data is defined as any information relating to an individual or identifiable individual e.g by means of an identification number.

This Policy applies to all business streams, regional teams, support teams, processes and systems across IMC and in all countries in which we work.

It applies to all employees, independent consultants, agents and affiliates (IMC staff), that may collect, process, or have access to personal data (including sensitive personal data). It is the responsibility of all of the above to familiarise themselves with this Policy and ensure adequate compliance with it.

This Policy applies to all personal data held by IMC. Examples of information include but are not limited to:

- Name
- Date of Birth
- Postal address
- CVs
- Fitness to Travel Assessments
- Personal contact details (eg telephone, mobile number, email, or facsimile number)
- Occupation, references and previous employment history, qualifications and skills
- Information regarding availability, fees rates and working preferences
- Personal Information provided through our website, Facebook or Twitter accounts
- Personal data provided by partner organisations or clients
- Consultant invoices
- Information obtained through other public media forums (e.g. LinkedIn, Devex, Indeed, etc)
- Bank Accounts
- Passports
- Contractual and performance history

- Photographs
- Medical Screening data

It does not cover retention of more general data such as project documentation.

RETENTION RULES

GENERAL PRINCIPLE

For any category of documents not specifically defined in the Data Retention Schedule and unless otherwise mandated differently by applicable law or by specific contractual requirements, the required retention period for such documents will be deemed to be 10 years from the date of creation of the document.

RETENTION SCHEDULE

The time period for which documents and electronic records should be retained is managed through IMC's Data Retention Schedule.

There are exemptions to the retention periods specified within the Data Retention Schedule, these include:

Donor or client requirements for data to be held for a specified period longer or less than our standard retention periods;

Ongoing investigations, if there is a chance records of personal data will be required by IMC to prove compliance with any legal requirements;

When exercising legal rights in cases of lawsuits or similar court proceeding.

DESTRUCTION OF PERSONAL DATA

IMC will review personal data whether held electronically or in hard format on a periodic basis and decide whether to destroy or delete any data once the purpose for which the document was stored is no longer relevant or the retention period stated in the Data Retention Schedule has been reached.

Once the decision has been made to dispose of data it should be deleted, shredded or otherwise permanently destroyed. The method of disposal varies and is dependent upon the nature of the document. For example, any printed documents that contain sensitive or confidential personal information must be disposed of confidentially. The specific deletion or destruction process may be carried out either by IMC staff or by a service provider subcontracted for this purpose.

Any applicable general provisions under relevant data protection legislation and IMC's Data Protection Policy and Privacy Policy shall be complied with.

Appropriate controls shall be in place that prevent the permanent loss of essential information to the company as a result of malicious or unintentional destruction of information – these controls are described in IMC's IT Security Policy.

The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection legislation, shall be fully observed.

BREACH, ENFORCEMENT AND COMPLIANCE

The person appointed with responsibility for data protection within IMC is the Finance Director who has responsibility to ensure that each of IMC's offices complies with this Policy. It is also the responsibility of the IMC Finance Director to assist any overseas offices with enquiries from any local data protection or governmental authority.

Any suspicion of a breach of this Policy must be reported immediately to the IMC Finance Director. All instances of suspected breaches of the Policy shall be investigated and action taken as appropriate.

Failure to comply with this Policy may result in adverse consequences, including, but not limited to, loss of client/donor confidence, litigation and loss of competitive advantage, financial loss and damage to IMC's reputation, personal injury, harm or loss. Non-compliance with this Policy by employees may result in disciplinary action and may be considered gross misconduct. For independent consultants, or any third parties, who have been granted access to IMC's premises or information a non-compliance with this Policy may result in termination of their contract. Such non-compliance may also lead to IMC taking legal action against the parties involved in such activities.

DOCUMENT DISPOSAL

ROUTINE DISPOSAL SCHEDULE

The types of Personal Data which should be routinely destroyed by staff, unless subject to an on-going legal or regulatory inquiry, are as follows:

- Email correspondence that is no longer relevant or required
- Announcements and notices of day-to-day meetings and other events including acceptances and apologies
- Requests for ordinary information such as travel directions
- Reservations for internal meetings
- Transmission documents such as letters, fax cover sheets, e-mail messages, routing slips, compliments slips and similar items that accompany documents but do not add any value

- Duplicate documents such as CC and FYI copies, unaltered drafts, snapshot printouts or extracts from databases and day files

Out of date CV's (e.g where an updated version has been received).

PERIODIC DISPOSAL SCHEDULE

Personal data held for independent consultants and partner staff will be reviewed periodically and if the personal data is no longer required it shall be deleted or securely disposed of in line with the provisions of IMC's Data Retention Schedule and/or in line with agreed timescales as set out in the client's contract. Data to be reviewed may include, inter-alia:

- Name
- Date of Birth
- Postal address
- CVs
- Passports
- Fitness to Travel Assessments
- Personal contact details (eg telephone, mobile number, email, or facsimile number)
- Occupation, references and previous employment history, qualifications and skills
- Information provided through our website, Facebook or Twitter accounts
- Personal data provided by partner organisations or clients
- Information obtained through other public media forums (e.g. LinkedIn, Devex, Indeed, Twitter, Facebook and Instagram etc)
- Information regarding availability, fees rates and working preferences
- Photographs

On occasion it may be necessary to maintain a limited record for individuals including the individuals name and detailing that contact is no longer relevant/welcome, for example when someone notifies us that they have retired.

DESTRUCTION METHOD

When deleting or destroying any personal data, every reasonable measure must be taken to ensure it is undertaken in a manner which is secure and safeguards privacy;

Care must be taken to ensure that:

Duplications are identified.

Historical versions are identified (eg in computer history).

Versions held in backup files or servers are identified.

All identified versions that are no longer required are deleted securely and irrevocably.

Where IMC is acting as a Processor on behalf of a client. On instruction from the Controller, any personal data held on behalf of a client must be returned to the client without undue delay and deleted from our systems immediately.

On occasion it may be necessary to retain evidence of the removal, deletion or destruction of personal data, particularly when the data subject has requested information regarding the erasure or has asserted the right to be forgotten.

If we receive a request to have personal data erased or forgotten in accordance with a data subject access request, we may need to inform any previous recipients of that data so that they can take steps to remove, return, delete or destroy the data as appropriate.

Gavin English, Managing Director, IMC Worldwide Limited

April 2020

RELATED DOCUMENTS AND POLICIES

IMC Data Protection Policy

IMC Privacy Policy

IMC's IT Security Policy