IMC Worldwide Ltd. Data Protection Policy

The General Data Protection Regulations (GDPR) imposes responsibilities on all companies regarding the collection and use of information about individuals. This policy outlines IMC Worldwides's (IMC) duties and obligations under the GDPR. It also sets out a standardised approach for IMC staff to follow to allow them to manage personal data within the terms of the GDPR. Other individuals should refer to IMC's Privacy Policy which provides information about their rights with respect to any personal data that IMC may hold about them.

SCOPE

This policy applies to all personal data collected by IMC in the conduct of its business and applies to both automated personal data and to manual filing systems.

This policy applies to all IMC Worldwide Ltd staff whether they are employees, permanent or otherwise, or independent consultants or agents contracted by IMC. It applies wherever the employee or independent consultant is based, including when working and/or managing personal data outside the EEA.

PERSONAL DATA DEFINITION

Personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

IMC'S APPROACH

IMC Worldwide policy is to treat individuals fairly and within the terms of the law. IMC obtains and holds personal information and data for a variety of lawful basis as specified in our Privacy Policy

Personal data should be held securely and confidentially, paying attention to the individuals right to privacy.

GDPR PRINCIPALS

The GDPR outlines six principles which underpin the handling of personal data. To ensure compliance with the Regulation, IMC must ensure that personal data is:

a) Processed **lawfully, fairly and in a transparent** manner. In practice this means:
   - Having a legitimate ground for collecting and using personal data. In the majority of cases we are processing data for legitimate business interest or contractual necessity.
   - Not using personal data in a way that would have an adverse effect on the individual concerned.

- Being transparent about how you intend to use personal data and provide privacy notices where appropriate.
- Handling personal data in a way that the individual would reasonably expect.
- Ensuring that you do nothing unlawful with personal data.

(b) Collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes. In practice this means:

- Being clear about why you are collecting personal data and what you will do with it.
- Providing privacy notices when collecting personal data.
- Ensuring that any additional processing of personal data is fair.

(c) **Adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed. In practice this means:

- Only processing personal data that is necessary for the successful delivery of our business.

(d) **Accurate** and, where necessary, kept up to date. In practice this means:

- Taking reasonable steps to ensure the accuracy of any personal data held. E.g an extremely old CV or passport cannot be considered accurate.
- Ensuring that the source of the personal data is clear.
- Carefully considering any challenges to the accuracy of personal data.
- Considering whether it is necessary to update the information.

(e) **Time Limited** and not kept for longer than is necessary. In practice this means:

- Reviewing the length of time you keep personal data for. In practice this means:
- Considering the purpose you hold the personal data for in deciding whether, and how long, you retain it.
- Securely deleting information that is no longer needed.

(f) Processed in a manner that ensures adequate security of data using appropriate technical and organisational measures against unauthorised or unlawful processing, loss, damage or destruction. In practice this means:

- Designing and organising security to fit the nature of the personal data held and the harm that may result from the breach.
- Ensuring that the right physical and security measures are in place, backed by robust policies and procedures and reliable, well-trained employees.
- Reporting security breaches promptly so that they can be reported to the Information Commissioner's Office within the required 72 hours timescale.

IMC staff who process or use any personal information must they comply with these principles at all times.

There are stringent restrictions on sensitive data. Individuals must give their explicit consent if IMC wishes to process such data. Sensitive data includes racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sexual life or criminal record.

ACCESS TO PERSONAL DATA

Staff have access to the personal data they require to successfully win and deliver our business and to meet our contractual obligations.

DATA SUBJECT ACCESS REQUESTS

All data subjects (including employees, independent consultants and other individuals) have the right to make a Subject Access Request to see what personal data we hold about them. Exemptions may apply in certain circumstances.

Data Subject Access Requests (DSAR) are co-ordinated by the Finance Director in accordance with the Data Subject Access Request Policy. If you receive a DSAR you must forward it to the Finance DIrector immediately. IMC has one month to respond to DSAR's.

Once a DSAR is received you must not delete or change any data that we may hold about that individual.

DATA SHARING

Where it is necessary to share data with a third party and/or outside the EEA, you must obtain the data subjects permission to do this prior to sharing the information. Where personal data is being shared outside the EEA, for example in proposals, you must have clearly documented confirmation from the individual concerned that they are aware that their personal data is being shared.

DATA RETENTION

Personal data should only be kept for as long as necessary. The duration depends on the nature of the personal data and the purposes for which it was received.

When we no longer need to process or retain personal data to to meet our business needs, fulfil our contractual obligations, comply with legal obligations, resolve disputes, or enforce our agreements it should be deleted from our systems.

ROLES AND RESPONSIBILITIES

The Finance Director has overall responsibility for IMC's compliance as a data controller.

It is the responsibility of IMC Worldwide's International Resource, Business Improvement Leader, HR and Finance Teams to ensure that sensitive personal information about individuals is kept securely and confidentially.

All IMC staff are responsible for ensuring that:

- they meet the requirements of the GDPR
- are familiar with this policy and related documents

- Any personal data which they hold is kept securely, for example:
    - Computers and laptops are password protected,
    - Any data kept on a disc or memory stick, must be kept securely,
    - If it is in hard copy, to be kept in a locked drawer, or kept in a locked filing cabinet.
- Personal information is not disclosed accidentally or otherwise either orally or in writing to any unauthorised third party.
- Personal data, whether digital or hardcopy is disposed of safely and confidentially.

IMC staff should note that unauthorised disclosure of personal data will usually be a disciplinary matter, and could be regarded as constituting gross misconduct.

Gavin English, Managing Director, IMC Worldwide Limited

RELATED POLICES AND DOCUMENTS

IMC Privacy Policy