1 Applicant Privacy Policy – IMC

1.1 Introduction

This policy establishes a set of privacy principles and applies those principles as policy requirements in respect to all IMC offices with regards to all Data Subjects.

These principles and policy requirements establish IMC's Privacy Policy ("Privacy Policy") and govern how Personal Data in both electronic and paper formats is processed. This Privacy Policy is in effect for all offices of IMC and applies to all IMC Employees, contractors, vendors and third parties contracted by IMC ("IMC Data Processors") who work with or have access to Personal Data regarding IMC's Data Subjects.

1.2 IMC Privacy Principles

Privacy is both a necessity and an opportunity. It is imperative that IMC Data Processors protect Personal Data as outlined within this Privacy Policy.

This Privacy Policy will help IMC Data Processors to comply with IMC's Privacy Principles and applicable local privacy laws and regulations.

1.2.1. Below IMC's privacy principles are stated:

a) Personal Data shall be processed fairly and lawfully and according to the provisions in this Privacy Policy.

b) Personal Data shall be obtained only for one or more specified and lawful purposes ("Purpose"), and shall not be further processed in a manner that is incompatible with that Purpose.

c) Personal Data shall be adequate, relevant and not excessive in relation to the Purpose for which they are processed.

d) Personal Data shall be accurate and, where necessary, kept up to date. IMC makes use of reasonable steps to verify that Personal Data is accurate, complete and current.

e) Personal Data processed for any Purpose shall not be kept longer than necessary for the Purpose for which the information was collected or for which it is further processed, or for such longer period as may be required by applicable laws, regulation, or contractual responsibilities.

f) IMC will limit the collection and use of Personal Data to that which is required and relevant for business purposes and in accordance with the initial Privacy Notice as provided to the Data Subject by IMC.

g) Departments within IMC will rely to the fullest extent possible on original sources of Personal Data. The use of secondary copies of Personal Data (e.g. created spreadsheets, databases, and printed reports) will be limited.

h) IMC provides Data Subjects at reasonable intervals the ability to request in writing access to their Personal Data. IMC shall inform the Data Subject in writing within four weeks after the request as to whether Personal Data relating to him/her are being processed or shall be corrected.

i) Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data. IMC will implement Physical, Administrative, and Technical safeguards to protect Personal Data about Data Subjects from loss, misuse, unauthorized access, disclosure, alteration or destruction. Reference is made to IMC's Information Security Policies for specific guidance about implementing measures for protection of Personal Data about Data Subjects. This policy is intended to supplement, but does not supersede, IMC's Information Security Policies.

j) Personal Data shall not be transferred to a country or territory outside the European Economic Area or Australia[1] unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of Personal Data. IMC has entered into an intercompany Model Contract that ensures an adequate level of protection for each office location (including Hong Kong and Chicago), based on which IMC can internally transfer Personal Data.

1.3 Disclosure

Although, IMC recognizes the need to apply the principles from this Privacy Policy, there may be circumstances, based on which IMC will need to disclose Personal Data. These circumstances are listed below:

Internal:

IMC may share Personal Data internally for legitimate and approved business purposes as laid down in the Model Contract or the Applicant Notification.

External:

Personal Data may be disclosed by IMC to non-affiliated third parties in the following circumstances, unless restricted by law, regulation or contract:

- When consistent with IMC's business purposes as laid down in the Model Contract and/or the Applicant Notification, or
- When the non-affiliated Third Party is acting as a service provider or Processor, or
- When the Data Subject has requested IMC to Transfer their Personal Data, or

[1] Based on applicable local privacy legislation that requires an adequate level of protection.

- When necessary to respond to an emergency that is believed to threaten risk of harm to the Data Subject, or
- When necessary to respond to a governmental inquiry or where required by applicable laws, court orders or government regulations, or
- When necessary to protect IMC's legal interests. In that case the interests of IMC will always be weighed against the interests of the Data Subject.

Furthermore, the following general principles apply with regard to disclosures:

- IMC will not sell or lease the Personal Data of its Data Subjects.
- Whenever possible, only Anonymized and aggregated Personal Data will be provided to third parties for analysis and reporting purposes.
- Exceptions, other than those for administrative or judicial process, must be approved by the General Counsel in writing before they are implemented or accepted. Requests for exceptions must be submitted in writing to IMC's Legal Department in Amsterdam, for review and approval.
- Third Party data processors will be carefully reviewed for suitability and reliability, given the nature of the Processing and data involved.
- Formal contracts with Third Party data processors address the following subject matters:
    - Personal Data will be processed in accordance with IMC's instructions
    - Personal Data will not be used for purposes other than as authorized by IMC's Legal Department
    - Data Subject requests to correct or amend their Personal Data may be executed only as stated in the terms as agreed between IMC and the Third Party contract
    - Personal Data about Data Subjects will be kept confidential
    - Security controls will be put in place to protect Personal Data against internal and external threats
    - Suitable legal protection will be stipulated so that IMC is protected from any potential harm or loss from unauthorized or accidental events by the Third Party
    - A procedure will be developed to allow for auditing and monitoring of Third Party Processing activities
    - Once the contracted service has been completed, any Personal Data held by the Third Party data processor will be destroyed or returned to IMC, unless required for further, agreed-upon Processing activities

These principles are intended to provide a set of requirements upon which IMC can develop additional data privacy and protection policies, procedures, and guidelines.

1.4 Notification

External

The processing of Personal Data intended to serve a single purpose or different related purposes will be notified to the relevant Data Protection Authority and/or the Legal Department before the processing is started.

Internal

Before starting a new processing of Personal Data, the processing has to be notified to IMC's Legal Department. The notification shall contain the following particulars:

- The name and address of the involved department;
- The purpose or purposes of the processing;
- A description of the categories of Data Subjects and of the data or categories of data relating thereto;
- The recipients or categories of recipients to whom the data may be supplied;
- The planned transfers of data to countries outside the European Union or Australia;
- A general description allowing a preliminary assessment of the suitability of the planned measures to guarantee the security of the processing.

1.5 Monitoring and Enforcement

Reasonable procedures are established to monitor compliance with this policy and to process inquiries and provide appropriate responses to complaints regarding Personal Data that is subject to this Privacy Policy.

2 Applicant Personal Data

2.1 Overview

In this paragraph IMC's Privacy Principles are specifically applied to Personal Data of Applicants. The additional privacy requirements for governing the Processing of Personal Data (in electronic and paper format) of Applicants are set forth in this paragraph.

2.2 Privacy Notice

IMC provides a reasonable, clear, and conspicuous notice describing its Processing of Personal Data about Applicants by means of this paragraph.

2.3 Purposes of Processing Applicant Personal Data

Personal Data of Applicants may only be processed based on legitimate grounds and for well-defined purposes. The purposes are included in the Applicant Notice.

2.4 Applicant' rights

IMC provides Applicants the ability to request in writing Access to their Personal Data. Applicants are further provided with the possibility to request Correction of their Personal Data.

When IMC receives a request of an Applicant to Access their Personal Data, IMC will:

- accurately identify an Applicant who requests Access to his/her own information.
- response to Applicant access requests in a reasonable timeframe, with a maximum of four weeks.
- Human Resources Departments will be able to correct or amend Applicant Personal Data in its electronic or paper format files if it is deemed to be inaccurate

Applicants will abide by instructions from the Human Resources Department when granting Access to, or facilitating the Correction of Personal Data about Applicants.

If Personal Data about an Applicant is stored in multiple locations and that Applicant makes a request to correct or amend the information, then the Correction will occur at all locations where their Personal Data resides, unless such Access would be a disproportionate effort in either time or IMC's resources.

IMC's obligation to respond to requests for Access, Correction may be limited in the following situations:

- when the burden or expense of providing Access would be excessive;
- when the rights of individuals other than the Applicant would be jeopardized.

2.5 Information Storage, Retention and Destruction

IMC takes reasonable steps to keep Personal Data about Applicants only as long as it is necessary for the purposes for which the information was collected or for which it is further processed or for such longer period as may be required by applicable laws, regulation or contractual responsibilities.

- If the holding of any information on criminal convictions of Applicants is justified, the information will be deleted once the information is no longer required.
- Applicant Personal Data that becomes irrelevant for Applicant administration purposes, when an Applicant's relationship status with IMC changes, will be destroyed when the information is no longer necessary.
- Personal Data about Applicants will be disposed of securely and effectively in all systems and locations where it may reside (e.g., documents containing Personal Data about Applicants will be shredded when no longer required, or removable media containing Personal Data about Applicable will be securely erased when it is no longer needed).
- IMC will identify Personal Data which are legally not allowed to be destroyed, even if requested by an Applicant due to either specified Retention periods or as required by court order or litigation requirements.
- Departments who have been approved to create secondary copies of Personal Data about Applicants (e.g., databases and printed reports) are responsible for prompt Destruction of that information when it is no longer necessary to complete legitimate business activities.

3 Appendix A: Glossary of Terms

The Glossary of Terms is a collection of applicable privacy-related terms and resources.
Many of the terms identified and defined in this Glossary of Terms originate from European privacy and security-related laws, regulations, guidelines and principles.

Term	Definition
Access	The ability to obtain or make use of Personal Data.
Administrative Safeguards	Administrative actions, including policies and procedures, to manage the selection, development, implementation and maintenance of security measures to protect Personal Data, and to manage the conduct of employees in relation to the protection of that information.
Affiliate	An entity that controls, is controlled by, or is under common control with another entity.
Anonymity	A condition wherein an individual's true identity is unknown.
Anonymize	A process of removing all personally identifying characteristic of information in such way that an individual's true identity is unknown.
Applicant	The term “Applicant” refers to an individual who is applying, or has applied, for a job at IMC.
Collection	The stage in the data life cycle that refers to the process of obtaining Personal Data from either an individual directly (such as via a registration form), or from another Party, such as an enterprise client or service provider.
Correction	The amendment of incomplete or inaccurate Personal Data. An Individual's or Entity's ability to Access their Personal Data also includes the ability to make Corrections.
Data Subject	The natural person whose Personal Data is processed.
Data Protection	The safeguarding of individuals' Personal Data collected or otherwise processed by an Entity.
Destruction	The stage in the data life cycle during which Personal Data is removed from the Entity and destroyed.
Disclosure	The release, Transfer, provision of Access to, or divulging in other manner of information outside the Entity holding the information. Disclosure is often used interchangeably with the terms "sharing" and "onward Transfer."
Employee	The term “Employee” refers to an individual who is currently, or was formerly, employed by IMC, and also includes contractors, vendors and third parties that are contracted by IMC.

Term	Definition
Entity	A legal body or organization that is not a natural person.
Government Identifier	A government-issued personal identifier such as a social security number, passport number, license number or vehicle identifier.
IMC offices	All subsidiary companies of IMC B.V.
IMC Data Processors	IMC Employees, contractors, vendors and third parties contracted by IMC who work with/or have access to Personal Data
Individual	A natural person.
Personal Data	As used in this document, Personal Data means any information regarding identified or identifiable individuals. Examples of Personal Data include, but are not limited to, any one or more of the following data elements: • Names, addresses, telephone numbers, date of birth • Financial account numbers (bank account, credit card, etc.) • Government identifiers (such as Social Security numbers or driver's license numbers) • Photograph or video identifiable to an individual • Other information related to an individual that may directly or indirectly identify the individual (e.g. salary, purchase history, call history, names of family Applicants etc.)
Privacy	The rights and obligations of individuals and entities with respect to the Collection, storage, use, Transfer and Destruction of Personal Data.
Privacy Policy	An internal document communicating a set of privacy principles and requirements for the Collection, storage, use, Transfer, and Destruction of Personal Data.
Processing	An operation or a set of operations which is performed upon Personal Data whether by automatic or manual means, such as Collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, Use, Disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or Destruction.
Retention	Storage, archival or warehousing of Personal Data.
Security	The use of Physical, Administrative, and Technical Safeguards to protect Personal Data from loss, misuse, unauthorized Access, Disclosure, alteration and Destruction.
Sensitive Personal Data	A category of Personal Data that requires an extra level of protection or a higher duty of care (i.e. Personal Data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union Membership or information specifying the sexual orientation of an individual).
Storage	The stage in the data life cycle during which Personal Data is stored, whether electronically or in paper format.

Term	Definition
Technical Safeguards	The technology (and the Privacy Policy and procedures for its use) that protects Personal Data and controls Access to it.
Third Party	An Entity that is not an affiliate of IMC, or an individual who is not an employee or acting in the capacity of an individual client of IMC. Third parties may include contractors, service providers, vendors, alliance parties and other nonaffiliated parties. Note that in some circumstances an Entity or individual may be acting in the capacity of an employee and in other circumstances may be acting in the capacity of a Third Party.
Transfer	The release, provision of Access to, or divulging of information outside the Entity holding the information. The term "Transfer" is often used interchangeably with the terms "sharing" and "Disclosure."