IMC GROUP'S POLICY AND PROCEDURES -
COLLECTION AND PROCESSING OF PERSONAL DATA IN LIGHT OF GDPR
March 2018

The European General Data Protection Regulation ("GDPR") will apply as of May 25, 2018. This policy (the "Policy") encompasses rules and guidelines which regulate activities of collecting, transferring, processing and any handling of Personal Data by IMC and its subsidiaries. As such, it should be adopted and implemented by each IMC Member, to secure compliance with GDPR.

TABLE OF CONTENTS

1. Policy:

During ordinary course of business, IMC Members are likely to obtain and handle Personal Data (as defined in this Policy) regarding employees, customers, suppliers, contact persons, online and E-commerce users, as well as other individual third parties.

This Policy sets forth the rules and guidelines which govern all activities in connection with Personal Data. Each IMC member is expected to implement this Policy and to conduct its activities in accordance therewith.

To comply with the GDPR, and as part of this Policy, IMC HQ will:

- Update IMC website's terms of and conditions of use, as well as the privacy policy;
- Draft inter-company agreements to facilitate data transfer and processing between IMC Members;
- Prepare template agreements to facilitate data transfer to entities who provide Personal Data Processing services for IMC Members;
- Periodically review and update this Policy to secure ongoing compliance with GDPR.

1.1. *What is "Personal Data"?*

Any information relating to an identified or identifiable natural person constitutes "Personal Data". This applies only to natural persons, and may include, for example, the persons' -

- name;
- address details (street, postal code and city);
- contact details (e-mail address and phone number);
- identification number (identity card, passport, national security or other personal number);
- location data;
- online identifier (including IP address);
- salary and financial information;
- computer use history;
- religious beliefs;
- medical records;
- images (including pictures and other images captured by surveillance cameras).

1.2. *What is Data Processing?*

Any operation performed on any Personal Data, such as:

- collection and storage (e.g. saving on servers, including e-clouds);
- behavior analysis (including through web cookies, preferences and purchase patterns);
- transfer or allowing access, to third party (e.g. uploading to cloud, reporting to IMC HQ);
- erasure, change or destruction; and
- any other use (such as consultation or retrieval) of Personal Data.

1.3. *How should Personal Data be collected and treated?*

Personal Data can be collected, processed and handled generally ***only if***:

- the purpose for collecting/processing/ handling is lawful and is pre-determined;
- the data-subject is informed of the collection and of the purpose;
- the data-subject is provided with access to data collected about him/her, and, if requested by such data-subject, the Personal Data pertaining to him/her is updated, corrected or (when there is no legal basis for its continued processing) deleted;
- the Personal Data is secured by proper protection against unauthorized use/access.

2. What does each IMC Member need to do when collecting and processing Personal Data?

- *Operate with lawfulness, fairness and transparency*. Personal Data should be processed only lawfully, fairly and in a transparent manner.
    - Examples: Personal Data of employees should be processed only to perform legal obligations. All employees should be properly informed about processing of their Personal Data. An Employee's Personal Data should not be processed for purposes other than the performance of legal employment requirement.

- *Determine the purpose for the processing of Personal Data*.
    - Example: payment of salaries to employees or deduction of salary taxes; suggesting products to a customer and/or facilitating customers' training or use of products.

- *Inform each data subject about collecting and processing his/her Personal Data.*
    - example: use standard contractual provisions; update website's privacy statement.
    - Each data subject should be informed of:
        - The identity and contact details of the specific IMC Member who possesses, handles and processes his/her Personal Data;
        - The contact details of the data protection officer of the relevant IMC Member, where applicable;
        - The purpose(s) of processing its Personal Data;
        - The legal basis for processing its Personal Data, such as performance of a contract, or the data-subject's consent (please refer to paragraph 3 of this Policy);
        - The categories of recipients of the Personal Data, such as other IMC Members, IMC shareholders, subcontractors, suppliers, supervisory, tax or other governmental authorities;
        - If applicable, the transfer of its Personal Data to countries outside the European Economic Area (including transfers to Israel, Asia and the USA);
        - The period for which the Personal Data is stored;
        - Its rights under the GDPR, such as the data subject's right to request access to, rectification, erasure or portability of its Personal Data;
        - The possibility to withdraw its consent, where handling or processing of Personal Data is based on the data-subject's consent;
        - The right to lodge a complaint with a supervisory authority;
        - The existence of automatic decision making, including profiling (for example, e-recruiting without human intervention), if applicable.

- *Maintain a Personal Data Registry.*
    - Such registry should include all relevant information regarding all Personal Data that is being handled or possessed, as well as all processing activities and the purposes thereof.

- *Collect and process only such portion of Personal Data that is required to achieve the purpose.*
    - Example: no data of employee internet use is required for payment of salaries to employees.
- *Conduct periodic review the scope of Personal Data collected, update it and erase data no longer required for the collection purpose.*
    - Example: if a customer's contact person no longer works for such customer, his contact details are no longer required and should be erased.

- *Ensure proper protection and security measures against unauthorized access, use or destruction.*
    - Example: secure data by password, limit access on a need-to-know basis and require identification. Use all protection protocols adopted and recommended by IMC's IT department, alongside a secured access to all locations and files containing Personal Data.

- *Allow data-subject access to his/her Personal Data upon request, and erase or update it if requested*, notwithstanding other rights of data subjects under GDPR (for example, the right to data portability or to object to processing of his/her Personal Data), but as long as retaining such Personal Data is not required under another legal basis.

- Whenever a data subject's request to erase personal data is received, if it is practically impossible to erase it from back-up files, then the relevant IMC Member shall: (i) record which personal data was required to be deleted; and (ii) delete such personal data in all cases where such data is restored from back-up files, without making or allowing any use thereof.

- *Conduct periodic training regarding this Policy and the obligations under GDPR.*

- *Perform Data Protection Impact Assessments ("DPIAs")*;
    - Example: if an IMC Member intends to introduce tracing devices to track employees or customers' usage, it should first conduct a DPIA to assess the impact and privacy risks for all concerned, with particular review of such introductions' compliance with the GDPR.
    - Record and properly document all DPIA activities.

- *Notify Personal Data breaches to the Supervisory Authority*;
    - Example: an unsecured laptop which contains a list of names and salary details of employees is stolen. Such an incident constitutes a Personal Data breach and is required is to be notified with the Supervisory Authority and the involved employees.

- *Conclude or update Data Processing Agreements*;
    - When an IMC Member engages a third party for provision of services (such as hosting or payrolling services), such third party may process Personal Data on behalf of such IMC Member as a 'Data Processor'. In such event, a data processor agreement should be concluded between the IMC Member and that third party in which arrangements are made to regulate and safeguard processing of Personal Data in accordance with this Policy.
    - Each IMC Member should advise IMC HQ regarding all third parties with whom it is engaged for any Personal Data processing and/or hosting services. Data Processing Agreements will be provided by IMC's legal department as needed.

- *Apply retention periods for Processed Personal Data*:
    - If a candidate applies for a job and the candidate is not hired, the Personal Data of this candidate are generally to be deleted within four (4) weeks after termination of the job application procedure (unless a candidate would consent to a longer retention period).

- *Apply the principles 'privacy by design' and 'privacy by default'*. This means that data protection principles should be taken into account when developing new products, services or processes which involve processing of Personal Data, both in the initial design stage and throughout the development process. In addition, default settings for these new products, services or processes should be 'privacy friendly'.

- *Accountability*. Maintain proper documenting of all actions taken with respect to processing Personal Data in accordance with this Policy, to ensure ongoing compliance with the GDPR and to demonstrate such compliance and measures taken o secure it, whenever needed.

3. Legal Basis for Data Processing

Personal Data may only be processed on the basis of one or more of the following six (6) legal grounds:

a) *Consent*: the data subject has given consent for the processing of his or her personal data, for one or more specific purposes; consent means a freely-given, specific, informed and unambiguous indication of the data-subject's wish, by which he/ she signifies agreement to the processing of personal data relating to him/her.

b) *Performance of contract*: processing is necessary to perform a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;

c) *Legal obligation*: processing is necessary to comply with a legal obligation to which controller is subject;

d) *Vital interests*: processing is necessary to protect vital interests of the data subject or of another natural person;

e) *Task in the public interest:* processing is necessary to perform a task carried out in the public interest, or in to exercise an official authority vested with the controller;

f) *Legitimate interest*: processing is necessary to maintain/safeguard legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data-subject which require protection of personal data, in particular where the data subject is a child.

Please Note:

A. IMC Members should generally process Personal Data only for the performance of a contract (set out above under (b)), or to comply with legal obligations (set out above under (c)), or if the processing serves the legitimate interest of the IMC Member (set out above under (f)).

B. Consent (as set out above under (a)) can be used as a legal basis for processing Personal Data only if the processing of Personal Data cannot be based on any of these legal bases.

C. If consent is used as a legal basis, paragraph 4 below must be strictly adhered to.

D. Any handling or processing of Personal Data which is not based on any of the legal grounds set out above is not permitted.

4. Guidelines to Obtain Consent

Consent must be: freely given, specific, informed and unambiguous. For that:

- Request for consent should be in plain language, and easily distinguishable.
    - Example: use **bold** font for the consent provision in agreement or in website's terms and conditions.
- Data subject shall be able to easily withdraw consent at any time. This should be specified in the consent form.
- Do not condition provision of services or sale on grant of consent.
- Document consent forms. If consent is given by a data subject, such consent must be documented to demonstrate compliance with the GDPR.

Each IMC Member shall ensure obtaining consent for data processing from each data subject when needed pursuant to Section 3 above.

- A template consent form is attached to this Policy as **Annex A**.

5. Guidelines for Personal Data Protection

Use adequate protection measures to secure unauthorized access to, or use of, Personal Data, such as:

- Physical files and computer systems in which Personal Data is stored, should be secured in a locked room/cabinet. Access should be restricted only to those having a need-to-know and registered to ensure monitoring of all authorized personal.
- Personal Data stored in, or accessible by, IT systems should be stored in secured files, protected by passwords, access to which must be restricted only to personnel authorized by management.

IMC HQ may from time to time issue instructions regarding security measures to be implemented. In addition, protective measures should be periodically reviewed and updated to protect against new threats.

In any event of suspected or actual data breach (e.g. unauthorized access, erasure, destruction or encryption of Personal Data), IMC HQ should be notified immediately. Additional actions and reporting will be made in coordination with IMC HQ.

6. Guidelines for transfer of Personal Data

Each commercial engagement which includes Data Processing by third parties (for example – payroll services) and/or involve transferring Personal Data or granting access to Personal Data, must be in writing and should include standard GDPR compliance provisions or otherwise reviewed and approved by IMC legal department in advance, to facilitate assessment of roles of the parties under the GDPR (such as controller, processor or joint controller) and thereby determine whether it is required to conclude a:

- Data Processing Agreement;
- Controller to Controller Agreement;
- Joint Controller Agreement.

Transfer of Personal Data to a third party (including other IMC Members) is permitted only if:

- It is required for the purpose for which Personal Data was collected.
- Data subject was informed of the transfer.
- A written agreement is in place between transferor and transferee, in a form approved by IMC legal department.
- If transfer is made to a territory outside of which it was collected, then if such other territory is -
    - Within the European Economic Area ("EEA") – no additional measures are required;
    - To Israel – no additional measures are required (as long as Israel is recognized as a country that offers an adequate level of data protection);
    - To the USA – should be made under "Privacy Shield" terms (to be provided by IMC HQ on an as-needed basis);
    - To any other country/territory that is not recognized as a country which offers adequate level of data protection – should be made under standard model clauses, with the prior review of IMC legal department.

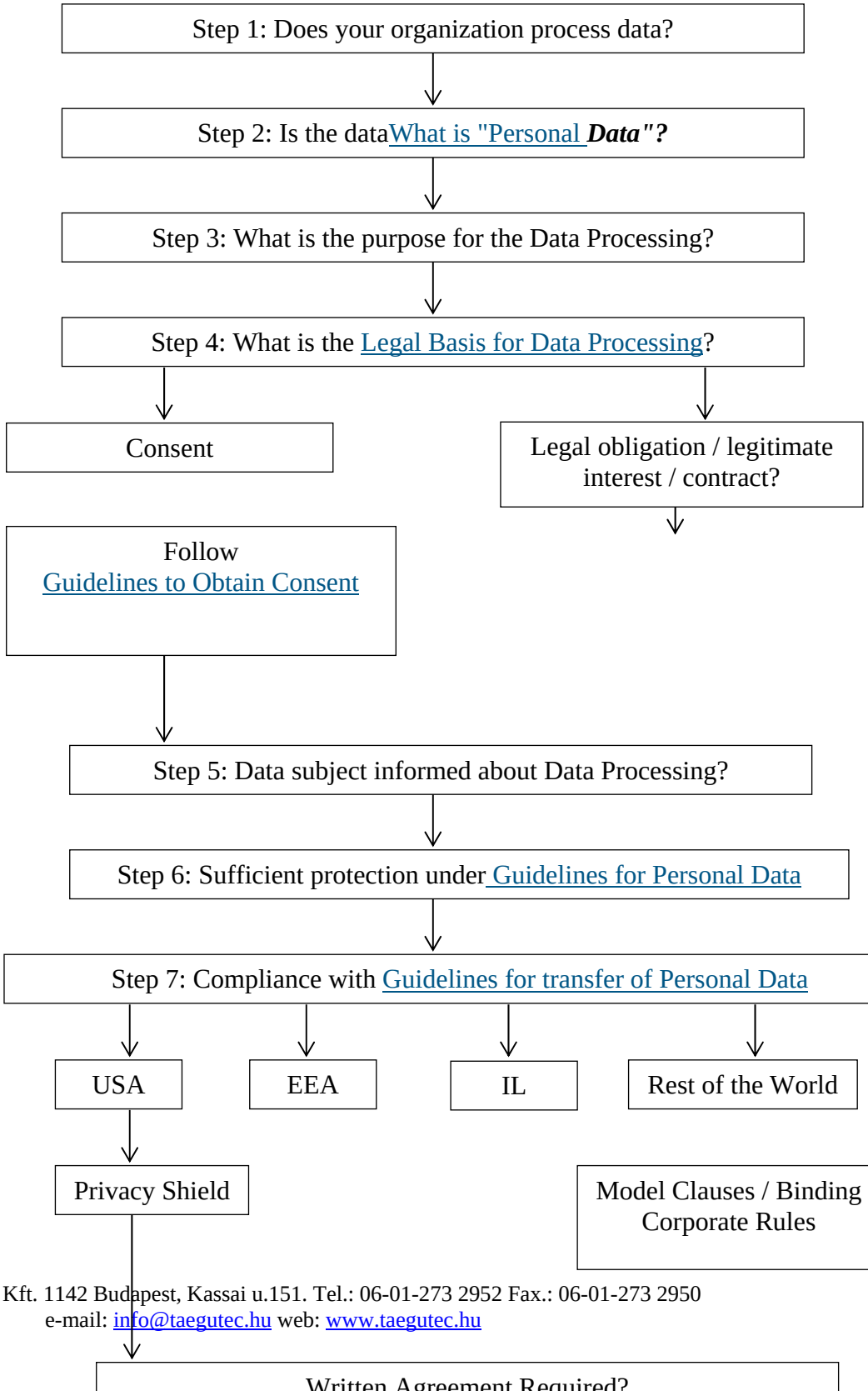
7. Implementation & Responsibility:

Each IMC subsidiary and branch manager should ensure implementation of this Policy before the GDPR effective date (May 25, 2018).

IMC legal department will take care of drafting and adopting required corporate resolutions to adopt this Policy amongst all IMC Members.

All provisions of this Policy should be adhered to and continuously applied by all IMC Members.

Checklist: Lawful Processing of Private Data



TaeguTec Hungary Kft. 1142 Budapest, Kassai u.151. Tel.: 06-01-273 2952 Fax.: 06-01-273 2950
e-mail: info@taegutec.hu web: www.taegutec.hu