

Privacy Policy of imc AG



Content

Privacy Policy	4
§ 1 Intention, purpose, accessibility	4
§ 2 Scope of application	4
§ 3 Definitions	5
§ 4 Data protection organisation	7
§ 5 Handling of personal data	8
§ 6 Special categories of personal data	11
§ 7 Data transmission	11
§ 8 External service providers	12
§ 9 Data minimisation, Privacy by Design/Privacy by Default	13
§ 10 Rights of data subjects	13
§ 11 Third party requests for information on data subjects	16
§ 12 Record of processing activities	16
§ 13 Advertising	17
§ 14 Training	17
§ 15 Data secrecy	17
§ 16 Complaints	18
§ 17 Audits	18
§ 18 Internal investigations	19
§ 19 Availability, confidentiality and integrity of data	19
§ 20 Data protection impact assessment	21
§ 21 Data breaches	22
§ 22 Consequences of infringements	22
§ 23 Accountability	23
§ 24 Updating of the policy; accountability	23

imc
information multimedia communication AG
 Hauptsitz Saarbrücken
 Scheer Tower, Uni-Campus Nord
 D-66123 Saarbrücken
 T. +49 681 9476-0 | Fax -530
 info@im-c.com
 www.im-c.com

Privacy Policy

§ 1 Intention, purpose, accessibility

(1) This policy is the binding foundation for a legally compliant and sustainable protection of personal data at imc AG and all its affiliated companies.

(2) The purpose of this Corporate policy is to safeguard and protect the fundamental rights and freedoms of data subjects, in particular their right to the protection of personal data.

(3) This policy must be easily accessible to all employees and managers at all times.

§ 2 Scope of application

(1) This policy applies to imc AG and all its affiliated subsidiaries domiciled in the European Union.

(2) This policy also applies to all subsidiary companies affiliated with imc AG - regardless of the respective domicile of the subsidiary - in the context of the processing of personal data of data subjects residing in the European Union.

(3) It applies personally to all employees and executives of the company.

(4) The rules and restrictions of this Corporate policy apply to all handling of personal data, whether electronic or paper. They also include all types of data subjects (customers, employees, suppliers, etc.) in their scope of application.

§ 3 Definitions

(1) **Personal data** means any information relating to an identified or identifiable individual (data subject). Customer data is just as much a part of personal data as personal data of employees. For example, the name of a contact person can be traced back to a natural person in the same way as his or her e-mail address. It is sufficient if the respective information is linked to the name of the data subject or can be determined independently of this from the context. A person may also be identifiable if the information must first be linked to additional knowledge, e.g. with a license plate. The origin of the information is irrelevant for a personal reference. Photos, video or sound recordings can also represent personal data.

(2) **Special categories of personal data** are information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data relating to the sex life or sexual orientation of a natural person.

(3) **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by

transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(4) **Restriction of processing** is the tagging of stored personal data with the aim of limiting their future processing.

(5) **Profiling** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

(6) **Pseudonymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

(7) **Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

(8) **Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

(9) **Recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

(10) **Third party** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

(11) **Consent of the data subject** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

§ 4 Data protection organisation

(1) imc AG (Germany) has appointed a Data Protection Officer. You can reach him under the following contact data:

Florian Caspar

datenschutz@im-c.de / florian.caspar@im-c.de

Phone +49 681 9476-301,

Uni-Campus Nord | 66123 Saarbrücken | Office 5.22

(2) The Data Protection Officer shall monitor compliance with data protection requirements, including the stipulations of this and other company policies on data protection. The Data Protection Officer advises

and informs the company management regarding existing data protection obligations and is responsible for communication with supervisory authorities. Selected processes are randomly, risk-oriented and checked by him at appropriate intervals to ensure that they comply with data protection requirements.

(3) The Data Protection Officer shall carry out his tasks in an independent manner and by applying his expertise. In his function, the Data Protection Officer reports directly to the Executive Board and has a direct right of proposal.

(4) The Data Protection Officer is fully supported by all employees in the performance of his duties and is involved in all data protection issues at an early stage.

(5) In addition, imc AG has a security team consisting of Roman Muth (IT security officer) and Florian Caspar (Data Protection Officer). The security team regularly meets to discuss current topics in the field of data protection and information security and pushes data protection management within the company.

§ 5 Handling of personal data

(1) The processing of personal data is generally forbidden, unless a legal norm explicitly permits the handling of data. According to the GDPR, personal data may in principle be processed:

- In the case of an existing contractual relationship with the person concerned.

Example: The storage and use of necessary personal data within the framework of a service contract.

- In the context of pre-contractual activities at the request of the data subject and the execution of the contract with the data subject.

Example: Customer K requests information on product X and acquires it. The data required for sending the information material and for processing the legal transaction (delivery of the goods and payment of the purchase price) may be processed.

- If and to the extent that the person concerned has consented.

Example: The data subject registers to receive a newsletter.

- When there is a legal obligation to which the entity is subject.

Example: Legal retention periods according to the German Commercial Code (HGB) and the Fiscal Code (AO).

- If there are legitimate interests of the company, unless the interests or fundamental rights of the data subject prevail, in particular if the data subject is a child. However, data processing operations based on a legitimate interest should not be carried out without prior consultation with the Data Protection Officer.

Example: The use of the postal address for sending advertising letters.

(2) Data subjects shall not be subject to a decision based solely on automated processing, including profiling, which has legal effects or affects them significantly in a similar manner.

(3) Personal data shall be processed for a predetermined, explicit and legitimate purpose. A storage of data without purpose, for example the storage of data on stock, is not allowed.

(4) If possible, the use of personal data should be avoided. Pseudonyms or anonymous data processings should be preferred.

(5) The change of a goal and purpose, which were originally taken as a basis for data handling, is - apart from the declared consent by the data subject - only permitted if the purpose of the further processing is compatible with the original purpose. In particular, the data subject's reasonable expectations of the company with regard to such further processing, the type of data used, the consequences for the data subject as well as the possibility of encryption or pseudonymisation must be taken into account.

(6) When collecting his personal data, the data subject must be comprehensively informed about the handling of his data. The information must contain the purpose, the identity of the responsible body, the recipients of his personal data and all other information within the meaning of Art. 13 GDPR in order to ensure fair and transparent processing. The information must be written in an understandable and easily accessible form and in as simple a language as possible.

(7) If personal data is not obtained from the data subject but, for example, obtained from another company, the data subject must be informed subsequently and comprehensively about the handling of his data in accordance with Art. 14 GDPR. This also applies to changes to the purpose and purpose of data processing.

(8) Personal data must be accurate and, if necessary, up to date. The extent of data processing should be necessary and relevant for the purpose for which it is intended. The respective specialist department must ensure that this is carried out by establishing appropriate processes. Likewise, databases must be regularly checked for their correctness, necessity and up-to-dateness.

§ 6 Special categories of personal data

Special categories of personal data may in general only be collected, processed or used with the consent of the data subject or exceptionally on the basis of explicit legal permission. Furthermore, additional technical and organisational measures (e.g. encryption during transport, minimum allocation of rights) must be taken to protect special categories of personal data.

§ 7 Data transmission

(1) The transfer of personal data to third parties is only permitted on the grounds of a legal basis of permission or the consent of the data subject.

(2) If the recipient of personal data is located outside the European Union or the European Economic Area, special measures are required to safeguard the rights and interests of data subjects. Data shall not be transmitted if the receiving party does not have an adequate level of data protection or if, for example, special contractual clauses cannot be used to establish it.

§ 8 External service providers

(1) If external service providers shall have access to personal data, the Data Protection Officer shall be informed in advance.

(2) Service providers with possible access to personal data shall be carefully selected before commissioning. The selection shall be documented and should take particular account of the following aspects:

- Technical suitability of the contractor for the concrete handling of data
- Technical and organisational security measures
- Supplier's experience in the market
- Other aspects that indicate the reliability of the provider (data protection documentation, willingness to cooperate, reaction times, etc.)

(3) If a service provider shall be commissioned to collect, process or use personal data, a contract for commissioned processing must be concluded. In this contract data protection and IT security aspects shall be regulated.

(4) The service provider shall be regularly reviewed with regard to the technical and organisational measures contractually agreed with him. The result shall be documented.

§ 9 Data minimisation, Privacy by Design/Privacy by Default

(1) The handling of personal data shall be guided by the objective of collecting, processing or using as little data as possible from a data subject ('data minimisation'). In particular, personal data shall be anonymised or pseudonymised, as far as this is possible according to the purpose of use. For example, it will not be necessary to know and use the full name of a data subject in the context of a statistical evaluation of data. Rather, this information can be replaced by a random value, which can also ensure that the underlying information is distinguishable.

(2) The same applies to the selection and design of data processing systems. Data protection shall be integrated from the outset into the specifications and architecture of data processing systems in order to facilitate compliance with the principles of privacy and data protection, in particular the principle of data minimisation.

§ 10 Rights of data subjects

(1) Data subjects have the right to information about the personal data stored in the company about their person.

(2) When processing requests, the identity of the data subject must be established beyond doubt. If there are justified doubts as to the identity, additional information may be requested from the requester.

(3) Information shall be provided in writing unless the data subject has submitted the request for information electronically. The information must be accompanied by a copy of the data subject's data which, in addition to the personal data available, also contains the recipients of the data, the purpose of the storage and all other information required by law pursuant to Art. 15 GDPR in order to make the data subject aware of the processing and to have the lawfulness itself assessed. At the special request of the data subject, the data will be made available in a structured, common and machine-readable format. The responsible IT department determines the standard to be provided for this purpose.

(4) Data subjects are entitled to have their personal data corrected if they prove to be inaccurate. They may also request the completion of incomplete personal data.

(5) The data subject has the right to have his/her personal data deleted under the following conditions:

- The knowledge of the data is no longer necessary for the fulfilment of the purpose of storage, or
- the data subject has withdrawn his consent and no other legal basis for the processing exists, or
- the processing is not permitted, or

- the data subject objects to the processing for advertising purposes or invokes a right of objection based on a particular personal situation which must be justified, or
- It concerns special personal data, whose correctness cannot be proven, or
- there is another legal obligation to delete data.

If there is an obligation to delete and the personal data has been made public in advance, further controllers must be informed of the data subject's request to delete all copies of his data and all links to this data.

(6) The data subject may request that the processing of his data be restricted if,

- the accuracy of the personal data is disputed, but only for as long as the accuracy is verified by the company
- the processing is inadmissible but the data subject refuses to delete the data, or
- the company no longer needs the personal data for processing purposes, but the data subject needs the data for the assertion, exercise or defence of legal claims, or
- the data subject has filed an opposition against the processing on the basis of a particular situation and the competent department is still examining the opposition.

(7) The data subject shall be informed, within one month at the latest, of any measures taken at his request.

(8) The data subject's rights shall be fulfilled in accordance with the binding process (available here jira.im-c.de/confluence/display/LEG/) laid down for this purpose. In addition, the Data Protection Officer shall provide advice.

§ 11 Third party requests for information on data subjects

Where an entity requests information about data subjects, such as customers or employees of that company, information may only be disclosed if

- the providing authority can demonstrate a legitimate interest in this, and
- a legal norm is obligated to provide information, and
- the identity of the requesting party or body is established beyond reasonable doubt.

§ 12 Record of processing activities

(1) The company shall keep a record of all data processing operations. Each department shall designate a responsible person to document all necessary information on the procedures of the respective department in accordance with the legal requirements of Art. 30 GDPR. The Data Protection Officer may be called in to advise on the information required by law.

(2) The individual lists of the various specialist departments shall be handed over to the Data Protection Officer. The Data Protection Officer shall consolidate the individual directories of the specialist departments and administer them centrally.

(3) The company shall make the records available to the supervisory authority on request. The Data Protection Officer shall be responsible for this in agreement with the management of the company.

§ 13 Advertising

(1) The contact of data subjects by letter, telephone, fax or e-mail is only permitted if the data subject has previously consented to the use of his data for advertising purposes.

(2) Exceptions shall only be permitted in the case of the existence of a permission regulation. Please consult the Data Protection Officer in this regard.

§ 14 Training

Employees who have permanent or regular access to personal data, who collect such data or who develop systems for processing such data shall receive appropriate training on data protection regulations. The Data Protection Officer shall decide on the format and frequency of the corresponding training courses.

§ 15 Data secrecy

(1) Employees shall not collect, process or use personal data without authorisation. They shall be obliged to treat personal data confidentially

before taking up their duties. The obligation is made by the Human Resources Department using the form provided for this purpose.

(2) Employees with special confidentiality obligations (e.g. telecommunications secrecy pursuant to § 88 TKG) shall be additionally obligated in writing by the company management.

§ 16 Complaints

(1) Every data subject has the right to complain about the processing of his/her data should he/she feel that his/her rights have been violated as a result. Employees may also report violations of this Corporate policy at any time.

(2) The competent authority for the above complaints is the Data Protection Officer as an internal, independent and non-directed body.

§ 17 Audits

(1) In order to ensure a high level of data protection, relevant processes shall be subject to regular audits by internal bodies or external auditors. If a potential for improvement is identified, immediate remedial action shall be taken.

(2) The findings of the audit shall be documented. The documentation shall be handed over to the Data Protection Officer, the company management and the persons responsible for the respective process.

(3) An audit is successfully completed when all measures documented in the report have been implemented. If required, follow-up audits shall be carried out by reviewing the implementation of recommendations of the initial audit.

§ 18 Internal investigations

(1) Measures to clarify and prevent or detect criminal offences or serious breaches of obligations in the employment relationship shall be implemented in strict compliance with the relevant statutory provisions on data protection. In particular, the associated collection and use of data must be necessary to achieve the purpose of the investigation, appropriate and proportionate to the legitimate interests of the data subject.

(2) The data subject shall be informed as soon as possible about the measures taken with regard to his person.

(3) In all forms of internal investigations, the Data Protection Officer shall be involved in advance with regard to the selection and design of the measures.

§ 19 Availability, confidentiality and integrity of data

(1) Depending on the type, scope, circumstances and purposes of the processing and the probability of occurrence, a documented determination of the need for protection and an analysis of the risks to the data subjects shall be made for each procedure.

(2) In order to ensure the availability, confidentiality and integrity of data, a general security concept shall be drawn up depending on the determination of the need for protection and the risk analysis, which shall be binding for all procedures. In particular, the state of the art shall be taken into account as well as means and measures for encryption and data security. The security concept shall be regularly reviewed, evaluated and evaluated with regard to the effectiveness of the technical and organizational measures provided for therein.

(3) It shall be ensured that data processing systems cannot be used by unauthorised persons. Doors of unoccupied rooms shall be locked. Effective measures for access control to equipment shall be in place and activated. System access shall always be blocked in the absence.

(4) Passwords enable access to systems and the personal data stored therein. They represent a personal identification of the user and are not transferable. It must be ensured that passwords are always kept under lock and key. Passwords must have a minimum length of ten characters and consist of a mix of characters. Passwords must not appear in a dictionary or be formed from terms that are easy to guess, in particular terms that are related to the company.

(5) Access to personal data shall only be granted to those persons who need to gain knowledge of the respective data in the course of performing their

duties ("need-to-know principle"). Access authorisations must be precisely and completely defined and documented.

(6) Data transmissions through public networks shall be encrypted wherever possible. Encryption shall be mandatory if the need to protect personal data so requires.

(7) Personal data collected for different purposes shall be processed separately. The separation of data shall be ensured by appropriate technical and organisational measures.

(8) Maintenance work on systems or telecommunications equipment by external service providers shall be supervised. Furthermore, it shall be ensured that service providers cannot access personal data without authorization. Remote maintenance access shall only be granted in individual cases and must follow the principle of minimum rights allocation. If possible, remote maintenance activities must be recorded or logged.

§ 20 Data protection impact assessment

(1) Each department is obliged to carry out data protection impact assessments for procedures carried out under its responsibility if a high risk for rights and freedoms of data subjects is to be expected due to data processing. The data protection impact assessment contains all legally required descriptions of Art. 35 para. 7 GDPR.

(2) The Data Protection Officer shall advise the departments concerned on the performance of the data protection impact assessment and on the question of when processing operations may involve a high risk for data subjects.

§ 21 Data breaches

(1) Should personal data have been unlawfully disclosed to third parties, the security team must be informed immediately in compliance with the process provided for this purpose (available here jira.imc.de/confluence/display/LEG/).

(2) The notification shall contain all relevant information necessary to clarify the facts, in particular the receiving party, the persons concerned and the nature and extent of the data transmitted.

(3) Any duty to provide information to the supervisory authority shall be fulfilled exclusively by the Data Protection Officer. Data subjects shall be informed by the management, whereby the Data Protection Officer shall be consulted in an advisory capacity.

§ 22 Consequences of infringements

A careless or even intentional infringement of this policy may give rise to measures under labour law, including dismissal without notice or within the prescribed period. Criminal sanctions and other consequences, such as compensation for damages, may also be considered.

§ 23 Accountability

Compliance with the requirements of this policy must be demonstrated at all times. Particular attention must be paid to the traceability and transparency of the measures taken, for example in the form of associated documentation.

§ 24 Updating of the policy; accountability

(1) This policy shall be regularly reviewed in the light of developments in data protection law and technological or organisational changes with a view to adapting or supplementing it.

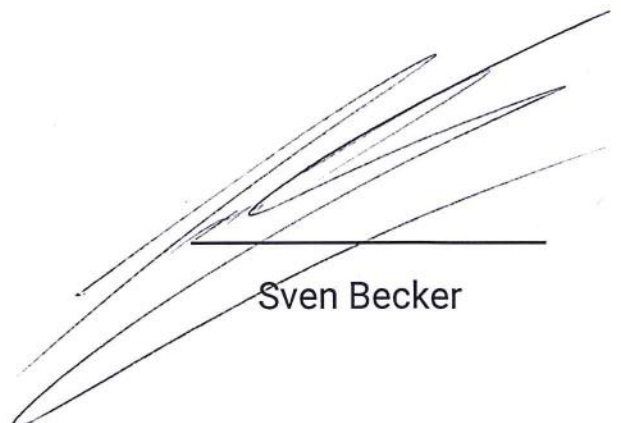
(2) Amendments to this policy shall take effect informally. Employees and executives shall be informed immediately and in an appropriate manner of the changed requirements.

Saarbrücken, January 18, 2019

Executive Board of imc information multimedia communication AG



Christian Wachter (CEO)



Sven Becker