

I. OBJECTIVES

Inoweiser's objective is to apply adequate global data protection and privacy standards of our stakeholders' personal information.

II SCOPE

All companies of Inoweiser ecosystem follow our corporate rules. They are corporate guidelines that apply to the processing of User Information, which means any information relating to an identifiable User. An identifiable User is an individual who can be identified, directly or indirectly, based upon the information collected about the individual in the context of a service provided by Inoweiser. The term Service applies to the website or other product/service offered by us for use by a User. In this context "Users" refers to employees, customers, providers and any other stakeholder.

Inoweiser does not knowingly process User Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or concerning health, sexual life or criminal records (Sensitive Information). To the extent Sensitive Information is manifestly made public by the User him/herself and provided to us, we do not process it for our own purposes.

III. APPLICATIONS OF LAW

Inoweiser will comply with applicable laws that may impose a stricter standard than those set forth in these Corporate Rules. Collection and processing of User Information shall occur in accordance with the Service's term and conditions, the law applicable to the User and the guidelines established by these Corporate Rules. Where applicable law is more protective than the guidelines set forth by the Corporate Rules, Inoweiser will process User Information in accordance with the applicable law. If applicable law provides for a lower level of protection, the guidelines of the Corporate Rules shall apply. The Corporate Rules are binding obligations and failure to follow them may result in employee corrective action, including termination and other penalties as provided by law.

Where an Inoweiser Entity has reason to believe that applicable law may prevent compliance with the Corporate Rules resulting in a substantial effect on the protections provided by the Corporate Rules, the Inoweiser Entity will promptly inform the privacy team, which will, in turn, inform the relevant data protection authorities (except where prohibited by law enforcement or other government official).

Where there are multiple interpretations of the commitments, terms or definitions made in these Corporate Rules, Inoweiser Entities shall interpret the Corporate Rules in a way that is most consistent with the basic concepts of the principles of EU Directive 95/46/EC.

IV. PRINCIPLES FOR PROCESSING PERSONAL INFORMATION

Personal Information Processing means any operation or set of operations, which is performed upon User Information, whether or not by automatic means. In our process for user information, we follow these principles:

- Process User Information fairly and lawfully;

DATA PROTECTION CORPORATE RULES

- Provide notice to Users about the processing of their personal information and their rights;
- Collect User Information for specified, legitimate purposes
- Maintain User Information in adequate and relevant ways,
- Keep User Information accurate and up-to-date as reasonably possible;
- Process User Information in a way that is relevant and not excessive for the purposes which they are collected and used;
- Store User Information for as long as necessary for the Services;
- Protect User Information with appropriate physical, technical and organizational security measures to prevent unauthorized access, unlawful processing and unauthorized or accidental loss, destruction and damage.

V. PURPOSES FOR PROCESSING USER INFORMATION

Our team must follow must provide a privacy policy and disclose the nature and type of User Information processed and transferred. Generally, we process User Information to facilitate the Services Users request, resolve disputes, troubleshoot problems, process transactions, collect fees owed, inform Users about offers and updates, detect and protect Inoweiser against error, fraud and other criminal activity, enforce the Service's terms and conditions and as otherwise described to Users at the time of collection.

When User Information is transfer to a Data Processor, the Service's privacy policy must describe the processing performed by the Data Processor and the nature and type of Data Processors. Processing of User Information is limited to the purposes and conditions described above, the disclosures made in the Service's privacy policy and the directions of the Data Controller. Further processing in a way incompatible with those purposes will not take place unless a User is notified and consent is received according to applicable law.

The Services' privacy policy shall be accessible via a link in a prominent location of each Service and/or displayed during registration provides additional details according to applicable law regarding the collection, processing, protection and transfer of User Information.

VI. SECURITY, CONFIDENTIALITY AND PRIVACY AWARENESS TRAINING

Inoweiser uses physical, technical and organizational security controls proportionate with the amount and sensitivity of the User Information to prevent unauthorized access, use, loss, destruction and damage. Our entities use encryption, firewalls, access controls, standards and other procedures to protect User Information from unauthorized access. Physical and logical access to electronic and hard copy files is further restricted based upon job responsibilities and business needs.

We conduct privacy and information security awareness training to emphasize and inform employees of the need to protect and secure User Information. Access to User Information shall determine the need for additional training relating to specific policies as well as these Corporate Rules. Employees are also required to review the Company Confidentiality Agreement and these Corporate Rules.

The failure to comply with these policies may result in disciplinary actions. A copy of these Corporate Rules and other relevant privacy and security related policies and procedures are available to employees at any time.

VII. USER CHOICES

Inoweiser will strive to provide Users with the opportunity to review, access and rectify their own User Information using direct contact or the appropriate online tool or self-service process as is described on the Service's website they visited, when available. In all cases, Users have the right to submit a data subject access request to view User Information not accessible via the Service's website.

We will comply with reasonable requests in a commercially reasonable period so long as it does not require a disproportionate effort to retrieve and where applicable law requires access. In these instances, Users may be required to provide proof of their identity and may be subject to a servicing fee as permitted by applicable law.

VIII. TRANSFERRING AND SHARING USER INFORMATION

Inoweiser shares User Information in the normal course and scope of business with other companies of our ecosystem to facilitate the Services Users request, prevent fraud, provide joint content and Services and as described in the Services Privacy Policy or at the time of collection. We may transfer User Information to other Inoweiser company worldwide under the authority and only on the instructions of the Data Controller when there is a legitimate business need, sufficient technical and organizational security measures exist and the recipient has complied with the Corporate Rules or provides an adequate level of protection when processing User Information (for instance by entering into contracts based on the model clauses for the transfer of EU User Information to processors or controllers established in third countries published by the European Commission).

We may share User Information with third party processors (such as service providers or vendors) worldwide who help with their business operations. The Service's Privacy Policy further describes the types of third parties Inoweiser may share User Information with and under what circumstances. Contracts with third party processors require sufficient technical and organizational security measures, limit the use of User Information to purposes defined by the Data Controller and retain control of User Information where applicable. Additionally, Inoweiser will only transfer User Information of Users located in the EU to third party processors that provide an adequate level of protection when processing User Information (for instance by entering into contracts based on the model clauses for the transfer of EU User Information to processors established in third countries published by the European Commission). Agreements with third party processors provide for legal remedies in the event of a breach of the agreement.

IX. LIABILITY AND THIRD PARTY BENEFICIARY RIGHTS

Inoweiser will comply with these Corporate Rules. The Corporate Rules are binding obligations and failure to follow them may result in employee corrective action, including termination and other penalties as provided by law.

If an EU User suspects a breach of the Corporate Rules based upon User Information transferred from the EU to an entity located outside of the EU, the User should report his/her concern to the Data Controller's customer support via email, the Service's website, or as otherwise indicated in the Service's terms and conditions. The Data Controller will investigate claims of non-compliance to determine if a violation of the Corporate Rules has occurred. If the violation is confirmed, the Data Controller and Inoweiser shall work together to address and resolve the violation within a commercially reasonable time.

EU Users that suspect a breach of the Corporate Rules have the right to claim enforcement of the Corporate Rules or liability as third party beneficiaries for the following sections of the Corporate Rules: III, IV, V, VI, VII, VIII, IX, X, XI and XIV and, where appropriate compensation from the exporting Data Controller in the EU or its EU Headquarters (as defined in the Service's terms and conditions) before the relevant data protection authority or courts in accordance with the terms set up in the Corporate Rules and applicable law. While it is not required, an EU User should first report his/her concern directly to the Data Controller rather than the data protection authorities or the courts. This enables an efficient and prompt response from the Data Controller and minimizes possible delays from data protection authorities or court procedures. The exporting Data Controller and its EU headquarters shall not be liable if they reasonably demonstrate that the non-EU Entity has not violated the Corporate Rules or is not responsible for the act resulting in the damage claimed by the EU User.

According to applicable law, treaties or applicable international conventions, Inoweiser may share User Information with law enforcement, regulatory authorities or other third parties when: required as a matter of law; it is necessary to protect Inoweiser rights; it is necessary to keep the Services free from abuse; or there is a legitimate purpose.

We may disclose User Information to other third parties for the third party's own purposes in accordance with the User's instructions or with the unambiguous informed consent of the User (where permissible under applicable law).

X. AUDIT PROCEDURES

Inoweiser privacy team reviews, on a regular basis, User Information processing activities and practices or recommends that our internal audit team conduct a review of the identified activities and practices. The internal audit team and the Inoweiser privacy team shall, if necessary, require an action plan to ensure compliance with the Corporate Rules. To the extent that internal groups do not resolve matters adequately, we may appoint independent external auditors for further resolution.

Inoweiser privacy team shall review and address matters relating to non-compliance with the Corporate Rules identified in the course of a review or upon notice by an our entity, User, employee or other individual. Audit findings are available to relevant data protection authorities upon request. We will redact portions of the audit to ensure confidentiality of proprietary or otherwise company confidential information. Further, we will only provide audit findings relating to privacy.

XI. MODIFICATIONS TO THE CORPORATE RULES

Inoweiser reserves the right to modify the Corporate Rules as necessary, for example, to comply with changes in laws, regulations, our practices, procedures and organizational structure or requirements imposed by data protection authorities.

Our privacy team must approve all changes to the Corporate Rules and shall track all modifications to the Corporate Rules. Inoweiser shall report to the relevant data protection authorities' changes to the Corporate Rules where approval is required or at least on an annual basis.

We will provide notice of material changes to Users in accordance with their Service preferences and/or shall post the revised Corporate Rules on select external websites accessible by Users. Revisions to the Corporate Rules are effective within a reasonable period after we notifies the User and/or posts the revised Corporate Rules

XII. OBLIGATIONS TOWARD DATA PROTECTION AUTHORITIES

Inoweiser will respond diligently and appropriately to requests from data protection authorities about the Corporate Rules and their compliance with privacy laws and regulations. If an employee receives such a request from a data protection authority, he or she should immediately inform the legal department so that Inoweiser can provide the data protection authorities with names and contact details of relevant contact persons who will reply to the data protection authority.

For further clarification on the conditions of use:

E-mail: mypersonalinfo@inoweiser.com