isonike

Privacy and Personal Data Protection Policy

Privacy and Personal Data Protection Policy

Classification: Public [1]

[1] *This document is classified as Public. Read only use outside ISONIKE is allowed. Copy in any form is strictly prohibited*

Privacy and Personal Data Protection Policy

0.Table of Contents

0. Table of Contents.....2
1. Preamble.....3
2. Principles.....3
3. Rights of the Individuals.....4
4. Policy.....5

Privacy and Personal Data Protection Policy

1. Preamble

a. The purpose of this document is to communicate ISONIKE's responsibilities and policy for privacy and protection of personal data.

b. In its everyday business operations ISONIKE makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees and associates
- Customers
- Users of its websites
- Subscribers
- Other stakeholders

c. In collecting and using those data, ISONIKE is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect them.

d. The policy stated below applies to all systems, people and processes that constitute the organization's information systems.

e. ISONIKE recognizes that providing privacy and personal data protection is a mandatory requirement and adds trust to clients and employees/associates. All stakeholders, internal and external personnel are herewith aware of the need for privacy and personal data protection.

2. Principles

ISONIKE acts and operates according to the fundamental principles which GDPR is based. Those are:

1. Personal data shall be:
   - processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
   - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
   - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');
   - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
   - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)

subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with all of the above ('accountability').

ISONIKE ensures that it complies with all of these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems.

3. Rights of the Individuals

The data subjects, as stated in GDPR, also have rights. These are:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

The rights of the data subjects are supported by:

Data Subject Right/ Request	Action
The right to be informed	Inform data subject when data is collected (if supplied by the data subject) or within one month (if not supplied by the data subject)
The right of access	Providing access to his data within one month from the request.
The right to rectification	Rectify his data within one month from the request
The right to erasure	Erase his data without undue delay
The right to restrict processing	Process his data with the requested restriction without undue delay
The right to data portability	Portable his data where requested within one month from the request.
The right to object	Allowing the data subject to object.

4. Policy

a. ISONIKE commits to process any personal data received lawfully, in accordance with GDPR and according the specific case of processing of personal data. The cases are described below:

- **Consent**
  ISONIKE Unless it is necessary for a reason allowable in the GDPR, always obtain explicit consent from a data subject to collect and process their data. In case of children below the age of 16 parental consent will be obtained. Transparent information about our usage of their personal data will be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information will be provided in an accessible form, written in clear language and free of charge.
  If the personal data are not obtained directly from the data subject then this information will be provided to the data subject within a reasonable period after the data are obtained and definitely within one month.
- **Performance of a Contract**
  Where the personal data collected and processed are required to fulfil a contract with the data subject, explicit consent is not required. This will often be the case where the contract cannot be completed without the personal data in question e.g. a delivery cannot be made without an address to deliver to.
- **Legal Obligation**
  If the personal data is required to be collected and processed in order to comply with the law, then explicit consent is not required. This may be the case for some data related to employment and taxation for example, and for many areas addressed by the public sector.
- **Vital Interests of the Data Subject**
  In a case where the personal data are required to protect the vital interests of the data subject or of another natural person, then this may be used as the lawful basis of the processing. ISONIKE will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing of personal data. As an example, this may be used in aspects of social care, particularly in the public sector.
- **Task Carried Out in the Public Interest**
  Where ISONIKE needs to perform a task that it believes is in the public interest or as part of an official duty then the data subject's consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required.
- **Legitimate Interests**
  If the processing of specific personal data is in the legitimate interests of ISONIKE and is judged not to affect the rights and freedoms of the data subject in a significant way, then this may be defined as the lawful reason for the processing. Again, the reasoning behind this view will be documented.

b. ISONIKE will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purposes.
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s).
- Assessment of the risks to individuals in processing the personal data.
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization and pseudonymization will be considered where applicable and appropriate.

c. ISONIKE will ensure that all relationships it enters into that involve the processing of personal data are subject to a documented contract that includes the specific information and terms required by the GDPR.

d. In case of transfers of personal data outside the European Union, data will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.
Intra-group international data transfers will be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

e. A defined role of Data Protection Officer (DPO) is required under the GDPR if an organization is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.
Based on these criteria, ISONIKE does not require a Data Protection Officer to be appointed.

f. ISONIKE is fair and proportionate when considering the actions to be taken to inform affected parties in case of breaches of personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours. This will be managed in accordance with our *Information Security Incident Response Procedure* which sets out the overall process of handling information security incidents.

g. The following actions are undertaken to ensure that ISONIKE complies at all times with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear and unambiguous
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff

- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
    - Organization name and relevant details
    - Purposes of the personal data processing
    - Categories of individuals and personal data processed
    - Categories of personal data recipients
    - Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
    - Personal data retention schedules
    - Relevant technical and organizational controls in place

These actions are reviewed on a regular basis as part of the management process concerned with data protection.