IHE – Europe Privacy Policy

1. Introduction

The right to informational self-determination is a fundamental right in Europe and one of the basic principles of the EU General Data Protection Regulation (GDPR). Every individual has the right to decide which data to disclose, to what extent, and for which purpose. Any collection, processing, or use of personal data requires a legal basis.

The GDPR is applicable to all work undertaken in Europe or relating to data of a person resident in Europe. The GDPR also applies when data are transfer outside Europe in the context of special rules (see below).

2. Purpose

This Global Privacy Policy is aimed to further increasing the awareness of Data Privacy and Data Protection among staff and contractors and establishing rules for responsible conduct so as to avoid violations of the GDPR. It also serves to inform IHE Clients and Partners who wish to know more about IHE's Privacy Policy than is contained in the Information Notice provided on all occasions when personal data are collected.

3. Definition of Privacy Policy Terms

- ***Data Subject*** is the natural person who is described by or identified by *personal data*
- ***Personal data*** is any information relating to a natural person that can be identified, directly or indirectly by that data. A legal basis must exist for processing any personal data
- Certain information is considered ***sensitive personal data*** Information this includes any data on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data collected for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation are considered to be special categories of personal data. Processing of special categories of personal data requires a specific legal basis.
- The term ***processing*** includes the collection, recording, organization, storage, adaptation or alteration, transmission, dissemination or otherwise making available, alignment or combination and erasure or destruction of personal data.
- The ***data controller*** is the natural or legal person, who decides upon the purpose of processing and directs such processing. The controller may delegate the act of processing to a *data processor.*
- IHE may employ the services of external service providers (e.g. for IT service, hosting, external service providers, event co-ordinators, etc.). Such services providers will be ***data processors*** if they handle personal data collected by IHE or for IHE.
- When IHE employs a data processor a specific ***Processor-Controller Agreement*** is adopted which specifies the duties of the processor and controller.
- A ***third party*** is a natural or legal person or public authority other than the Controller. The transmission or dissemination of personal data to third parties always requires a legal basis.

IHE's staff will therefore always need to ensure that there is an appropriate legal basis for the transmission of data to third parties every time data is transmitted or disclosed.

4. Obligation of Confidentiality

Employees and contractors of IHE are prohibited from collecting, processing, or using personal data without authorisation. Employees act without authorisation when they use the data outside the scope of their duties and authorizations. The GDPR is applicable to all IHE activities which involve the collection of personal data such as names, contact details, credentials and CVs, event attendance. All IHE staff and contractors working with IHE are required to understand their duties under the GDPR and to abide by such duties. Non-compliance may lead to termination of contract.

5. Basic Principles of the GDPR

5.1 Data Minimization

Only such personal data may be collected that are necessary in relation to the purposes for which they are processed. Only as much data as necessary and as little as possible should be collected and processed.

5.2 Purpose limitation

Personal data may only be used for the purpose for which they were collected. This principle is also addressed in the Confidentiality Agreement for IHE Employees and Contractors.

5.3 Transparency

Data Subjects are entitled to transparency, i.e., they must be informed about the nature, scope and purposes of the collection, processing, and use of their personal data. They also have a comprehensive right to information against the Controller.

6. Rights of Data Subjects

Data Subjects may assert various rights. Employees and contractors must take such requests seriously and process them quickly.

6.1 Right of Access and Portability

Data Subjects have a comprehensive Right of Access and may request the Controller to disclose all data stored on the Data Subject. When the data has been collected on the basis of consent, or the processing is carried out by automated means, the controller must be able to provide the data subject with a commonly machine readable format of the data concerning him or her.

6.2. Rectification and Erasure

Data Subjects are entitled to have verifiably false or inaccurate data rectified or deleted. In addition, there is a right to erasure if data are no longer required for the purposes for which they were initially collected.

6.3. Right of Objection

Where data processing is carried out on the basis of legitimate interests of IHE, data subjects have the Right to Object to the processing. Please forward any such requests to the IHE-Europe

Secretariat (secretariat@ihe-europe.net). Where necessary, standard processes will be developed for regularly affected processing activities.

6.4. Restriction of Processing

If processing is restricted, access to certain data must be made unavailable. This may in particular be the case if the correctness of the data is disputed or if a conclusive decision on an objection has not yet been reached.

7. Records of Processing Activities

Controllers are obliged to keep records of all Processing Activities. IHE will keep a record of all processing undertaken in a Data Processing Map, which shall be kept updated

8. Risk Assessment and Security of Processing

The GDPR introduces a risk based approach to Data Security. Every Controller must perform a risk assessment and ensure they have adequate procedures and tools in place to address the risks **identified.** IHE has undertaken a full data mapping exercise and will ensure it is kept up to date. Should the nature of data collected and purposes of processing change to include more sensitive categories of data, or higher risks forms of processing, a new risk assessment will be undertaken**.**

9. Liability and Fines

Violations of data protection regulations may result in severe fines. It is therefore essential for all employees and contractors to be attentive and cautious when handling personal data.

10 Related Documents

This Privacy Policy is addressed to all IHE Europe employees, contractors and interested parties. It is further defined and supported by the following documents:

- Data Collection Information Notice & Consent Form Template
- Contractor / Employee Relationship Policy (& Signature Form)
- IT Security Checklist
- Breach Notification Procedure
- Processor Contractor Agreements (Template)