Institute of Sales Professionals – GDPR and Data Protection Policy

Introduction

The Institute of Sales Professionals (ISP) is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

This policy details expected behaviours of ISP's Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to ISP's Customers and Staff (i.e., the Data Subject) and irrespective of the media used to store the information.

Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data.

An organisation that handles personal data and makes decisions about its use is known as a Data Controller. ISP, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy.

Non-compliance may expose ISP to complaints, regulatory action, fines and/or reputational damage. ISP's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all ISP Employees and Third Parties to share in this commitment.

Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

Scope

1. This policy applies to all ISP Entities where a Data Subject's personal data is processed:
   - in the context of the business activities of the ISP Entity
   - for the provision or offer of goods or services to individuals (including those provided or offered free-of-charge) by ISP
   - to actively monitor the behaviour of individuals.

2. Monitoring the behaviour of individuals includes using data processing techniques such as persistent web browser cookies or dynamic IP address tracking to profile an individual with a view to:
   - taking a decision about them
   - analysing or predicting their personal preferences, behaviours and attitudes.

3. This policy applies to all processing of personal data in electronic form (including electronic mail and documents created with word processing software) or where

it is held in manual files that are structured in a way that allows ready access to information about individuals.

4. This policy has been designed to establish a baseline standard for the processing and protection of personal data by all ISP Employees. Where national law imposes a requirement that is stricter than that imposed by this policy, the requirements in national law must be followed. Furthermore, where national law imposes a requirement that is not addressed in this policy, the relevant national law must be adhered to.

5. The protection of personal data belonging to ISP Employees is not within the scope of this policy.

6. The DPO is responsible for overseeing this Privacy Standard and, as applicable, developing Related Policies and Privacy Guidelines. The DPO is within our company Head of Operations.

7. Please contact the DPO with any questions about the operation of this Privacy Standard or the GDPR, or if you have any concerns that this Privacy Standard is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:
   - if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company)
   - if you need to rely on Consent and/or need to capture Explicit Consent
   - if you need to draft Privacy Notices or Fair Processing Notices
   - if you are unsure about the retention period for the Personal Data being Processed
   - if you are unsure about what security or other measures you need to implement to protect Personal Data
   - if there has been a Personal Data Breach
   - if you are unsure on what basis to transfer Personal Data outside the EEA
   - if you need any assistance dealing with any rights invoked by a Data Subject
   - whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA or plan to use Personal Data for purposes others than what it was collected for
   - if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making
   - if you need help complying with applicable law when carrying out direct marketing activities; or
   - if you need help with any contracts or other areas in relation to sharing Personal Data with Third Parties (including our vendors).

Policy Governance

1. Policy Dissemination and Enforcement

The management team of ISP must ensure that all ISP Employees responsible for the Processing of Personal Data are aware of and comply with the contents of this policy. In addition, ISP will make sure all Third Parties engaged to Process Personal

Data on their behalf (i.e. their Data Processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal Data controlled by ISP.

2. Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing. ISP must ensure that a Data Protection Impact Assessment (DPIA) is conducted, for all new and/or revised systems or processes for which it has responsibility. ISP should consult with a Data Protection subject matter expert during the course of completing the DPIA. The subsequent findings of the DPIA must then be submitted to the senior risk office for ISP for review and approval. Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will cooperate with the Data Protection subject matter expert to assess the impact of any new technology uses on the security of Personal Data.

3. Compliance Monitoring

To confirm that an adequate level of compliance is being achieved by ISP in relation to this policy, ISP will carry out an annual Data Protection compliance audit. Each audit will, as a minimum, assess compliance with this policy and the operational practices in relation to the protection of Personal Data, including:

1. the assignment of responsibilities
2. raising awareness
3. training of Employees
4. adequacy of organisational and technical controls to protect Personal Data
5. records management procedures (including data minimisation)
6. adherence to the qualified rights of the Data Subject
7. Privacy by Design and Default
8. consent for direct marketing
9. Personal Data transfers
10. Personal Data incident management (including Personal Data breaches)
11. Personal Data complaints handling
12. the currency of Data Protection policies and Privacy Notices
13. the accuracy of Personal Data being stored
14. the conformity of Data Processor activities
15. the adequacy of procedures for redressing poor compliance.

Any major deficiencies identified will be reported to and monitored by the ISP Executive Management team.

Principles

ISP has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data.

PRINCIPLE	DEFINITION
Principle 1: Lawfulness, Fairness and Transparency	Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, ISP must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).
Principle 2: Purpose Limitation	Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means ISP must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.
Principle 3: Data Minimisation	Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed. This means ISP must not store any Personal Data beyond what is strictly required.
Principle 4: Accuracy	Personal Data shall be accurate and kept up to date. This means ISP must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.
Principle 5: Storage Limitation	Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed. This means ISP must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.
Principle 6: Integrity & Confidentiality	Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. ISP must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data are maintained at all times.

Accountability

The Data Controller shall be responsible for, and be able to demonstrate, compliance. This means ISP must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

Data Collection

Personal Data should be collected only from the Data Subject unless one of the following applies:

1. The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.
2. The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

3. If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:
    - the Data Subject has received the required information by other means
    - the information must remain confidential due to a professional secrecy obligation
    - a national law expressly provides for the collection, Processing or transfer of the Personal Data.