Institute for Supply Management®

Privacy and Personal Data Protection Policy

SC739 6/20

ISM®
INSTITUTE FOR SUPPLY MANAGEMENT

Contents

1. Introduction

In its everyday business operations, Institute for Supply Management, Inc.® (ISM®) makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees
- Members, customers and other professionals served
- Users of its websites
- Other stakeholders

In collecting and using this data, the organization 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 it.

The purpose of this policy is to set out the relevant legislation and to describe the steps Institute for Supply Management is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to ISM's systems and data.

2. Privacy and Personal Data Protection Policy

2.1 The General Data Protection Regulation

The General Data Protection Regulation 2016 (GDPR) is one of the most significant pieces of legislation affecting the way that Institute for Supply Management carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of citizens of the European Union. It is Institute for Supply Management's policy to ensure that our compliance with the GDPR and other relevant legislation is clear and demonstrable at all times.

2.2 China's Personal Information Protection Law

Adopted on Aug. 20, 202[1], at the 30th Session of the Standing Committee of the 13th national People's Congress, China's Personal Information Protection Law (PIPL), is the first national-level law comprehensively regulating issues in relation to personal information protection.

2.3 Definitions

The most fundamental definitions, under both laws, are listed below:

***Personal data* is defined as:**

(GDPR) any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier.

(PIPL) any kind of information, electronically or otherwise recorded, related to an identified or identifiable natural person within the People's Republic of China (PRC). PI excludes anonymized information that cannot be used to identify a specific natural person and is not reversible after anonymization. PIPL Art. 4.

***'processing'* means:**

(GDPR) 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(PIPL) Processing (sometimes translated as "handling") includes the collection, storage, use, alteration, transmission, provision, disclosure, deletion, etc. of PI. PIPL Art. 4.

***'controller'* means:**

(GDPR) 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

2.4 Principles Relating to Processing of Personal Data

There are a number of fundamental principles upon which the GDPR is based.

These are as follows:

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) 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');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) 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');

(e) 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');

(f) 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, using appropriate technical or organizational measures ('integrity and confidentiality').

(PIPL) any kind of information, electronically or otherwise recorded, related to an identified or identifiable natural person within the People's Republic of China (PRC). Personal Information (PI) excludes anonymized information that cannot be used to identify a specific natural person and is not reversible after anonymization. PIPL Art. 4.

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Institute for Supply Management will ensure 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.

2.5 Rights of the Individual

The data subject also has rights under the GDPR. These consist of:

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.

Data subject rights under PIPL:
Unless laws or administrative regulations stipulate otherwise, the PIPL grants individuals the right to know about, decide on, limit use of, or object to the use of their PI. PIPL Art. 44. The PIPL also grants individuals the right to access and copy their PI subject to certain exceptions, as well as the right to correct or supplement their PI if incorrect or incomplete. PIPL Art. 45; PIPL Art. 46.

Handlers must proactively delete—or alternatively individuals may request handlers to delete—PI where: (1) the processing is no longer necessary for the stated purpose; (2) the handler is no longer providing a product or service, or the retention period has expired; (3) individuals have revoked consent; (4) the processing would violate specific laws, regulations, or agreements; or (5) other laws or regulations so provide. PIPL Art. 47.

The PIPL also creates a right to data portability, provided any transfer to a new handler satisfies the conditions prescribed by the relevant enforcement authorities. PIPL Art. 45.

2.6 Lawfulness of Processing

It is Institute for Supply Management policy to identify the appropriate basis for processing and to document it, in accordance with both regulations and other regulation that might impact our operations. The options are described in brief in the following sections.

2.6.1 Consent

Unless it is necessary for a reason allowable in the GDPR, Institute for Supply Management will always obtain explicit consent from a data subject to collect and process their data. Transparent information about our usage of personal data will be provided to data subjects and 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.

2.6.2 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 under GDPR. This will often be the case where the contract cannot be completed without the personal data in question. For example, the delivery of an order will require an email address and/or a physical address.

PIPL provides several legal bases for processing PI:

- Obtaining individuals' consent.
- Where necessary for the performance of a contract to which the individual concerned is a party, or for the implementation of human resources management.
- Where necessary for the performance of statutory responsibilities or obligations.
- Where necessary for responding to a public health emergency or protecting the life, health, or property of individuals in cases of emergency.
- For purposes of news reporting and other activities in the public interest.
- For purposes of processing PI already disclosed by the individuals themselves or otherwise lawfully disclosed.
- Where otherwise permitted by laws and regulations.

2.6.3 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 under GDGR. This may be the case for some data related to employment and taxation for example, and for many areas addressed by the public sector.

2.6.4 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. Institute for Supply Management 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.

2.6.5 Task Carried Out in the Public Interest

Where Institute for Supply Management 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. For example, some of research performed by the Report on Business® group and the CAPS Research group may fall into this area.

2.6.6 Legitimate Interests

If the processing of specific personal data is in the legitimate interests of Institute for Supply Management 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 under GDPR. The reasoning behind this view will be documented.

2.7 Privacy by Design

Institute for Supply Management has adopted the principle of privacy by design and 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 pseudonymisation will be considered where applicable and appropriate.

2.8 Contracts Involving the Processing of Personal Data

Institute for Supply Management 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. For more information, see the *GDPR Controller-Processor Agreement Policy*.

2.9 International Transfers of Personal Data

Transfers of personal data outside the European Union and China borders will be carefully reviewed prior to the transfer taking place to ensure that
they fall within the limits imposed by the GDPR and PIPL.

ISM does not currently have any offices within the EU nor China borders.

2.10 Data Protection Officer and/or Data Handler

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, Institute for Supply Management does not require a Data Protection Officer to be appointed.

A “PI handler” refers to organizations and individuals that independently determine the purposes and means of processing PI. Institute for Supply Management’s data handlers can be reached at 1+ 480.752.6276.

2.11 Breach Notification

It is Institute for Supply Management’s policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding 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 following the knowledge of the incident and pursuant to legal and technical guidance. This will be managed in accordance with our Information Security Incident Response Procedure which sets out the overall process of handling information security incidents.

2.12 Addressing Compliance to the GDPR

The following actions are undertaken to ensure that Institute for Supply Management 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 inquiries are handled effectively
- Annual 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

2.13 Addressing PIPL Compliance

Any organization or individual has the right to file a complaint with the relevant enforcement authorities about a PI handler’s unlawful practices. PIPL Art. 65.

Where PI handlers reject individuals’ requests to exercise their rights, individuals may file a lawsuit in court. PIPL Art. 50.

Where illegal processing of PI harms the rights and interests of individuals, the procuratorates, consumer organizations prescribed by the law, and other organizations designated by the relevant enforcement authorities may bring an action before a court. PIPL Art. 70.

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

Institute for Supply Management®
309 W. Elliot Road, Suite 113
Tempe, AZ 85284
+1 480.752.6276
www.ismworld.org