Privacy and Personal Data Protection Policy
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.

The following policies and procedures are relevant to this document:

- Data Protection Impact Assessment Process
- Personal Data Mapping Procedure
- Legitimate Interest Assessment Procedure
- Information Security Incident Response Procedure
- GDPR Roles and Responsibilities
- Records Retention and Protection Policy

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 Definitions
There is a total of 26 definitions listed within the GDPR and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:

**Personal data** is defined as:
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.

**'processing'** means:
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;

**'controller'** means:
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;

2.3 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').
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.

2.4 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.

Each of these rights are supported by appropriate procedures within
Institute for Supply Management that allow the required action to be
taken within the timescales stated in the GDPR.

<table>
<thead>
<tr>
<th>Data Subject Request</th>
<th>Timescale</th>
</tr>
</thead>
<tbody>
<tr>
<td>The right to be informed</td>
<td>When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)</td>
</tr>
<tr>
<td>The right of access</td>
<td>One month</td>
</tr>
<tr>
<td>The right to rectification</td>
<td>One month</td>
</tr>
<tr>
<td>The right to erasure</td>
<td>Without undue delay</td>
</tr>
<tr>
<td>The right to restrict processing</td>
<td>Without undue delay</td>
</tr>
<tr>
<td>The right to data portability</td>
<td>One month</td>
</tr>
<tr>
<td>The right to object</td>
<td>On receipt of objection</td>
</tr>
<tr>
<td>Rights in relation to automated decision making and profiling.</td>
<td>Not specified</td>
</tr>
</tbody>
</table>

Table 1 — Timescales for data subject requests

2.5 Lawfulness of Processing
There are six alternative ways in which the lawfulness of a specific
case of processing of personal data may be established under the
GDPR. It is Institute for Supply Management policy to identify the
appropriate basis for processing and to document it, in accordance
with the Regulation. The options are described in brief in the following
sections.

2.5.1 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. In case of children below the
age of 16 (a lower age may be allowable in specific EU member states),
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.

2.5.2 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.
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.

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

2.5.4 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.

2.5.5 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.

2.5.6 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. The reasoning
behind this view will be documented.
2.6 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.

2.7 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.

2.8 International Transfers of Personal Data
Transfers of personal data outside the European Union 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.

ISM does not currently have any offices within the EU; however, this could apply to data collected in its Shanghai office and transmitted to ISM’s corporate office.

2.9 Data Protection Officer
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.

2.10 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.

Under the GDPR the relevant DPA has the authority to impose a range of fines of up to four percent of annual worldwide turnover or twenty million Euros, whichever is the higher, for infringements of the regulations.

2.11 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

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