

Publication of Particulars based on Act on the Protection of Personal Information

JAMCO Corporation

We hereby announce the particulars about our appropriate handling of personal data (this “Policy”) in accordance with the Act on the Protection of Personal Information (Act No. 57 of 2003; the “Personal Information Protection Act”).

**1. Company name and address, and name of representative**

JAMCO Corporation

1-100 Takamatsu-cho, Tachikawa-shi, Tokyo, Japan, 190-0011

Representative Director : Harutoshi Okita

**2. Compliance with relevant laws and regulations, guidelines, etc.**

We comply with laws and regulations such as the Personal Information Protection Act, and guidelines such as the Personal Information Protection Commission’s guidelines, and appropriately handle personal data.

**3. Collection and use of personal information**

We will announce or give notice of the purpose of use (including announcement in this Policy) when collecting your personal information and we will specify the purpose of use before collecting personal information detailed in agreements or other documents (including electronic or magnetic records) directly from you, and collect the personal information through legal and fair means.

We will use personal information appropriately to the extent necessary to achieve the purpose of use.

**4. Purpose of use of personal information**

We will use the personal information for the following purposes:

- (1) Personal information of business partners (in the case of corporate customers, all employees and officers of that corporation)
  - Communications, inquiries, responses, and business administration in the course of business
  - Execution of agreements and performance of agreement terms and conditions
  - Processing payments and billing
- (2) Personal information of shareholders (in the case of corporate shareholders, all employees and officers of that corporation)

- Performance of rights and obligations in accordance with the Companies Act and other laws and regulations
  - Provision of various advantages from us to people with shareholder status
  - Implementation of various policies to facilitate the relationship between shareholders and JAMCO
  - Shareholder management, such as preparation of shareholder data based on the designated standards under laws and regulations
- (3) Personal information of persons using our inquiries contact
- Management of persons using our inquiries contact, such as preparation of user data based on the designated standards under laws and regulations
  - Responding to and handling inquiries
- (4) Personal information of employment applicants
- Provision of employment information and communication regarding employment screening
- (5) Personal information of persons wishing to participate in internships
- Provision of internship information, recruitment and selection of participants, and procedures for participating
  - Implementation of internships
- (6) Personal information of outsourcees and dispatched workers who carry out work at JAMCO
- Work communications and emergency communications
  - Site access management and employment management
- (7) Personal information of officers, employees, etc., former officers, employees, etc., and their families
- Services regarding employment and induction procedures, and resignation or retirement procedures
  - Services regarding performance management, employee performance evaluations, transfers, job rotation, secondment and transfers of registered domicile, and personnel management such as commendations and disciplinary action
  - Services regarding payment of compensation, such as salaries, bonuses, and retirement benefits
  - Services regarding employment management, such as start and finish times, leave, temporary absence from work, administrative leave, and working hours
  - Services regarding taxation procedures for income tax, such as withholding at the source, and local tax
  - Services regarding procedures for social insurance and labor insurance
  - Services regarding procedures for social services, group insurance, etc.

- Services regarding communication with, and provision of information to, health insurance societies and employees stock ownership plan associations
  - Services regarding development of personnel such as education and training
  - Services regarding industrial safety, industrial health, and health management
  - Services regarding internal disclosure such as work communications and emergency communications
  - Services regarding facility management, such as site access management
  - Services regarding expense settlement
  - Other services regarding procedures required for personnel and work management and matters required under laws and regulations
- (8) Other
- Other services incidental or related to the purposes detailed in (1) through (7) above

**5. Joint use of personal information**

We will jointly use the personal information as follows:

- (1) Jointly used personal information
- (i) Personal information of business partners
    - Name, address, company name and address, affiliated department and role, telephone number, cellphone number, FAX number, email address, and other matters required for the joint purpose of use in (3) below
  - (ii) Personal information of persons using our inquiries contact
    - Name, address, company name and address, affiliated department and role, telephone number, cellphone number, FAX number, email address, and other matters required for the joint purpose of use in (3) below
  - (iii) Personal information of officers, employees, etc., and their families
    - Name, date of birth, gender, address, nationality, academic background, work experience, telephone number, cellphone number, email address, basic pension number, information regarding family (name, date of birth, gender, relationship, address, occupation, income, and health condition), employee number, employment pattern, affiliated department, role, internal qualifications and performance rating, transfer history, salary, allowance, bonus and retirement benefit amounts, health insurance insured number, matters regarding employee performance evaluations, matters regarding health information, matters regarding labor insurance, employment status, commendations and disciplinary action, qualifications and licenses, history of attending education sessions, matters regarding intellectual property, matters regarding employee stock ownership plans,

matters regarding property accumulation savings, matters regarding corporate pensions, membership in group insurance, and other information required to achieve the joint purpose of use in (3) below

(2) Joint users

JAMCO and JAMCO's domestic and foreign subsidiaries

(3) Joint purpose of use

We will jointly use personal information within the scope of the purpose of use in 4 above.

(4) The name, address, representative, and other information of the company that is responsible for managing personal data

JAMCO is responsible for jointly used personal data. Please see 1 above regarding our address and representative.

Following is the contact information for any inquiries regarding joint use.

Contact information

1-100 Takamatsu-cho, Tachikawa-shi, Tokyo, Japan, 190-0011

JAMCO Corporation, Corporate Administration & Human Resource Department,  
General Affairs Section

Telephone no.: +81(0)42-503-9900

Reception hours: Monday through Friday (excluding national holidays, and year-end and new year holidays)  
9:30 a.m. to 12:00 p.m., 1:00 p.m. to 4:30 p.m.

## 6. Provision of personal information to third parties

We will not provide any third party with personal information we have gathered, except in the following cases:

- (1) If you have consented beforehand
- (2) If outsourcing to the extent necessary to achieve the purpose of use
- (3) If requested to provide the personal information in accordance with laws and regulations
- (4) If necessary for the protection of the life, body, or property of a person and it is difficult to obtain your consent
- (5) If particularly necessary for improving public health or promoting the sound upbringing of children and it is difficult to obtain your consent
- (6) If it is necessary to cooperate with a state, local, or other government to perform their duties set out in laws and regulations, and the execution of those duties is likely to be impeded by obtaining your consent
- (7) If the personal information is provided to a party listed in the scope of joint users in 5 above

## 7. **Matters regarding safety management measures**

We will take the necessary and appropriate safety management measures to prevent the leaking or destruction of, or damage to, and otherwise manage, personal data. In addition, employees and outsourcees that handle personal data (including parties that are subcontracted to handle personal data) will be subject to the necessary and appropriate supervision. The safety management measures for personal data are specifically set out separately in the Personal Information Management Regulations. Following is an outline of the main provisions of those regulations.

### **Announce of the particulars based on Act on the Protection of Personal Information**

- To announce this Policy (the particulars about our appropriate handling of personal data) regarding matters such as compliance with relevant laws and regulations, guidelines, etc. and a point of contact for questions and complaints processing in order to ensure the appropriate handling of personal data.

### **Maintenance of Personal Data Handling Regulations**

- To establish the Personal Information Management Regulations regarding handling methods, the person responsible or in charge, and their role, etc. for each stage of collecting, using, storing, providing, deleting, and disposing of personal data.

### **Systematic Safety Management Measures**

- To appoint a person responsible for administration of personal data handling, clarify the scope of employees who handle personal data and personal data handled by those employees, and maintain a system for reporting to and communicating with the person responsible for administration if any facts or signs are recognized as being in breach of the Personal Information Protection Act or the Personal Information Management Regulations.
- To periodically verify the appropriate handling of our personal data and compliance with laws, regulations, and the Personal Information Management Regulations, and encourage improvement thereof by the persons responsible for personal information such as officers, persons responsible for personal information managed within each department and personal information disclosed from outside the company within each department, and other relevant persons.

### **Personal Safety Management Measures**

- To provide regular training to employees on matters of concern in relation to the handling of personal data.

### **Physical Safety Management Measures**

- To control access by employees to rooms in, and restrict devices, etc. brought into, the area where personal data is handled, and take measures to prevent unauthorized people from accessing personal data.

- To take measures to prevent the theft, loss, etc. of devices, electronic media, documents, etc. for handling personal data, and take measures so that personal data is not easily identified if that device, electronic media, etc. is taken, including if it is moved within the office.

#### **Technological Safety Management Measures**

- To control access, and limit the scope of people in charge and personal information data bases, etc. that are handled.
- To introduce a system for protecting the information system that handles personal data from external unauthorized access or malware.

#### **Handling of Personal Data in Foreign Countries**

- To store personal data in Japan, as well as the foreign countries in 8 below, and take security management measures with an understanding of the systems for protecting personal information in those foreign countries. For details, please see 8 below.

### **8. Handling of personal data in foreign countries**

- Some personal information regarding our employees (see 4(7) above) is handled at our Toulouse Branch in France. The Toulouse Branch in France is in the European Economic Area (the “EEA”) and is subject to the General Data Protection Regulation (the “GDPR”). However, we have set out the EU GDPR Personal Information Management Regulations based on our understanding of the terms and conditions of the GDPR and take the safety management measures set out in those regulations. An outline of the GDPR is found at the end of this Policy.
- The legal support system operated by Ricoh Japan in Japan uses servers located in Japan. Ricoh Japan also uses back-up servers located in the U.S.
- The location of the server for Microsoft 365 (which is a program of Microsoft, with its headquarters in the U.S.) differs depending on the Microsoft service. SharePoint and Skype use servers located in Japan, but Exchange and Teams have servers in the Asia-Pacific region, but the specific country in that region has not been disclosed.

### **9. Handling of personal information on our website**

- Use of cookies  
The technology that records and manages information from customers using our website on computer and application software is referred to as “cookies.” Our website uses cookies to make the experience more user friendly. Cookies identify the IP address and browser that you use, but do not identify personal information, and are only used to gain an insight into your browsing experience on our website.
- Use of beacons  
Our website uses web beacons to collect information and statistics with the objective of

improving the user experience. Web beacons cannot be used to identify your personal information, and are only used to gain an insight into your browsing experience on our website.

- **Use of Google Analytics**

We use Google Analytics, which is a Google Inc. (“Google”) service, to gain an insight into your visit to our website.

When you use our website, Google collects, records, and analyzes your visit history based on the cookies issued by our website.

We receive the results of that analysis from Google and gain an insight into your visit to our website.

The information collected, recorded, and analyzed by Google Analytics does not contain information that identifies specific individuals. That information is managed by Google in accordance with their privacy policy.

You can also prevent your information from being collected through our use of Google Analytics by disabling Google Analytics in the browser ad-on settings. The setting for disabling Google Analytics can be implemented by downloading and installing the “Google Analytics opt-out browser ad-on” on Google’s download page for the opt-out ad-on, and changing the ad-on settings in your browser. If you disable Google Analytics, Google Analytics will also be disabled for other websites that you visit, but you can enable Google Analytics again through your browser add-on settings. For an explanation of the Google Analytics Terms of Service, please visit the Google Analytics website, and for an explanation of Google’s Privacy Policy, please see Google’s website.

[Google Analytics Terms of Service](http://www.google.com/analytics/terms/jp.html)

<http://www.google.com/analytics/terms/jp.html>

[Google’s Privacy Policy](http://www.google.com/intl/ja/policies/privacy/)

<http://www.google.com/intl/ja/policies/privacy/>

[Google Analytics Opt-Out Browser Add-On](https://tools.google.com/dlpage/gaoptout?hl=ja)

<https://tools.google.com/dlpage/gaoptout?hl=ja>

## **10. Requests for disclosure of personal information**

If we receive a request inquiring about, to correct, to suspend use of, to delete, or to otherwise act regarding, the personal information, we will respond promptly after confirming that person’s identity using the prescribed procedures. Please direct any questions about this Policy to, or exercise your rights in relation to this Policy with, the inquiries contact in 11 below.

## **11. Inquiries contact**

Please direct any questions or complaints regarding the handling of personal data at JAMCO to the following point of contact.

(i)	Address	1-100 Takamatsu-cho, Tachikawa-shi, Tokyo, Japan, 190-0011 JAMCO Corporation, Corporate Administration & Human Resource Department, General Affairs Section
(ii)	Telephone no.:	+81(0)42-503-9900
(iii)	Reception hours:	Monday through Friday (excluding national holidays, and year-end and new year holidays) 9:30 a.m. to 12:00 p.m., 1:00 p.m. to 4:30 p.m.

End of Publication of Particulars based on Act on the Protection of Personal Information

Outline of GDPR

Existence of a system for the protection of personal information	The following law exists in the European Economic Area (EEA) in which France is located, as a comprehensive law regarding the protection of personal information. <ul style="list-style-type: none"> <li>● General Data Protection Regulation (the “GDPR”) <ul style="list-style-type: none"> <li>- URL : <a href="https://eur-lex.europa.eu/eli/reg/2016/679/oj">https://eur-lex.europa.eu/eli/reg/2016/679/oj</a></li> <li>- Enforcement: May 25, 2018</li> <li>- Target bodies: Natural or legal persons, public authorities, agencies, and other bodies</li> <li>- Target information: ‘Personal data’ means any information relating to an identified or identifiable natural person; 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 or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</li> </ul> </li> </ul>
Existence of information indicating a system for the protection of personal information	France is a member state of the European Economic Area (EEA), and therefore any company in France is subject to the GDPR.
Business operator obligations and data subject rights that correspond to the eight	According to Section 5-2 (p. 43) of the <a href="#">Guidelines to the Revised Personal Information Protection Act (for Transfers to Third Parties in Foreign Countries) (in Japanese)</a> , if there are no business operator obligations and no data subject rights that correspond to the eight



<p>principles in the OECD Privacy Guidelines</p>	<p>principles in the OECD Privacy Guidelines, the non-existence of those business operator obligations and data subject rights demonstrates a substantial difference to Japan’s Personal Information Protection Act. Therefore, information must be provided to that data subject on the details thereof. The eight principles of the OECD Privacy Guidelines are as shown below. Please refer to the text of the OECD Privacy Guidelines provided by the Organisation for Economic Co-operation and Development for precise details (see “Part Two. Basic Principles of National Application” <a href="#">here</a>).</p> <p><u>Outline of the eight principles of the OECD Privacy Guidelines</u></p> <p>1. Collection Limitation Principle</p> <p>When collecting personal data, it should be obtained by lawful and fair means and with notice to or the consent of the data subject.</p> <p>2. Data Quality Principle</p> <p>Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.</p> <p>3. Purpose Specification Principle</p> <p>The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use should not be incompatible with those purposes at the time of collection.</p> <p>4. Use Limitation Principle</p> <p>Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject or by the authority of law.</p> <p>5. Security Safeguards Principle</p> <p>Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.</p> <p>6. Openness Principle</p> <p>There should be openness about the policy for collection of personal data, and the existence and purposes of use of personal data, as well as the identity and residence of the data controller should be made clear.</p> <p>7. Individual Participation Principle</p> <p>An individual should be guaranteed that they can request confirmation of whether or not the data controller has data relating to that individual</p>
--	--

	<p>and that they can challenge the denial of such request.</p> <p>8. Accountability Principle</p> <p>The data controller should be accountable for complying with the principles stated above.</p> <table border="1" data-bbox="544 506 1326 1182"> <tr> <td data-bbox="544 506 887 600">(i) Collection Limitation Principle</td> <td data-bbox="887 506 1326 600">Prescribed in the above law.</td> </tr> <tr> <td data-bbox="544 600 887 651">(ii) Data Quality Principle</td> <td data-bbox="887 600 1326 651">Prescribed in the above law.</td> </tr> <tr> <td data-bbox="544 651 887 745">(iii) Purpose Specification Principle</td> <td data-bbox="887 651 1326 745">Prescribed in the above law.</td> </tr> <tr> <td data-bbox="544 745 887 840">(iv) Use Limitation Principle</td> <td data-bbox="887 745 1326 840">Prescribed in the above law.</td> </tr> <tr> <td data-bbox="544 840 887 934">(v) Security Safeguards Principle</td> <td data-bbox="887 840 1326 934">Prescribed in the above law.</td> </tr> <tr> <td data-bbox="544 934 887 985">(vi) Openness Principle</td> <td data-bbox="887 934 1326 985">Prescribed in the above law.</td> </tr> <tr> <td data-bbox="544 985 887 1079">(vii) Individual Participation Principle</td> <td data-bbox="887 985 1326 1079">Prescribed in the above law.</td> </tr> <tr> <td data-bbox="544 1079 887 1182">(viii) Accountability Principle</td> <td data-bbox="887 1079 1326 1182">Prescribed in the above law.</td> </tr> </table>	(i) Collection Limitation Principle	Prescribed in the above law.	(ii) Data Quality Principle	Prescribed in the above law.	(iii) Purpose Specification Principle	Prescribed in the above law.	(iv) Use Limitation Principle	Prescribed in the above law.	(v) Security Safeguards Principle	Prescribed in the above law.	(vi) Openness Principle	Prescribed in the above law.	(vii) Individual Participation Principle	Prescribed in the above law.	(viii) Accountability Principle	Prescribed in the above law.
(i) Collection Limitation Principle	Prescribed in the above law.																
(ii) Data Quality Principle	Prescribed in the above law.																
(iii) Purpose Specification Principle	Prescribed in the above law.																
(iv) Use Limitation Principle	Prescribed in the above law.																
(v) Security Safeguards Principle	Prescribed in the above law.																
(vi) Openness Principle	Prescribed in the above law.																
(vii) Individual Participation Principle	Prescribed in the above law.																
(viii) Accountability Principle	Prescribed in the above law.																
<p>Existence of a system that may have a material impact on the rights and interests of a data subject</p>	<ul style="list-style-type: none"> <li>● A system regarding the obligation to keep personal information in a certain region that may have a material impact of the rights and interests of a data subject Such system has not been identified.</li> <li>● A system imposing an obligation on business operators to cooperate with the government's information collection activities that may have a material impact on the rights and interests of a data subject Such system has not been identified.</li> </ul>																