ITOCHU DEUTSCHLAND GMBH -Hamburg Branch
PRIVACY STATEMENT

ITOCHU Deutschland GmbH, Hamburg Branch respects the privacy and rights of all individuals and takes very seriously its responsibilities under the data protection and privacy laws which apply to our business.

This privacy statement explains how and why we use personal data, and what we do to ensure that your information is kept safe and secure in accordance with the General Data Protection Regulation and any other applicable data protection and privacy laws (**Data Protection Laws**).

This statement explains:

1. WHO WE ARE AND HOW TO CONTACT US

We are ITOCHU Deutschland GmbH,Hamburg Branch (the **Company**, **we**, **our**, or **us**), a German GmbH with the register number HRB 10638, having our registered office and main place of business at Am Seestern 18, 40547 Düsseldorf, Germany. You can contact us by writing to us at our office address or telephoning us in Hamburg on 49-40-41529-143.

For the purposes of Data Protection Laws, we are a controller in relation to much of the personal data we collect and process. This means that we are responsible for deciding how and why we use personal data, and for keeping it safe. According to the General Data Protection (GDPR) we will arrange registration after May 25th 2018.

2. HOW WE COLLECT AND PROCESS PERSONAL DATA

A. BUSINESS, PROFESSIONAL AND OTHER CONTACTS

How we collect personal data

We collect and process personal data (meaning information which relates to an identifiable individual) relating to individual business and professional contacts

and other people we engage with in the course of our business, such as the employees of our corporate customers. Usually this information is:

- provided by the individuals themselves;
- collected in the process of providing goods and services to our corporate customers (such as through correspondence and exchanging business cards);
- provided to us by third parties (such as other businesses we work with); or
- obtained from external sources.

The types of personal data we collect

The types of personal data we hold about these individuals typically consists of some or all of the following:

- contact information (such as name, address, telephone and email address);
- bank details (provided by a supplier and processed when we receive or make a payment).

There may of course be situations where we may process other types of personal data in the course of providing goods and services to our corporate customers, receiving goods and services from our suppliers and promoting our business. If we do, then it will be protected to the same high standards explained in this statement.

Why we need to use personal data

Depending on the circumstances, and the nature of our relationship with the people involved, we may use your personal data to:

- fulfil our contractual obligations or exercise contractual rights (such as paying our suppliers);
- communicate with other organisations, advisers or intermediaries; or
- send business related communications (usually by email);
- in order to comply with our legal obligations;
- pursue our legitimate interests in operating and promoting the success of our business, or to pursue the interests of our corporate customers in providing our goods and services.

B. RECRUITMENT

We collect, store and use personal data about individuals who apply to join us. This may include information:

- you provide to us (such as in CVs, application forms, and through correspondence);
- you provide during an interview;
- obtained from previous employers and referees;
- provided to us by recruitment agencies; and
- received as a result of our carrying out background checks (such as checks for criminal convictions with the Disclosure and Barring Service).

The information we collect might include sensitive personal data, such as information about your health and sickness records. If we need to process sensitive personal data then we will ask for your explicit consent before doing so.

If you apply for a position with us, we may carry out a check for criminal convictions in order to satisfy ourselves that there is nothing in your history which makes you unsuitable for the role. We do this because working with us involves a high degree of trust (as you will have access to confidential information).

We only carry out criminal records checks and ask for references at the last stage of the application process, when making an offer of employment, and always act in accordance with the specific requirements of Data Protection Laws and other applicable national laws.

How we use applicant information

We use the personal data we collect about you to:

- assess your skills, qualifications, and suitability for a role;
- carry out background and reference checks;
- communicate with you about your application;
- keep records related to our hiring process; and
- comply with legal or regulatory requirements.

We do all of this because either it is a necessary part of entering into a contract of employment with you or because we have a legitimate interest in ensuring that you are suitable for a particular role.

If you fail to provide personal data when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully.

3. RECIPIENTS OF PERSONAL DATA

Personal data you provide to us will be kept private and confidential and except as set out in this statement we will not disclose or share it with other data controllers without your permission. The only exception to this is where we are legally required to disclose personal data. For example, to comply with a court order. We may also be required to share personal information with regulatory authorities (including the Data Protection Authority) in the event of an audit or investigation.

We share your personal data with some of the third parties who provide services to our firm. This includes software and cloud service providers and IT support services. However, these third parties will only process personal data (which may include your information) on our behalf for specified purposes and in accordance with our strict instructions.

We only use third party service providers who have provided sufficient guarantees, as required by Data Protection Laws, that your personal data will be kept safe. We always ensure there is a written contract in place which protects your personal data and prevents it from being used for any purpose other than providing services to our business, in accordance with Data Protection Laws.

We may also share your personal data within the ITOCHU group of companies where this is necessary for the purposes for which it was obtained and in accordance with the safeguards explained in section 7 (International Transfers).

4. HOW LONG WE STORE PERSONAL DATA FOR

We only retain personal data for as long as is necessary for the specific purpose(s) it was collected for (or for related compatible purposes such as complying with applicable legal, accounting, or record-keeping requirements).

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from its unauthorised use or disclosure, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

5. HOW WE KEEP PERSONAL DATA SAFE

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, damaged or destroyed, altered or disclosed. This includes both physical security measures (such as keeping paper files in secure, access-controlled premises) and electronic security technology (such as digital back-ups and sophisticated anti-virus protection).

We limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to legal and contractual confidentiality obligations.

We have put in place reporting procedures to deal with any suspected personal data breach and will notify you and any applicable supervisory authority of a breach when we are legally required to do so.

6. INTERNATIONAL TRANSFERS

We normally only store personal data within the European Economic Area (**EEA**). However, some of the technology and support services we use are provided by international organisations and/or companies which are based outside the EEA. We may also share your personal data within the ITOCHU group of companies, which will involve transferring it to Japan and other countries outside the EEA.

Before using such service providers or making such transfers to ITOCHU group companies outside the EEA, we take steps to make sure that any personal data they process is adequately protected and transferred in accordance with Data Protection Laws, usually by one or more of the following methods:

- ensuring the recipient is in a country which the EU Commission has deemed provides adequate protection for personal data;
- implementing appropriate safeguards such as requiring the recipient to enter into Standard Contractual Clauses approved by the European Commission; or
- (if the recipient is based in the USA) transferring personal data to recipients who are certified under the EU-US Privacy Shield scheme.

7. YOUR RIGHTS AS A DATA SUBJECT

Data Protection Laws provide you with certain rights in relation to your personal data. These are as follows:

- **The right to access your personal data.** This enables you to receive a copy of the personal data we hold about you.
- **The right to request correction or completion of personal data**. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **The right to request erasure of your personal data**. This enables you to ask us to delete or remove personal data (though this may not apply where we have a good, lawful reason to continue using the information in question). You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).
- **The right to object to processing of your personal data.** You can object to us processing personal data for legitimate interests purposes or for direct marketing.
- **The right to restrict how your personal data is used**. You can limit how we use your information (primarily to storage or for use in legal claims).
- **The right to have a portable copy or transfer your personal data**. We will provide you, or (where technically feasible) a third party, with a copy of your personal data in a structured, commonly used, machine-readable format. Note this only applies to automated information we process on the basis of your consent or in order to perform a contract.
- **The right to withdraw consent.** If we are relying on consent to process your personal data you have the right to withdraw that consent at any time.

Responding

We try to respond to all personal data requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. Please also bear in mind that there are exceptions to the rights above and some situations where they do not apply.

We may need to request additional information from you to help us confirm your identity. This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you to clarify your request.

Fees for making a request

You will not normally have to pay a fee to access your personal data (or to exercise any of your other rights). However, we may charge a reasonable fee if your request is unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

How to make a request

If you want to exercise any of the rights described above, please write to Data Protection Requests, ITOCHU Deutschland GmbH - Hamburg Branch, Brandstwiete 1, 20457 Hamburg.

Your right to complain to a supervisory authority

You have the right to complain to a data protection supervisory authority (which is for us: Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Landesbeauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) if you are not satisfied with our response to a data protection request or if you think your personal data has been mishandled. For further information on how to make a complaint, https://datenschutz-hamburg.de/

8. UPDATES TO THIS STATEMENT

We will update this statement from time to time. The current version will always be posted on our website. This statement was last updated on 25 May 2018.