



JTC Group *Client Privacy Notice*

14 May 2025



POWERFUL TOGETHER



Introduction

The JTC Group takes your privacy seriously. Please read this privacy notice carefully as it contains important information on who we are and how and why we collect, use, retain and share your Personal Data. It also explains your rights in relation to your Personal Data and how to raise a concern. Capitalised terms are defined below.

This privacy notice covers our Processing of Personal Data when you interact with us as an existing or potential client/customer or in relation to a service that we provide to an entity you work for or are connected to.

Note that this Privacy Notice does not cover Personal Data that we may process on behalf of our clients or customers as part of the services we provide to them (such as Administration Services we provide to a Fund in which you are an investor) where we are not the Controller of the Personal Data. We cannot erase your Personal Data or provide you with details of the Personal Data held about you in relation to those services without an instruction to do so from our customer, so please contact them in the first instance.

When we collect, use or are responsible for Personal Data about you, we are subject to Data Protection Laws.

1. Defined Terms

Data Subject means the person to whom the Personal Data relates.

Data Protection Laws means all applicable laws and regulations relating to the processing of personal data by JTC.

DPGO means the Director (Data Privacy Governance Officer).

JTC or the JTC Group means the JTC group of companies as set out in its Terms of Business, which can be found on the JTC Group website. When we mention 'we', 'us' or 'our' in this privacy notice, we are referring to the JTC corporate entity controlling your Personal Data.

Personal Data under the Data Protection Laws means any information that identifies or could identify you. In certain jurisdictions it is referred to as 'personal information'.

Processing means any operations performed on Personal Data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special Category Data means Personal Data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs, trade union membership, genetic and biometric data (when processed to identify an individual uniquely), data concerning health, sex life or sexual orientation, and in Jersey and Guernsey, criminal records or alleged criminal conduct.

2. Personal Data We Process About You

We will never Process Personal Data outside of reasonable expectations. Depending on the nature of our interaction with you, our Processing encompasses:



- contact information, including your postal address, email address(es), telephone number(s), company details and where applicable, social media contact information;
- identity information, including your current and former names, gender, date and place of birth, nationality, passport information, and birth certificate;
- preference information, including dietary restrictions, preferred correspondence language, etc.
- verification information, including government-issued documents, bank statements, signatures, images and utility bills;
- taxation information, including domicile, tax identification number, tax returns and tax advice;
- source-of-wealth information, including pension plans, property sale documentation and loan documents;
- financial information, including, bank account information, assets held and on what basis (eg legal/beneficial ownership, etc);
- trusts information (if applicable), including settlor details and letters of wishes;
- employment information;
- criminal records or allegations information, including details of any official body's investigation of you and sanctions applying against you;
- insolvency/bankruptcy/en desastre information (as applicable);
- debtor information;
- connected-persons information, including familial relationships;
- politically exposed person information or senior public figure information, including your political activities and relationships;
- health or medical information, including whether you are suffering from a disability that may require us to adjust how we distribute trust assets;
- religious beliefs, including where these impact the type of service we may be able to provide (e.g. services that adhere to sharia principles)
- information in the public domain;
- correspondence between you, your agents/representatives, and us;
- billing, transaction and payment information; and
- technical data, including information about how you use our website, IT, communication and other systems. Further information on how we process cookies data can be found [here](#).

We collect and use this Personal Data to provide services to you or to communicate with you. If you do not provide Personal Data we ask for, it may delay or prevent us from providing such services to you.

3. How We Collect Your Personal Data

We collect most of this Personal Data directly from you—in person, by telephone, video call, text or email and/or via our website. However, we may also collect information from:



- publicly accessible sources, eg the Jersey Financial Services Commission Registry, Companies House, news outlets, websites and other media sources; international sanctions lists.
- settlors, interest holders or other types of clients who engage our services on your behalf (e.g. your employer for an employment related share plan);
- sanctions screening providers;
- customer due diligence providers, eg World Check;
- agents / investigators we engage to help us locate beneficiaries, settlors or other parties we have lost contact with.
- professional suppliers.
- a third party with your consent, eg your bank or building society, intermediaries or lawyers.
- cookies on our website
- marketing directories or platforms, e.g. Zoom Info, Prequin.
- event providers where you are attending an event we are hosting or sponsoring.
- third parties/third party systems that you provide your personal data to for processing on our behalf (e.g. Electronic ID Verification systems)
- other JTC Group companies, for example where you receive another service from JTC.
- our IT systems, eg:
- from door entry systems and reception logs; and
- through automated monitoring of our websites and other technical systems, such as our computer networks and connections, CCTV and access control systems, communications systems, email and instant messaging systems.

We may from time to time record telephone calls.

4. How And Why We Use Your Personal Data

Under Data Protection Laws, we can only use your Personal Data if we have a proper reason, including:

- where you have given consent;
- to comply with our legal and regulatory obligations;
- for the performance of a contract with you or to take steps at your request before entering into a contract;
- in the substantial public interest;
- to protect your vital interests; or
- where applicable, for our legitimate interests or those of a third party.

A legitimate interest is when we have a business or commercial reason to use your non-sensitive Personal Data, so long as this is not overridden by your own rights and interests. We will carry out an assessment when relying on legitimate interests, to balance our interests against your own.



Where our basis for Processing your Personal Data is your consent, you can withdraw such consent without penalty. For consent to receive marketing communications, this can be done by updating your preferences on our preference centre or clicking the unsubscribe button at the bottom of an email communication.

Alternatively, you can use the contact details set out below to notify us that you wish to withdraw your consent. Withdrawal of your consent will not affect the lawfulness of the processing based on consent before its withdrawal.

The table below further explains what we use your Personal Data for and why.

What we use your Personal Data for	Our Lawful Basis / reasons and interests
Providing funds administration, trusts services or other agreed services to you or for your benefit.	To perform our contract with you or to take steps at your request before entering into a contract Where the contract is not with you, our legitimate interest in providing a service that a related party has requested for your benefit (e.g. where you are the beneficiary of a trust)
Preventing, detecting, investigating, prosecuting and reporting fraud or other unlawful financial activity against you or us (including identity verification exercises and authentication).	Our legitimate interest to minimise fraud or other unlawful financial activity that could be damaging for you and/or us. In some circumstances, we may not have a direct legal obligation to undertake these activities, however, we may assess that it is nonetheless in our legitimate interest to do so. For example, where it is necessary to comply with our internal policies as a regulated business. Equally, where the legal or regulatory obligation is not an EU Law (or law recognised by the applicable Data Protection Law) but it nonetheless applies to JTC, we will rely on our legitimate interest to process personal data for these purposes.
Conducting checks to identify our customers and verify their identity.	To comply with our legal and regulatory obligations such as legislation relating to anti-money laundering, Combating the Financing of Terrorism or Countering Proliferation Financing.
Screening for financial and other sanctions or embargoes.	In some circumstances, we may not have a direct legal obligation to undertake these activities, however, we may assess that it is nonetheless in our legitimate interest to do so. For example, where it is necessary to comply with our internal policies as a regulated business. Equally, where the legal or regulatory obligation is not an EU Law (or law recognised by the applicable Data Protection Law) but it nonetheless applies to JTC, we will rely on our legitimate interest to process personal data for these purposes.
Other activities necessary to comply with professional, legal and regulatory obligations that apply to our business, eg under health and safety law or rules issued by our regulators.	In some circumstances, we may not have a direct legal obligation to undertake these activities, however, we may assess that it is nonetheless in our legitimate interest to do so. For example, where it is necessary to comply with our internal policies as a regulated business. Equally, where the legal or regulatory obligation is not an EU Law (or law recognised by the applicable Data Protection Law) but it nonetheless applies to JTC, we will rely on our legitimate interest to process personal data for these purposes.
Gathering and providing information required by or relating to audits, enquiries or investigations by governmental or regulatory bodies or authorities or law enforcement. This includes	To comply with our legal and regulatory obligations such as obligations imposed on us by virtue of operating regulated services.



providing information (including the names of ultimate beneficial owners or controllers in some instances) to authorities so that they can make this information available for public inspection.	In some circumstances, we may not have a direct legal obligation to provide information to such bodies, however, we may assess that it is nonetheless in our legitimate interest to do so. For example, where law enforcement have requested information to assist with a criminal investigation but have not issued a warrant. Equally, where the legal or regulatory obligation is not an EU Law (or law recognised by the applicable Data Protection Law) but it nonetheless applies to JTC, we will rely on our legitimate interest to process personal data for these purposes.
Operating IT systems, software and business applications.	To perform our contract with you and provide agreed services to you in a safe and efficient manner.
Ensuring security and internet use policies are adhered to.	Our legitimate interest to make sure we are following our own internal procedures so we can deliver the best service to you.
Operational reasons, such as improving efficiency, training and quality control.	Our legitimate interest to be as efficient as we can so we can deliver the best service to you at the best price.
Ensuring the confidentiality of commercially sensitive information.	Our legitimate interest to protect trade secrets and other commercially valuable information.
Statistical analysis to help us manage our business, e.g. in relation to our financial performance.	Our legitimate interest to be as efficient as we can so we can deliver the best service to you at the best price.
Preventing unauthorised access and modifications to systems.	Our legitimate interest to prevent and detect criminal activity that could be damaging for you or us. To comply with our legal and regulatory obligations such as those imposed by Data Protection Laws or by virtue of providing regulated services.
Client/customer communication and relationship management	To perform our contract with you or to take steps at your request before entering into a contract. Our legitimate interest to make sure that we can keep in touch with our clients and customers about existing services or to update our records.
To prepare and disclose statutory and tax returns or other documents related to tax or regulatory reporting.	To comply with our legal and regulatory obligations such as the Companies Law. In some circumstances, we may not have a direct legal obligation to undertake these activities, however, we may assess that it is nonetheless in our legitimate interest to do so. For example, where it is considered to be in the best interests of our client or beneficiaries. Equally, where the legal or regulatory obligation is not an EU Law (or law recognised by the applicable Data Protection Law) but it nonetheless applies to JTC, we will rely on our legitimate interest to process personal data for these purposes.
Ensuring safe working practices, staff administration and assessments.	To comply with our legal and regulatory obligations such as Health and Safety legislation or Anti-Bribery regulations.



	Our legitimate interest to make sure we are following our own internal procedures and working efficiently so we can deliver the best service to you.
Marketing our services and those of selected third parties to: <ul style="list-style-type: none"> • existing and former customers; • prospective customers who have previously expressed an interest in our services; • prospective customers with whom we have had no previous dealings. 	<p>Consent</p> <p>Where consent is not required, our legitimate interest to promote our business to existing and future clients.</p>
External audits and quality checks, e.g. for ISO accreditations and the audit of our accounts.	<p>Our legitimate interest to maintain our accreditations so we can demonstrate we operate at the highest standards.</p> <p>To comply with our legal and regulatory obligations such as those imposed by virtue of providing regulated services.</p>
Conducting surveillance over electronic/telephonic communication; recording CCTV footage.	Our legitimate interest to assure service quality, for training, to detect and prevent potentially unlawful conduct.
To establish, enforce or defend rights for example to obtain advice on obligations whether to make a regulatory disclosure.	Our legitimate interest to ensure our rights and the rights of those under our scope of responsibility are protected.
To liaise with governmental or regulatory authorities and courts.	To comply with a legal obligation imposed on us by virtue of providing regulated services and to ensure we meet our reporting obligations and commitment to government agencies which have jurisdiction.
To disclose information in order to comply with any shareholder identification and disclosure requests received from third parties such as banks or intermediaries.	<p>To comply with our legal and regulatory obligations such under market abuse regulations or where we are subject to a reliance arrangement with a bank that you have requested we share personal data with.</p> <p>In some circumstances, we may not have a direct legal obligation to provide information to such third parties, however, we may assess that it is nonetheless in our legitimate interest to do so. For example, where it is necessary for other entities within a structure we are trustee for to meet their legal regulatory requirements. Equally, where the legal or regulatory obligation is not an EU Law (or law recognised by the applicable Data Protection Law) but it nonetheless applies to JTC, we will rely on our legitimate interest to process personal data for these purposes.</p>
To disclose information with third parties that our client has requested us to establish a relationship with such as a financial institution, law firm, advisor, family officer, security issuer,	Our legitimate interest to provide an efficient and comprehensive service to our clients and comply with our client's directions where we consider it appropriate to do so.



company or other person in the JTC Group that are not directly related to the trust services we provide.

To comply with any duty to account or other duty imposed on us by a Trust deed or instrument.

Our legitimate interest to ensure our duties as trustees are properly exercised even after our contract has ended (e.g. because the settlor has died).

Where we Process your Special Category Data, we will also ensure we are permitted to do so under the Data Protection Laws. In most instances the purpose for processing your Special Category Data will be in order to conduct anti-money laundering or sanctions checks (which may require us to process your political opinions, race/ethnicity or your criminal record/alleged criminal activity). Our lawful basis in these instances is that the processing is necessary for reasons of substantial public interest to prevent unlawful acts including money laundering and financing terrorism.

We may also process your Special Category Data in some circumstances where it is necessary in order to carry out our services to or for you. For example, where you have requested that we make an early distribution from a trust on the grounds of ill-health and we, as Trustees, need to establish that the request meets the rules of the trust. In these instances, we will be processing your Special Category Data because it is necessary for the establishment, exercise or defend a legal claim or with your explicit consent. Where it is not possible for us to obtain your consent (e.g. due to incapacity), we may process your Special Category Data in order to protect your vital interests where it is deemed necessary.

If it is necessary to process your Special Category Data for another purpose, we will ensure we can rely on one of the following legal bases:

- we have your explicit consent
- we need to comply with a legal obligation in the field of employment, social security or social protection law
- we need to protect your (or someone else's) vital interests where you are physically or legally incapable of giving consent
- you made the personal data public
- we need to establish, exercise or defend legal claims;
- for the purposes of preventive or occupational medicine or for archiving purposes.

If you choose not to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing you with the information you have requested), or we may be prevented from complying with our legal obligations (such as performing anti-money laundering checks). This may mean we are unable to provide a service you (or the entity you work for/are related to) have requested.

5. Marketing

We may use your Personal Data to send you updates (by email, text message, telephone or post) about our services, including exclusive offers, promotions or new services.



You have the right to opt out of receiving marketing communications at any time by contacting us at digital@jtcgroup.com. You can also select your topic of interests for future communication using our Preference Centre link or opt-out from all future marketing communications via unsubscribe link. Both of these can be found in marketing emails which we send you.

We may ask you to confirm or update your marketing preferences if you ask us to provide further services in the future, or if there are changes in the law, regulation, or the structure of our business.

We will always treat your Personal Data with respect and never sell or share it with other organisations outside JTC's group for marketing purposes.

If you sign up to an event that we are hosting, we may share your contact details with the sponsors of that events so that they can contact you about the event and their services. If you do not wish for your personal data to be shared for this purpose, you can click the opt-out button at the time that you register for the event or contact us at digital@jtcgroup.com or using the contact details set out below.

6. With Whom We Share Your Personal Data

In certain circumstances, we may need to share your Personal Data with other companies or individuals. We are very careful about the third parties with whom we share your Personal Data and we ensure that we only share the minimum amount of information that is necessary.

Where necessary in order to fulfil the purposes set out above, we share your Personal Data with the following types of recipient:

- Other members of the JTC Group and staff of those group entities who have a need to know your personal data such as compliance officers, anti-money laundering officers or data privacy governance officers.
- KYC Screener providers or Electronic ID Verification Service providers
- Email and document storage providers
- Client data management system providers
- Customer Relationship Management system providers
- Marketing agencies or directories
- Website hosting providers;
- Organisations with whom we co-host marketing events;
- IT service or telecommunication providers
- professional advisors, including lawyers, regulatory specialists, and tax advisers;
- our insurers and banks;
- intermediaries or other professional advisers, agents or third parties providing services in relation to a matter for which JTC is providing services;
- third parties you approve or instruct us to share personal data with, eg social media sites you choose to link your account to or third party payment providers;



- successor service providers e.g. other trustees who take over a trust or a third-party structure that takes ownership of assets
- government or regulatory agencies to whom we have a disclosure obligation; and
- competent courts and tribunals who issue an order with which we are obliged to comply.

We only allow our service providers to handle your Personal Data if we are satisfied they take appropriate measures to protect it. We also impose contractual obligations on service providers to ensure they can only use your Personal Data to provide services to us and to you.

On occasion we may also need to:

- share Personal Data with external auditors, eg in relation to ISO accreditation and the audit of our accounts;
- disclose and exchange information with law enforcement agencies and regulatory bodies to comply with our legal and regulatory obligations; and
- share some Personal Data with other parties, such as potential buyers of some or all of our business or during a restructuring—usually, information will be anonymised but this may not always be possible, however, the recipient of the information will be bound by confidentiality obligations.

If you would like more information about who we share our data with and why, please contact us (see ‘How to contact us’ below).

7. Where Your Personal Data Is Held

Personal data may be held at our offices and those of our group companies, third party agencies, service providers (including CRM systems and servers), representatives and agents as described above (see above: ‘Who we share your Personal Data with’). For a list of the locations of our offices, please see Offices – JTC. JTC is headquartered in Jersey in the Channel Islands, so your personal data will be held on our servers in Jersey.

Some of these third parties may be based outside the jurisdiction where you reside. For more information, including on how we safeguard your Personal Data when this happens, see below: ‘Transferring your Personal Data abroad’.

8. How Long We Will Keep Your Personal Data

The length of time we will retain your personal data will depend on the purpose for which it was collected. If you are a previous or existing customer, we will keep your Personal Data while you have a relationship with us or we are providing services to you or for your benefit. If your personal data was collected in order for us to comply with a legal obligation, we will retain it for the length of time required by that legal obligation. If you are a potential customer, we will keep your Personal Data for three years from the date of your last interaction with us.

We will then keep your Personal Data only for as long as necessary:



- to respond to any questions, complaints or claims made by you or on your behalf;
- to show that we treated you fairly;
- to keep records required by law.

Further details on this can be requested using the contact details below.

When it is no longer necessary to keep your Personal Data, we will delete or anonymise it.

Where personal data is processed solely with your consent, it shall be processed until you ask JTC to stop, and for a reasonable period afterwards to allow JTC to comply with your request, unless another legal justification permits continued processing.

9. Transferring Your Personal Data Abroad

To deliver services to you, it is sometimes necessary for us to share your Personal Data abroad, eg:

- with our offices or other companies within our Group (for a list of the locations of our offices, please see Offices – JTC);
- with your and our service providers located abroad;
- if you are based in another jurisdiction from where we are;
- where there is an international dimension to the services we are providing to you.

We only transfer your Personal Data from jurisdictions whose local data protection laws contain restrictions on transferring personal data to third countries (including the British Islands, the UK, Switzerland, Dubai, the Cayman Islands and the European Union) where the transfer is compliant with the local Data Protection Law. This may be achieved by using one of the following transfer mechanisms, as is most appropriate in the circumstances:

- the recipient jurisdiction is a member of the European Union and/or the European Economic Area;
- the recipient jurisdiction ensures an adequate level of data protection, as determined by the European Commission (and/or relevant local data protection authority).;
- there are appropriate safeguards in place, such as approved ‘standard contractual clauses’ recognised by the local data protection authority together with enforceable rights and effective legal remedies for data subjects; or
- a specific exception applies under the Data Protection Laws.

All personal data exchanged between JTC Group entities is subject to an intra-group data sharing agreement which contains standard contractual clauses where applicable. A number of our Group entities are also located in jurisdictions which are deemed adequate by the European Commission including Jersey, Guernsey, the UK, the Isle of Man and Switzerland.



9.1 Further information

The exact locations where your personal data will be transferred will depend on the international dimension of the service being provided to you. For example, if you have asked us to set up an entity in the Bahamas, some of your personal data may be transferred to the Bahamas for registration and tax purposes.

If you would like further information about data transferred abroad, please contact our Director (Data Privacy Governance Officer) Legal (see 'How to contact us' below).

10. Eu Representative

To the extent that we are not established in the European Union, we have appointed an EU representative. This is JTC Data Services (Europe) Sarl. Any changes to the identity of this representative will be reflected in this privacy notice.

11. Your Rights Under Eu Data Protection Laws

If you are resident in the EU (or a jurisdiction which has adopted EU Data Protection Laws or the equivalent rights of EU Data Protection Laws, such as Jersey, Guernsey and the Cayman Islands) you may have the following rights, which you can exercise free of charge by using the contact details set out below:

Access	The right to know what personal data we hold about you and be provided with a copy of your Personal Data
Rectification	The right to require us to correct any mistakes in your Personal Data
Erasure (also known as the right to be forgotten)	The right to require us to delete your Personal Data—in certain situations
Restriction of processing	The right to require us to restrict processing of your Personal Data in certain circumstances, eg if you contest the accuracy of the data
To object	<p>The right to object:</p> <ul style="list-style-type: none">• at any time to your Personal Data being processed for direct marketing (including profiling);• in certain other situations to our continued processing of your Personal Data, eg processing carried out for the purpose of our legitimate interests
Not to be subject to automated individual decision making	The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you or similarly significantly affects you
Data Portability	The right to ask that we transfer the Personal Data you have provided to us to another organisation, in a machine-readable format, where technically feasible. The right only applies in certain circumstances and is not applicable under for residents of the Cayman Islands

Generally, we will have up to four weeks to respond to your request, but in limited circumstances where a request is complex, this period can be extended by a further eight weeks. In essence, the more targeted a request is, the quicker we will be able to assist you.

Please see the relevant Addendum to this Privacy Notice for details of the alternative rights that may apply to you under the non-EU Data Protection Laws that apply to the JTC Group.



12. Keeping Your Personal Data Secure

We have appropriate organisational and technical security measures to prevent Personal Data from being accidentally lost, or used or accessed unlawfully. We limit access to your Personal Data to those who have a genuine business need to access it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable supervisory authority of a suspected data protection breach where we are legally required to do so.

13. How To Raise A Concern

We encourage you to contact us directly if you have any query or concern about our use of your Personal Data (see below 'How to contact us'). We hope we can resolve any issues you may have.

You can also complain to the data protection supervisory authority where you reside, work or where you think an infringement took place. You can ask us if unsure of their contact details.

14. Accuracy Of Personal Data

Where you provide Personal Data to us (whether Personal Data of yourself or which relates to another individual), you acknowledge that we are entitled to regard such Personal Data as being complete, accurate and up to date. You also undertake to let us know without undue delay if there are changes to the Personal Data that you have provided us with so that the Personal Data in our possession remains complete, accurate and up to date.

15. Changes To This Privacy Notice

This privacy notice was last updated on 14 May 2025.

We may update this privacy notice from time to time. We will use commercially reasonable methods to notify you of such revisions, such as by posting a revised version of the Privacy Notice on our website. Your continued access to or use of our website, or provision of Personal Data to us after such notice had been given and such revised Privacy Notice had come into effect shall constitute your acceptance of the revised Privacy Notice.

Previous versions of the notice are available here:

[August 2024](#)

[February 2023](#)



16. How To Contact Us

You can contact our Data Privacy Governance Officer (DPGO) by post, email or telephone if you have any questions about this privacy policy or the information we hold about you, to exercise a right under the Data Protection Laws or to make a complaint.

Our contact details are shown below:

Our contact details	Our DPGO's contact details	Our EU Rep's contact details
PO Box 1075 JTC House 28 Esplanade St Helier JE4 2QP	C/- JTC House Jersey +44 1534 700 000 privacy@jtcgroup.com	JTC Data Services (Europe) Sarl 68-70 Boulevard de la Pétrusse L-2320 Luxembourg

+44 1534 700 000

<https://www.jtcgroup.com/contact/>

Alternatively, our Data Protection Officer contact details for those jurisdictions where we are required to appoint one are set out below:

Region	DPO contact details
Singapore	SingaporeDataPrivacy@jtcgroup.com
Mauritius	MauritiusDataPrivacy@jtcgroup.com
Dubai	UAEDataPrivacy@jtcgroup.com

16.1 Do you need extra help?

If you would like this notice in another format, please contact us (see 'How to contact us' above).

Singapore Addendum

Introduction



This Singapore Addendum (“Singapore Addendum”) applies to you if we Process your Personal Data in Singapore for the purposes stated in this Privacy Notice.

Where there is any inconsistency between this Singapore Addendum and the main body of the JTC Group Client Privacy Notice, this Singapore Addendum will prevail to the extent of that inconsistency.

Unless otherwise expressly stated, all terms in this Singapore Addendum have the same meaning as defined in the main body of this Privacy Notice or as otherwise defined in the Singapore Personal Data Protection Act 2012 (“PDPA”).

When we use the term “Personal Data” in this Singapore Addendum, we mean data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access.

1. Lawful Basis For Processing

By accessing or using our website, interacting with us in relation to our services, or otherwise providing us with your Personal Data, you hereby acknowledge that you have read and understood this Privacy Notice and Singapore Addendum, and expressly consent to our collection, use, disclosure, transfer, storage, retention or otherwise processing your Personal Data for the purposes as described/disclosed in this Privacy Notice and Singapore Addendum. If you do not agree with any terms of this Privacy Notice or Singapore Addendum, you should not access or use our websites and services, or otherwise provide any Personal Data to us.

Where our basis for Processing your Personal Data is your consent, you can withdraw such consent without penalty. For consent to receive marketing communications, this can be done by updating your preferences on our preference centre or clicking the unsubscribe button at the bottom of an email communication. Alternatively, you can use the contact details set out below to notify us that you wish to withdraw your consent. Withdrawal of your consent will not affect the lawfulness of the Processing based on consent before its withdrawal.

While we respect your decision to withdraw your consent, please note that if you withdraw your consent to the Processing of your Personal Data, it may prevent us from providing our services to you.

Please note that withdrawing your consent does not affect our right to continue to Process your Personal Data where such Processing without consent is permitted or required under the applicable Singapore laws.

2. Your Rights Under The PDPA

You have the following rights in respect of your Personal Data in our possession or under our control, subject to certain exceptions under the applicable Singapore laws. You can exercise your rights free of charge by using the contact details set out below.

Access

The right to access Personal Data about you that is in our possession or under our control, and information about how the Personal Data was used or disclosed by us within one (1) year prior to the date of your request



Correction	The right to request for us to correct an error or omission in your Personal Data that is in our possession or under our control @jtcgroup.com
Withdraw Consent	The right to withdraw any consent given, or deemed to have been given to us, in respect of the Processing of your Personal Data by us for any purpose

We will respond to your request within the time frame stipulated in the PDPA, its subsidiary regulations and/or the Singapore Personal Data Protection Commission's guidelines. In the event that we are unable to respond to your request within the stipulated time frame, we will inform you in writing. Generally, the more targeted a request is, the quicker we will be able to assist you.

Please note that notwithstanding any exercise of the rights described above by you, we may continue to Process your Personal Data where we are permitted or required to do so under the applicable Singapore laws.

3. Data Protection Officer

You can contact our DPGO by post, email or telephone if you have any questions about this Privacy Notice, this Singapore Addendum or the Personal Data we hold about you, to exercise a right under the PDPA or to make a complaint. Alternatively, we have appointed a Data Protection Officer in Singapore who is contactable at SingaporeDataPrivacy@jtcgroup.com

Switzerland Addendum



Introduction

This Switzerland Addendum ("Switzerland Addendum") applies to you if we Process your Personal Data in Switzerland for the purposes stated in this Privacy Notice.

Where there is any inconsistency between this Switzerland Addendum and the main body of the JTC Group Client Privacy Notice, this Singapore Addendum will prevail to the extent of that inconsistency.

Unless otherwise expressly stated, all terms in this Switzerland Addendum have the same meaning as defined in the main body of this Privacy Notice or as otherwise defined in the Swiss Federal Act on Data Protection ("FADP").

1. Transferring Your Personal Data Out Of Switzerland

In the event we transfer your Personal Data to a location outside Switzerland, we will take appropriate measures, in compliance with the FADP, to ensure that your transferred Personal Data is accorded a standard of protection that is comparable to that under the FADP. This includes ensuring that recipient countries are included on the list of countries deemed to have adequate data protection as published by the Swiss government from time to time or ensuring that our contract with the recipient contains standard contractual clauses approved by the Federal Data Protection and Information Commissioner.

The exact locations where your personal data will be transferred will depend on the international dimension of the service being provided to you. For example, if you have asked us to set up an entity in the Bahamas, some of your personal data may be transferred to the Bahamas for registration and tax purposes.

If you would like further information about data transferred abroad, please contact our Director (Data Privacy Governance Officer) Legal (see 'How to contact us' below).

2. Your Rights Under The FADP

In addition to the rights mentioned in the JTC Group Client Privacy Notice, you may request that a note of contest is added in case if neither the accuracy nor the inaccuracy of the Personal Data in question can be established.

