



JTC Group *Client Privacy Notice*

October 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 prospective 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 as Controller, 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.

If you provide JTC with Personal Data relating to another person, please ensure you draw their attention to this Privacy Notice, so that they are aware of how their information will be handled.

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 JTC's 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 means any information that identifies or could identify you (or has such different meaning as is set out in the applicable Data Protection Law). In certain jurisdictions it is referred to as 'Personal Information' or 'Personally Identifiable 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 under some Data Protection Laws, 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. This may also include biometric data where verification is being undertaken electronically but this information is retained by our Electronic ID Verification provider and not shared with JTC;
- taxation information, including domicile, tax identification number, tax returns and tax advice;
- source-of-wealth information, including inheritance events, 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;
- bankruptcy/en desastre or other personal insolvency 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 communicate or distribute 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 the Personal Data requested, 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, in writing, by telephone, video call, text or email and/or via our website. However, we may also collect information from:

- publicly accessible sources, e.g. companies registries, gazettes, news outlets, websites and other media sources; international sanctions lists;
- settlors, family members, 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, e.g. World Check;
- agents / investigators that we engage to help us locate beneficiaries, settlors or other parties with whom we have lost contact;
- professional suppliers;
- a third party with your consent, e.g. 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 that we are hosting or sponsoring;
- third parties/third party systems to whom you provide your personal data for processing on our behalf (e.g. Electronic ID Verification systems);
- other JTC Group companies where, for example, you receive another service from JTC;
- our IT systems, e.g. network monitoring;
- 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 or video calls.

4. How And Why We Use Your Personal Data

In compliance with Data Protection Laws, we only use your Personal Data if we have a legitimate business purpose and/or lawful basis, including:

- where you have given consent;
- to comply with our legal and regulatory obligations;
- for the performance of a contract with you or an entity or arrangement associated with you, or to take steps at your request before entering into a contract;
- in the 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 reason is not overridden by your own rights and interests. We will carry out an assessment when relying on legitimate interest, to balance our interests against your own.

4.1 *Withdrawing Consent*

Where our basis for Processing your Personal Data is your consent, you can withdraw such consent without penalty. Consent to receive marketing communications can be given or withdrawn by updating your preferences on our preference centre. It can also be withdrawn by 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.

4.2 *Legal Basis for Processing*

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

What we use your Personal Data for	Our Lawful Basis / Business Purpose
Providing funds administration, trusts services or other agreed services to you at your instruction or otherwise 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 circumstances where we may not have a direct legal obligation to undertake these activities, 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 or to ensure consistency of approach. 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.	



Other activities necessary to comply with professional, legal and regulatory obligations that apply to our business, e.g. under Health and Safety legislation or rules issued by our regulators.

In circumstances where we may not have a direct legal obligation to undertake these activities, 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 or to ensure consistency of approach. 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.

Where we are verifying your identity as part of an identity verification service that we are providing to you or the entity that you represent (e.g. verification services provided by JTC as an Authorised Corporate Service Provider of Companies House), our lawful basis will be performance of contract.

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 providing information (including the names of ultimate beneficial owners or controllers) to authorities so that they can make this information available for public inspection.

To comply with our legal and regulatory obligations such as obligations imposed on us by virtue of operating regulated services.

In circumstances where we may not have a direct legal obligation to undertake these activities, 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 obtained a warrant or other court order. 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 secure 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 that we can deliver the best service to you at the best price.

Ensuring the confidentiality of commercially sensitive information (such as to manage access controls and audit actions taken by users of our systems).

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 that 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, regulatory and tax returns or other documents related to statutory, regulatory or tax reporting.	To comply with corporate legislation and our legal and regulatory obligations. In circumstances where we may not have a direct legal obligation to undertake these activities, 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, Whistleblowing 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: • 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.	Consent Where consent is not required, our legitimate interest to promote our business to existing and future clients.
External audits and quality checks, e.g. for ISO accreditations and the audit of our accounts.	Our legitimate interest to maintain our accreditations so we can demonstrate we operate at the highest standards. To comply with corporate legislation and with our legal and regulatory obligations such as those imposed by virtue of providing regulated services.
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, intermediaries or competent authorities.	To comply with our legal and regulatory obligations such as market abuse regulations or where we are subject to a reliance arrangement with a bank that you have requested that we share personal data with. In circumstances where we may not have a direct legal obligation to undertake these activities, 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 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.
To disclose information to third parties with whom our client has requested us to establish a relationship such as a financial institution, law firm, advisor, family officer, security issuer, company or other entity within the JTC Group that are not directly related to the services we provide.	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.
To comply with any duty to account or other duty imposed on us as trustees e.g. 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).
To trace you as may be reasonably necessary (for example, if the contact details you have provided to us are no longer correct), to trace debtors and enforce or seek to obtain settlement of amounts owing to us.	Our legitimate interest in being able to recover monies that are owed to us.
To carry out market research and to identify trends. Market research agencies acting on our behalf may get in touch with you by post, telephone, email or other medium to invite you to take part in research.	Our legitimate interest in obtaining feedback in order to improve our brand and/or services.

4.3 Special Category Data

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 or religious opinions, race/ethnicity or your criminal record/alleged criminal activity). Our lawful basis in these



instances is that the processing is necessary to comply with Anti-Money Laundering, Combating the Financing of Terrorism or Countering Proliferation Financing requirements and for reasons of substantial public interest to prevent unlawful acts.

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 pension trust on the grounds of ill-health and we, as trustee, 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 defence of 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 assess and 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 Special Category Data public or agreed to it being made public
- we need to establish, exercise or defend legal claims;
- for the purposes of preventive or occupational medicine or for archiving purposes.

4.4 Consequences of failing to provide Personal Data

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 advancing payments to 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 to you (or the entity with which you are associated).

4.5 Consent-based Data Protection Regimes

If you are resident in a jurisdiction where consent is required in order for JTC to process your Personal Data (such as Singapore), you hereby acknowledge that you have read and understood this Privacy Notice 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. If you do not agree with any terms of this Privacy Notice, you should not access or use our websites and services, or otherwise provide any Personal Data to us.

By accessing or using our website, interacting with us, requesting or using our services or otherwise providing us with your Personal Data, you consent to JTC using your Personal Data as described. If you share another person's Personal Data with JTC, you must ensure that you have their consent to do so.



Consent can be withdrawn at any time using the procedure set out above (see “[4.1 Withdrawing Consent](#)”).

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 law.

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, relevant events, 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 topics of interest for future communication using our [Preference Centre link](#) or opt-out from all future marketing communications via the 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.

If you sign up to attend an event that we are hosting, we may share your contact details with the sponsors of that event or our co-hosts 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.

During marketing events, we may take photographs and videos in which you may appear. These will be used for our legitimate interest in marketing our services such as, but not limited to, social media posts, printed publications or other relevant promotional campaigns. If you do not wish for your image to be used in this way, please endeavour to make this known to the events team prior to being photographed or filmed either by contacting digital@jtcgroup.com or by locating a JTC member of staff at the event.

6. Sharing 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 recipients:

- Other members of the JTC Group and employees of those group entities who have a need to know your personal data, such as legal, risk and compliance officers, anti-money laundering officers or data privacy governance officers;
- KYC (‘Know Your Client’) 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 and educational events;
- IT service or telecommunication providers;
- professional advisors, including lawyers, regulatory specialists and tax advisers;
- our insurers and bankers;
- 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, e.g. social media sites to which you choose to link your account or third party payment providers;
- successor service providers e.g. replacement trustees or a third-party structure that takes ownership of assets;
- governmental, law enforcement 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, e.g. in relation to ISO accreditation and the audit of our accounts;
- disclose and exchange information with law enforcement agencies, governmental and regulatory bodies to comply with our legal and regulatory obligations; and
- share some Personal Data with other parties, such as potential buyers of our business or parties selling their business to ours, or during a restructuring—usually, information will be anonymised but this may not always be possible. The recipient of the information will always be bound by non-disclosure and confidentiality obligations as well as Data Protection Laws.

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 JTC Group offices, third party agencies, service providers (including CRM systems and servers), representatives and agents as described above (see above: [‘Sharing your Personal](#)



Data'). 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.

We will keep your Personal Data while you have a relationship with us or we are providing services to you or for your benefit. 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 or
- to comply with our prevailing data and document retention policy (utilising prudent retention timescales drawn from legal and regulatory requirements or recommendations).

If your Personal Data was collected for marketing purposes, we will keep it for three years from the date of your last interaction with us.

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.

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

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 JTC Group offices in other jurisdictions (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 a different jurisdiction from the JTC Group office providing services;
- where there is an international or multi-jurisdictional 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 Crown Dependencies, 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 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. Many JTC Group entities are also located in EU jurisdictions or 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 a particular jurisdiction, some of your personal data may be transferred to that jurisdiction to allow for registration and tax, compliance and reporting purposes.

If you would like further information about data transferred abroad, please contact our DPGO (see ‘[How to contact us](#)’ below).

10. EU Representative

JTC Group has appointed an EU representative to meet its obligations arising from any processing of any Personal Data of EU or EEA residents by JTC Group entities that are not themselves established in the EU. This representative is a Luxembourg company, JTC Data Services (Europe) Sàrl. Any changes to the identity of this representative will be reflected in this privacy notice.

11. Your Rights Under Data Protection Laws

GDPR /Equivalent Data Protection Law

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 the Crown Dependencies 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 ('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, e.g. if you contest the accuracy of the data
To object	The right to object: • 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, e.g. 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 for residents of the Cayman Islands

Generally, the applicable Data Protection Laws will allow us 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.

Switzerland

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

Singapore

You have the following rights in respect of your Personal Data in our possession or under our control, subject to certain exceptions under the Singapore Personal Data Protection Act 2012 ("PDPA"). 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
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 subordinate 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 by you of the rights described above, we may continue to Process your Personal Data where we are permitted or required to do so under the applicable Singapore laws.

California

Please see the [California Addendum](#) to this Privacy Notice for details of your rights under the Californian Consumer Privacy Act.

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 your own Personal Data or Personal Data belonging 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 24 October 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 has come into effect, shall constitute your acceptance of the revised Privacy Notice.

Previous versions of the notice are available here:

May 2025

[August 2024](#)

[February 2023](#)

16. How To Contact Us

You can contact our Data Privacy Governance Officer 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) Sàrl 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	SingaporeDPO@jtcgroup.com
Mauritius	MauritiusDPO@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).



California Addendum

Introduction

This California Addendum (“**California Addendum**”) applies if you are a resident of California and JTC processes your personally identifiable information as a business.

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

Unless otherwise expressly stated, all terms in this California Addendum have the same meaning as defined in the main body of this Privacy Notice or as otherwise defined in Californian Consumer Privacy Act (“**CCPA**”).

1. Your Rights Under This Policy

You have the following rights:

Right to Notice	You must be properly notified which categories of Personal Information are being collected and the purposes for which the Personal Information is being used.
Right to say no to the sale or sharing of Personal Information	You have the right to ask JTC not to sell or share your Personal Information. Please see section 3 below for further details.
Right to Know and Access	You have the right to request and obtain from JTC information regarding the disclosure of the following: • The categories of Personal Information collected • The sources from which the Personal Information was collected • The business or commercial purpose for collecting or selling the Personal Information • Categories of third parties with whom we share Personal Information • The specific pieces of Personal Information we collected about you
Right to Data Portability	You have the right to request a portable copy of your Personal Information.
Right to Delete	You have the right to request the deletion of your Personal Information that has been collected in the past 12 months.
Right to Correct	You have the right to request that JTC correct inaccurate Personal Information collected from you, subject to certain exceptions allowed under applicable law.
Right not to be discriminated against	You have the right not to be discriminated against for exercising any of your consumer’s rights, including by: • Denying goods or services to you • Charging different prices or rates for goods or services, including the use of discounts or other benefits or imposing penalties • Providing a different level or quality of goods or services to you • Suggesting that you will receive a different price or rate for goods or services or a different level or quality of goods or services



2 Exercising Your Privacy Rights

2.1 How to Exercise Your Rights

In order to exercise any of your rights under this Notice please use the contact details set out in the “How to Contact Us” section of this Notice.

You can also contact us using our toll-free telephone number: 1-800-339-1031

2.2 CCPA Authorized Agent

CCPA permits consumers to designate authorised agents to submit requests on their behalf. Under CCPA, an authorized agent is a natural person or a business entity in California that a consumer has authorized to act on his or her behalf subject to the requirements. If you would like to designate an authorized agent to submit a request to know, a request to delete or a request to correct Personal Information on your behalf, please contact JTC’s Group DPGO at privacy@jtcgroup.com. You or your authorized agent may provide us with a written power of attorney, executed by you, confirming the authority of the authorized agent with respect to your CCPA request(s). If we have not received a power of attorney, we may require your authorized agent to provide proof that you gave the agent signed permission to submit your CCPA request(s). In addition, we may also require you to do the following directly with us:

- Verify your own identity with us;
- Confirm you have provided the authorized agent permission to submit the CCPA request(s).

2.3 Verification

Whether you submit a request directly on your own behalf, or through an authorized agent, JTC will take reasonable steps to verify your identity prior to responding to your requests under CCPA. We will notify you upon receipt of your request of the information that you will need to provide in order for us to verify and process your request. This may include providing us with a copy of your identity documents, as well as your full name and email address.

2.4 Response Timing and Format

JTC will disclose and deliver the required information free of charge within 45 days of receiving your verifiable request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary and with prior notice.

We will deliver our written response by mail or electronically, at your option. Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your Personal Information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

3 Additional Disclosures

The CCPA defines a specific list of categories of Personal Information and requires that we indicate each category of Personal Information we collect, why we collect it, where we get it from, and to whom we disclose it for a Business Purpose. Each of these is addressed below.



3.1 Categories of Personal Information Collected and Disclosed in the Previous 12 Months

The categories of Personal Information we have Collected and Disclosed for a Business Purpose about Consumers in the previous 12 months is set out below. For further details on the Personal Information that we disclose for a Business Purpose, see [section 3.3](#) below.

CCPA Category	Collected Data	Business Purpose
Identifiers	Current and former names, familial relationships, postal address, email address(es), telephone number(s), passport information, Social Security Number, Driver's license number	We collect this information to help us identify and authenticate you, for fraud / money laundering prevention and similar purposes We collect contact details as needed to identify you, contact you and do business with you.
Personal Information described in subdivision (e) of s. 1798.80 of the Californian Civil Code	Name, signature, social security number, address, telephone number, passport number, driver's license or state identification card number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information	We collect this Personal Information to help us service your account, as needed to identify you, contact you and do business with you. We collect financial information in order to provide you with the financial products and services you request.
Protected characteristics	Politically exposed person information, senior public figure information, health or medical information, ethnicity, nationality	We collect this information as needed to identify and authenticate you, for fraud / money laundering prevention, and to do business with you.
Commercial information	records of personal property, assets, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies, communications with us related to the foregoing items.	We collect commercial data as needed to service your account and do business with you, and for fraud prevention and similar purposes.
Biometric information	Signature, facial recognition, finger prints	We collect this information for authentication purposes
Internet or other electronic network activity information	Information about how you use our website, IT, communication and other systems, browsing history, search history, and information regarding your interaction with an internet website, application, or advertisement.	We collect online and digital data to personalize our interactions with you and to administer and optimize our websites. We may also use it as part of our authentication processes.
Geolocation data	GPS Location	We collect this information for authentication purposes
Audio, electronic, visual, thermal, olfactory, or similar information.	Call recordings, CCTV footage	We collect this information in order to meet our obligation to maintain a record of your



		instructions and for crime prevention purposes.
Professional or employment-related information	Employment, employment history, and related information	We collect this Personal Information to help us service your account, as needed to identify you, contact you and do business with you.
Sensitive Personal Information *	Social security number, driver's licence, state identification card, passport number, financial accounts, citizenship or immigration status	We collect sensitive personal data with the intention of developing a complete and accurate "Know Your Customer" (KYC) profile in line with regulatory requirements, to identify you, contact you and do business with you.

* Note that we do not use or disclose Sensitive Personal Information for any purpose other than providing our services to you or for your benefit, or as otherwise permitted under applicable law.

3.2 Sources from which Personal Information is Collected

Information about the sources from which Personal Information is collected is set out in the 'How We Collect Your Personal Data' section of the Privacy Notice above.

3.3 Disclosure of Personal Information for a Business Purpose

The reasons that we may need to disclose your Personal Information and the data disclosed in each instance will vary depending on the type of service you are receiving from us. We only disclose the minimum amount of Personal Information to meet the Business Purpose for which the disclosure is necessary in each circumstance. Please contact us if you would like further details about the information we Disclose for a Business Purpose using the contact details set out above.

In general, we disclose Personal Information for the following purposes:

Category of Third Party	Purpose of Disclosure
JTC Group Companies	Data storage, service provision, compliance oversight
Support providers	Support of our internal ancillary processes e.g. general office support, IT functions, Electronic Identity Verification provision (e.g. Jumio)
Business partners e.g. banking/financial service providers,	To support or enhance the service we provide
Professional adviser e.g. law firms, tax advisers	To support or enhance the service we provide or obtain advise necessary for our business
Acquirer or successor of JTC	To facilitate the transfer of services
Regulatory bodies, government authorities, courts and tribunals etc	To help meet statutory disclosure requirements
Event hosts or sponsors	To facilitate an event that you are attending



Further information about the categories of third parties to whom we disclose Personal Information for a Business Purpose is set out in the 'Sharing Your Personal Data' section of this Privacy Notice.

3.5 Categories of Personal Information Sold or Shared in the Previous 12 Months

The categories of Personal Information we have Sold or Shared about Consumers in the previous 12 months is set out below.

Whilst we do not sell Personal Information in the common sense of the word, the following activities we undertake may be considered a "sale" or "sharing" for cross-context behavioural advertising under the CCPA:

- **Third-Party Advertising Companies** - We may disclose or make available Personal Information to third-party platforms and providers to obtain personalized and tailored advertising services, to provide or make available certain features on our website, or as necessary to respond to your requests. For example, we make information collected via cookies and similar technologies on our Platform available to third-party advertising companies to serve you with relevant advertisements and content and to manage, improve and measure our advertising campaigns. This information is limited to IP addresses.
- **Event Sponsors** – We disclose limited Personal Information about attendees of events we are hosting to the sponsors of those events, so that they can contact attendees about their services. This could be considered a "sale" of Personal Information as defined by the CCPA. This information is limited to names, email addresses and job titles.

4 Do Not Sell My Personal Information

If you wish to opt out of the sharing of your Personal Information with event sponsors, you may do so by emailing digital@jtcgroup.com or by clicking on the 'Do not Sell or Share my Personal Information' at the bottom of our website.

In relation to cookies, you may opt out of these uses via the following methods:

4.1 Website

You can opt out of receiving advertisements that are personalized as served by our Service Providers by following our instructions presented on the "Cookie Consent" notice banner. You can access the banner at any time by clicking on the cookie symbol on the bottom left of our website.

This will place a cookie on your computer that is unique to the browser you use to opt out. If you change browsers or delete the cookies saved by your browser, you will need to opt out again.

4.2 Mobile Devices

Your mobile device may give you the ability to opt out of the use of information about the apps you use in order to present advertisements that are targeted to your interests. Please refer to the following on your mobile device:

- "Opt out of Interest-Based Ads" or "Opt out of Ads Personalization" on Android devices
- "Limit Ad Tracking" on iOS devices

You can also stop the collection of location information from your mobile device by changing the preferences on your mobile device.



4.3 “Do Not Track” Policy as Required by California Online Privacy Protection Act (CalOPPA)

Our web page does not respond to “Do Not Track” signals.

However, some third party websites do keep track of your browsing activities. If you are visiting such websites, you can set your preferences in your web browser to inform websites that you do not want to be tracked. You can enable or disable DNT by visiting the preferences or settings page of your web browser.

5 Children’s Online Privacy Protection Act (COPPA)

Our web page does not address anyone under the age of 13. We do not knowingly collect personally identifiable information from anyone under the age of 13 through our website. If you are a parent or guardian and you are aware that your child has provided us with personal data via our website, please contact us. If we become aware that we have collected personal data from anyone under the age of 13 on our website without verification of parental consent, we will take steps to remove that information from our servers.

6 Your Direct Marketing Privacy Rights (California’s Shine The Light Law)

Under California Civil Code Section 1798 (California’s Shine the Light Law), California residents with an established business relationship with us can request information once a year about sharing their personal data with third parties for the third parties’ direct marketing purposes.

If you would like to request more information under the California Shine the Light law, you can contact us using the “How to Contact Us” section of this Notice.

6.1 California Privacy Rights for Minor Users (California Business and Professions Code Section 22581)

California Business and Professions Code section 22581 allows California residents under the age of 18 who are registered users of online sites, services or applications to request and obtain removal of content or information they have publicly posted.

To request removal of such data, and if you are a California resident, you can contact us using the “How to Contact Us” section of this privacy notice and include the email address associated with your account.

Be aware that your request does not guarantee complete or comprehensive removal of content or information posted online and that the law may not permit or require removal in certain circumstances.

7 Links to Other Websites

Our website may contain links to other websites that are not operated by us. If you click on a third party link, you will be directed to that third party’s site. We strongly advise you to review the privacy policy of every site you visit.

We have no control over, and assume no responsibility for, the content, privacy policies or practices of any third party sites or services.

