

Jefferies South Korea Privacy Notice

1. Introduction

This Privacy Notice explains what we do with your personal data. It describes how we collect, use and process your personal data, and how, in doing so, we comply with our legal obligations to you. Your privacy is important to us, and we are committed to protecting and safeguarding your data privacy rights.

This Privacy Notice applies to each of the following who interact with Jefferies Hong Kong Limited, Seoul Branch (whether directly or through an affiliate in the Jefferies Group), their branches and/or subsidiaries (together “we” “our” or “us”): existing and prospective clients, suppliers/vendors, personnel of corporate clients/suppliers/vendors, other persons (excluding employees and job applicants to whom a separate privacy notice applies) and website users whose personal data we may process.

For the purpose of applicable data protection legislation, the company responsible for your personal data is Jefferies Hong Kong Limited, Seoul Branch, the details for which can be found in Section 11.

We may amend this Privacy Notice from time to time. Please just visit this page if you want to stay up to date, as we will post any changes here.

2. What types of personal data do we collect?

We will collect your contact details (name, name of the organization you are from or represent, telephone numbers, job title and email or postal addresses) when you engage with us in connection with our or your services in order to ensure our relationship runs smoothly. Where we are required to carry out verification checks, to comply with our legal and regulatory obligations, we will collect from the company or organization you are associated with, specific additional information about relevant individuals (such as directors and beneficial owners), including, for example, full name, date of birth, gender, address and contact information, payment or account details, tax residence and tax return information, proof of source of wealth and/or assets, copies of photo identification documents (such as a driving licence and/or passport/identity card), information about nationality/citizenship/place of birth, national identification numbers and other identity verification documents. We may also hold information that another person within your organisation has chosen to provide us.

Where existing or prospective corporate clients/vendors provide us with personal data relating to their directors, employees, officers, agents, clients or any other person, such information is deemed to have been provided on the basis that: (i) those individuals have been informed and understand that their personal data is being provided to us or our affiliates; (ii) those individuals have been provided with information regarding the collection, use, processing, disclosure and overseas transfer of their personal data; (iii) the client/vendor has a lawful basis (in accordance with applicable data protection laws and regulations) to provide such personal data to us; and (iv) those individuals are aware of their data protection rights and how to exercise them.

We do not collect or otherwise process sensitive personal data (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data) or criminal conviction/offence data unless it is necessary for compliance with a legal and/or regulatory obligation.

To the extent that you access our website we may also collect certain data from you via cookies, further details of which can be found in Section 10.

3. How do we collect your personal data

3.1 *Personal data that we receive directly from you*

We will receive personal data directly from you in two ways:

- Where you contact us proactively, usually by corresponding with us by phone or email or by filling in forms; and/or
- Where we contact you, either by phone, email, meetings, or through investment activities more generally.

3.2 *Personal data we receive from other sources*

Where appropriate and in accordance with any local laws and requirements, we may seek more information about you or your organisation from other sources by way of due diligence or other market intelligence including:

- From third party data providers and by analysing online and offline media (which we may do ourselves, or employ other organisations to do so for us);
- From delegate lists at relevant events; and/or
- From other limited sources and third parties (for example, from third party brokers and counterparties who may provide us with your details in accordance with any regulatory requirements).

3.3 *Personal information we collect automatically*

To the extent that you access our website or read or click on an email from us, where appropriate and in accordance with any local laws and requirements, we may also collect your data automatically or through you providing it to us. For more information please see Section 10.

4. How do we use your personal data and what is the legal basis?

Having obtained data about you, we then make sure we use it appropriately.

4.1 *Client data*

Investment Activities

If you are a client or prospective client we use the personal data you provide in the following ways:

- storing your details (and updating them when necessary) on our database in order that we can contact you in relation to our ongoing services, agreements or dealings with you, including relevant offerings;
- managing and administering your account or relationship with us (and this may require that we verify information you provide in the course of your onboarding as a client and to carry out credit checks or assessments about you or your directors, officers and employees);
- to carry out our obligations arising from our contracts with you;
- undertaking anti-money laundering and know your client checks in accordance with our legal and regulatory obligations;
- maintaining records of our conversations and meetings so that we can provide relevant services to you and in order to comply with our legal and regulatory obligations;
- for internal analysis and research in order to facilitate the provision of relevant services to you;
- in more unusual circumstances, to help us to establish, exercise or defend legal claims; and
- to comply with legal and/or regulatory requests and requirements.

Relationship Management

- We may use your personal data to contact you to offer you additional services, keep you up to date with business development and market insights or to invite you to events that may be of interest (except where you have asked us not to).
- You have the right to opt out of receiving such communications from us by either liaising with your Jefferies contact or by electronically unsubscribing from emails we have sent you. After you unsubscribe we will not send you such communication emails but may continue to contact you to the extent necessary for the purposes of any services we are providing to you or as may be needed for regulatory purposes.

4.2 *Supplier/Vendor data*

We will use your information:

- To store (and update when necessary) your details on our database, so that we can contact you in relation to our agreements or our dealings with you;
- To obtain support and services from you;
- To perform certain legal and regulatory obligations, such as carrying out anti-money laundering and verification/background checks;
- Facilitating our invoicing and vendor risk management processes; and
- In more unusual circumstances, to help us to establish, exercise or defend legal claims.

4.3 *Our legal basis for processing your personal data*

We will rely on one of the following legal basis:

- Necessary for performance of the contract or to take steps preparatory to such contract;
- Compliance with legal and regulatory obligations that we are subject to in Korea; or
- Legitimate interests pursued by us or a third party to the extent such interests are not overridden by your interests or fundamental rights and freedoms.

Alternatively, we may be required to obtain your consent to the processing of your personal data in which case you will be asked to expressly consent.

We may additionally use or provide your personal data to another party without your consent after considering the below factors:

- Whether the additional use or provision of personal data is related to the original purpose of collection;
- Whether the additional use or provision of personal data is foreseeable in light of the circumstances in which personal data is collected or practices of processing personal data;
- Whether the additional use or provision of personal data unduly infringes on the interests of users; and
- Whether necessary measures have been taken to ensure security, such as pseudonymization or encryption.

We will carefully determine whether to additionally use or provide your personal data by comprehensively taking into account various circumstances, including the applicable laws and regulations such as the Personal Information Protection Act (“**PIPA**”) of the Republic of Korea, the purpose of use and provision of personal data, method of use and provision of personal data, items of personal data to be used and provided, details of the consent you have given or matters notified to or disclosed to you, impact of use and provision of personal data on you, and measures taken to protect your personal data.

5. **Who do we share your personal data with?**

Where appropriate and in accordance with local laws and requirements, we may share your personal data, in various ways and for various reasons, with the following categories of people:

- Affiliates within the Jefferies Group;
- Tax, audit, regulatory bodies or other authorities, when we believe in good faith that the law or other regulation requires us to share this data (for example, because of a request by a tax authority, in connection with any anticipated litigation or in compliance with our legal and regulatory obligations);
- Third party service providers who perform functions on our behalf (including, without limitation, administrators, external consultants, business associates and professional advisers such as lawyers, auditors and accountants, technical support functions and IT consultants carrying out testing and development work on our business technology systems, etc.);
- Third party outsourced IT and document storage providers (including cloud-based storage providers) where we have an appropriate processing agreement (or similar protections) in place; and
- If Jefferies (or a part of its business) is subject to a bid, or otherwise merges with or is acquired by another business or company in the future, we may share your personal data with the new (or prospective) owners of the business or company.

To ensure that your personal information receives an adequate level of protection, we put in place appropriate procedures with the third parties we share your personal data with to ensure that your personal information is treated by those third parties in a way that is consistent with, and which respects, applicable law and regulation on data protection.

Please refer to [Annex A](#) and [Annex B](#) of this document for more information on the parties to whom data is transferred to either through 'third-party provision' or 'delegation' as defined under Korean law.

6. How do we safeguard your personal data?

We are committed to taking all reasonable and appropriate steps to protect the personal data that we hold from misuse, loss, or unauthorised access. We do this by having in place a range of appropriate technical and organisational measures. These include measures to deal with any suspected data breach and training for staff on handling personal data.

Please note you are responsible for ensuring that any personal data that you send to us is sent securely (e.g. encrypting attachments).

We implement the following measures to ensure the security of your personal data, amongst other measures.

Organizational Measures

We have appointed a Chief Privacy Officer (“CPO”) to ensure that data subjects' personal data is processed in conformity with Korean privacy laws.

We will provide personal information protection training for our employees, delegates and others who are directly in charge of processing personal information, as appropriate and practicable.

Technical Measures

We control access to personal data and restrict and manage the access rights. We block the use of removable storage devices such as USBs. Data encryption is applied in storing information on hard disk drives.

We record access rights granted to personal data and retain such records for a certain period of time.

We implement safety measures (including access control function) to prevent any unauthorized access to personal data. In addition, safe access measures, including a virtual private network, are utilized to control access from external sources. For example, connection security between affiliates within the Jefferies group are strengthened by the use of dedicated lines.

We establish and apply password generation rules to enable you to set up and use a secure password if necessary. Upon designating a password to access our information processing system, you must keep the password confidential and must not disclose it to a third party.

We install and periodically update programs to fix security defects in software, including operating systems.

Our global information security team conducts monitoring and vulnerability analysis on a 24 hour basis.

Physical Measures

We take physical access prevention measures, including restrictions on physical access and placing locks, to store personal data kept by way of hard copy in a safe manner.

7. How long do we keep your personal data for?

We will ordinarily process your data throughout the course of our interactions and will then generally retain it for an appropriate amount of time after we have parted ways. The precise length of time will depend on the type of data, our legitimate business needs and other legal or regulatory rules that may require us to retain it for certain minimum periods following the expiration or termination of our contractual relationship. There may also be some legal, regulatory or risk-management requirements to retain data, including where certain data might be relevant to any potential litigation (bearing in mind relevant limitation periods).

Except as otherwise required by law, personal data is securely disposed of without delay when (i) the data subject revokes his or her consent for our use of the data; (ii) the purpose of our collection and use of the personal data has been accomplished; or (iii) the required retention period has expired. Personal data is disposed of using a method that is reasonably likely to prevent the personal data from being restored or reused. We will permanently destroy any personal data recorded and/or saved in electronic format by using a means that can ensure that it cannot be restored and recovered. Personal data printed on paper will be securely destroyed by shredding.

8. How can you access, amend or take back personal data you have provided to us?

Subject to applicable law, you may have various rights in respect of the processing of your data, as listed below.

- *Access:* You may ask us to confirm, and provide copies of, the information we hold about you at any time, and request us to modify, update or delete such information.
- *Erase:* You have the right to request that we erase your personal data in certain circumstances.
- *Restrict Processing:* You have the right to request that we restrict our processing of your personal data in certain circumstances.
- *Rectification:* You also have the right to request that we rectify any inaccurate or incomplete personal data that we process or control.
- *Data Portability:* If you wish, you have the right to transfer your personal data between data controllers. To allow you to do so, we will provide you with your data in a commonly used machine-readable format that is password-protected so that you can transfer the data.
- *Object:* This right enables you to object to us processing your personal data where we do so for one of the following reasons: (i) our legitimate interests; or (ii) to send you relationship management materials for additional products or services.
- *Withdraw Consent:* Where we have obtained your consent to process your personal data for certain activities (for example, for certain relationship management arrangements or any automatic profiling), you may withdraw this consent at any time.

If you would like to exercise any of these rights, including withdrawing your consent to the processing of your personal data (where consent is our legal basis for processing your personal data), details of how to contact us can be found in Section 11. Please note that we may keep a record of your communications to help us resolve any issues which you raise.

In accordance with data protection laws you also have the right to lodge a complaint with your local supervisory authority for data protection. In South Korea this is the Personal Information Protection Commission located at 209, Sejong-daero, Jongno-gu, Seoul, South Korea.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during the period for which we hold your data.

9. How do we store and transfer your data internationally?

In undertaking services for you, your personal data may be transferred to those set out in Section 5.

We want to make sure that your data is stored and transferred in a way which is secure. We will therefore only transfer data outside South Korea where such transfer is compliant with data protection legislation and the means of transfer provides adequate safeguards in relation to your data—i.e., where at least one of the following bases for overseas transfer is present:

- Your separate consent on the data transfer has been obtained;
- There are special provisions regarding the cross-border transfer of personal information in a statute, a treaty to which the Republic of Korea is a party, or other international conventions;
- The overseas transfer takes place in the context of delegation or storage of personal data that is necessary to execute or perform an agreement with you and information in relation to the delegation is disclosed in the privacy policy;
- The recipient of the personal data obtains certification designated by the PIPC; or
- The country or agency that receives personal information has obtained an adequacy decision by the PIPC.

Please refer to the Annex C of this document for more information on the parties to whom data is transferred overseas.

You may have the right to request that your personal data not be transferred overseas. However, if you refuse to give consent, this could affect our ability to provide services or transact with you or your organization. The details of how to contact us can be found in Section 11. Please note that we may keep a record of your communications to help us resolve any issues which you raise.

10. Cookies

We may collect personal data through the use of cookies. A cookie is a small file containing data that is created and stored on your device when you visit a website using a computer or mobile device. When you visit a website, a cookie may be used to track the activities of your browser and provide you with a more consistent and efficient online experience. Tracking your use of our website using cookies enables us to understand how you use the site and track any patterns that emerge individually or from larger groups. This helps us to develop and improve our website and services in response to what our visitors want and need.

We use strictly necessary, performance, functional, targeting and social media cookies on our website. You can view and change your cookie preferences at any time by clicking on the cookie icon on the bottom left-hand side of the screen when you visit our website.

Although you can click the 'reject all' button on our website to opt out of most cookies, please note that our 'strictly necessary' cookies are necessary for the website to function and cannot be turned off in our systems. You can set your browser to block these cookies, but some parts of the site may not work if you do.

The procedure for setting your web browser to block or delete cookies is as follows:

- Chrome: Web browser settings > Privacy and Security > Delete browsing data
- Edge: Web browser settings > Cookies and site permissions > Manage and delete cookies and site data

The procedure for setting your mobile browser to block or delete cookies is as follows:

- Chrome: Web browser settings > Privacy and Security > Delete browsing data
- Safari: Mobile device settings > Safari advanced > Block all cookies
- Samsung internet: Mobile browser settings > Internet browsing data > Delete internet browsing data

11. Jefferies contact details

If you have any comments, questions or concerns about any of the information in this Privacy Notice, or any other issues relating to the processing of personal data by Jefferies Hong Kong Limited, Seoul Branch, please contact our Jefferies Asia Privacy Office by email or post:

APACprivacy@jefferies.com

Jefferies Asia Privacy Office
Level 26, Two International Finance Centre, 8 Finance Street, Central, Hong Kong, China
For the attention of: Head of Asia Legal & Compliance

In order to protect your personal data and handle complaints related to it, we have designated the following Chief Privacy Officer for Jefferies Hong Kong Limited, Seoul Branch: WooHee LEE (woohee.lee@jefferies.com).

Annex A: Provision of personal data to a third-party

We provide personal data to third parties as described below:

Name of Recipient (Contact Information)	Items of Personal Data Provided	Recipient's Purpose of Use	Period of Retention and Use by Recipient	Legal Basis
Jefferies Hong Kong Limited and other offshore affiliates' investment banking division ¹	Name, address, phone numbers, email address, employer name, title, and employment status	Global client relationship management and business development related activities	Until the recipient's purpose of using the personal information is achieved or longer if required by law, litigation or investigation purposes	Consent from data subject obtained by our corporate client
Financial regulators in the Republic of Korea including the Financial Service Commission ² , and the Financial Supervisory Service ³	Subject to the requirements of the supervisory authority	Supervision of the Company and related regulatory and licensing activities	Until the recipient's purpose of using the personal information is achieved or longer if required by law	Korea legal and regulatory requirements

¹ For a list of affiliates of the Company and their contact information, please visit <https://www.jefferies.com/regulatory-disclosures/>

² <https://www.fsc.go.kr/eng/co010101>

³ <https://www.fss.or.kr/eng/bbs/B0000215/list.do?menuNo=400011>

Annex B: Delegation of the processing of personal data

We delegate the processing of personal data as described below, and the delegates may process personal data according to the purpose of the delegation:

Delegatee	Purpose of the Delegated Tasks	Details of Delegation
Jefferies Hong Kong Limited Jefferies India Services Private Limited Jefferies Singapore Limited Jefferies International Limited Jefferies LLC Jefferies (Australia) Pty Ltd Jefferies India Private Limited Jefferies (Japan) Limited Tokyo Branch Jefferies GmbH	Corporate support	Corporate functions including IT, Physical Security, Corporate Services, Internal Audit, Compliance, Legal, Operations (including Client Onboarding), Risk, Tax, Finance/Controllers and Treasury
Iron Mountain Korea Limited	Corporate services	Secure paper documents shredding and disposal
Chubb Fire & Security Ltd t/a Frontline Security Solutions (using Gallagher application)	Physical security	Office access card management
Microsoft Corporation	Information technology	Provider of Microsoft 365 software and cloud services
Bloomberg L.P.	Information technology	Data archiving in Bloomberg Vault
Zoom Communications Inc	Information technology	Provider of video conferencing service
Box, Inc.	Information technology	Secure sharing of documents with third parties

Annex C: Overseas transfers of personal data

Recipient's Name (Contact Information)	Territory where Recipient is Located	Items of Personal Data transferred	Recipient's Purposes of Use	Time/ Method of Transfer	Recipient's Period of Retention and Use	Legal basis for overseas transfer
Jefferies Hong Kong Limited Jefferies India Services Private Limited Jefferies Singapore Limited Jefferies International Limited Jefferies LLC Jefferies (Australia) Pty Ltd Jefferies India Private Limited Jefferies (Japan) Limited Tokyo Branch (Link in footnote for contact information ⁴)	Hong Kong, India, Japan, Australia, Singapore, UK, USA	Full name, date of birth, gender (for non-resident foreigners only), address and contact information, copies of photo identification documents (such as a driving licence and/or passport/identity card), information about nationality/citizenship/place of birth, national identification numbers ⁵ and other identity verification documents for anti-money laundering due diligence purposes	Delegated corporate functions for the Company	Transferred through telecommunication networks from time to time as needed	Until the recipient's purpose of using the personal information is achieved or longer if required by law, litigation or investigative purposes	Consent obtained by corporate client/vendor from data subject
Jefferies Hong Kong Limited Jefferies International Limited Jefferies LLC (Link in footnote for contact information ⁶)	Hong Kong UK US	Storage of CCTV recordings	Safety of facilities, prevention of fire and crime at the Company Investigation into suspected crime or breaches of Company internal policies	Transferred through telecommunication networks from time to time as needed	30 days or longer if required by law, litigation or investigation purposes	Consent from the data subject entering the Company's premises; Necessary for performance of contract with the organization the data subject is associated with
Chubb Fire & Security Ltd t/a Frontline Security Solutions	UK	- Name - Office physical access details	Physical security – installation and troubleshooting of	Transferred through telecommunication	Duration granted by Jefferies Physical Security Team from	Necessary to perform an agreement with

⁴ For a list of office locations and their contact information, please visit <https://www.jefferies.com/global-locations/>

⁵ Korea-issued Resident Registration Numbers (for citizens and foreigners); Korea-issued driver's license numbers; and all jurisdictions' passport numbers are not transferred overseas.

⁶ For a list of office locations and their contact information, please visit <https://www.jefferies.com/global-locations/>

Recipient's Name (Contact Information)	Territory where Recipient is Located	Items of Personal Data transferred	Recipient's Purposes of Use	Time/ Method of Transfer	Recipient's Period of Retention and Use	Legal basis for overseas transfer
(Chubb House, Shadsworth Road, Blackburn BB1 2PR)			office access card management system	networks from time to time as needed (Access via theGallagher application)	time to time ranging from several hours to a few days, depending on the task to be completed by the delegatee	the organization the data subject is associated with
Microsoft Corporation (https://www.microsoft.com)	Australia Japan	- Name - Company email address - Company telephone number - Company mobile phone number - Organization name Information transmitted via email and Microsoft Teams	Provider of Microsoft 365 software and cloud services	Cloud-based sync	10 years from the date of last employment or longer if required by law, litigation or investigation purposes	Necessary for performance of contract with the organization the data subject is associated with
Bloomberg L.P. (https://www.bloomberg.com/professional/products/compliance/vault)	USA	- Name - Company email address - Information transmitted via email	Data archiving in Bloomberg Vault	Direct integration with Jefferies systems	10 years from the date of last employment or longer if required by law, litigation or investigation purposes	Necessary for performance of contract with the organization the data subject is associated with
Zoom Communications Inc (https://zoom.com/en/contact)	Zoom's APAC servers	- Name - Email - Organization name - Department - Role - Profile photo (if added by user) - Geographic location - Employee ID - Information transmitted via Zoom audio or video calls	Provider of video conferencing service	Transferred through telecommunication networks from time to time as needed	Until user account is no longer operational	Necessary for performance of contract with the organization the data subject is associated with
Box, Inc. (Box Privacy, 900 Jefferson Avenue, Redwood City, CA 94063, United States of America)	Box's APAC servers	Information in files shared through Box.com	Secure sharing of documents with third parties	Transferred through telecommunication networks from time to time as needed	Until the recipient's purpose of using the personal information is achieved or longer if required by law	Necessary for performance of contract with the organization the data subject is associated with