

Client data protection policy

This Client Data Protection policy ("**Policy**") applies to personal information about you (whether as an individual or on behalf of any corporates), any of your employees, officers, directors, agents, contractors or consultants or any of your customers, suppliers or any other relevant individual that you engage with in the ordinary course of business ("**Client Business Personnel**") held by Wei Tu Law Firm ("**Wei Tu**" or "**we**", including any branch of Wei Tu), a PRC law firm incorporated in Guangzhou under PRC law. Wei Tu and Stephenson Harwood (a Hong Kong partnership) are in a CEPA association under the name "Stephenson Harwood – Wei Tu (China) Association". The association allows us to offer a 'one stop service' for Hong Kong, English and PRC law advice, with Wei Tu providing the PRC law advice. See "**Contacting us**" below for our contact details.

Please read this Policy carefully and make sure that you understand the rules for the processing of personal information by us. **For the terms and conditions in this Policy that we consider may have a significant concern with your or your Client Business Personnel's rights and interests and those involving sensitive personal information, we have used bold font to highlight them. Regardless of whether you are providing personal information of your Client Business Personnel or on behalf of a corporate, you hereby represent, warrant and undertake to us that you have obtained proper authorization from the relevant individuals, including any separate consent required, and will promptly provide documents evidencing such authorization as requested by us from time to time.**

In this Policy:

"**Data Protection Legislation**" means all applicable legislation relating to privacy or data protection in force from time to time, including any statute or statutory provision which amends, extends, implements, consolidates or replaces the same, and in particular to the extent applicable and without limitation the Personal Information Protection Law of the People's Republic of China ("**PIPL**") and the EU General Data Protection Regulation 2016/679. The terms "personal information/data", "sensitive personal information", "special categories of personal data", "controller", "entrusted party", "individual" and "process" (and its derivatives) shall have the meanings given to them in the Data Protection Legislation.

"**SH Group**" means Stephenson Harwood and other partnerships, corporations and undertakings which are authorised to carry the name "Stephenson Harwood" and Virtus Law LLP; and a "member of the SH Group" has a corresponding meaning. The SH Group is not a legal entity or a partnership and does not itself provide legal services. Legal services are provided to clients by the individual members of the SH Group, each of which is a separate and distinct business, and some of which are limited liability undertakings.

"PRC" means the People's Republic of China and, for the purpose of this Policy, excluding the Hong Kong Special Administrative Region, the Macao Special Administrative Region and Taiwan Region.

Using your information

We may collect and process information relating to you and your Client Business Personnel in order to provide our services to you. We shall process any information we collect in accordance with Data Protection Legislation and the provisions of this Policy.

Your Information

The information referred to above includes personal information, which means information that can be used to identify a natural person or to reflect the activity of a natural person, including (but not limited to) the following types of personal information:

- name and contact information, such as an individual's home or work address and contact details (including mobile phone number, WeChat ID and email address);
- gender, date of birth, **marital/civil partnership status**, details of dependants and next of kin;
- **copy of your document of identity**, including
 - identity card
 - passport
 - Mainland Travel Permits for Hong Kong and Macao Residents (Home Return Permits)
 - Mainland travel permit for Taiwan residents,and the relevant **serial number of these identity documents**;
- **financial information (including bank account details, salary and benefits, tax rates, housing information and information in relation to investments)**;
- employment status, employer, occupation and title;
- information about an individual's professional qualifications;
- **salary and pay records**;
- other information about an individual that you or your Client Business Personnel disclose to us when communicating with us;

- details of any complaints or concerns raised by you or your Client Business Personnel;
- information we obtain from the instructions you give to us;
- information we process when you and your Client Business Personnel communicate with us or any other time you or they contact us; and
- information we obtain from third parties, such as information that we obtain when verifying details supplied by you. This information obtained from other third party organisations may include fraud prevention agencies and information which is collected from publicly available sources.

Some of the information that we collect about you and your Client Business Personnel may include sensitive personal information or other special categories of personal data (such as information about racial or ethnic origin, criminal or alleged criminal offences or health and lifestyle). We will, to the extent required by the Data Protection Legislation, seek separate consent or permission from you or them in writing to process such information.

If you fail to provide us with this information, or you or your Client Business Personnel object to us processing such information (see "**General Rights**" for more information about your rights in relation to your information), the consequences are that we may be prevented from providing our services to you, or continuing to manage your matter(s) with us.

Our processing of your information

We may collect, record and use personal information about you and your Client Business Personnel, and the services we provide to you, in physical and electronic form and will hold, use and otherwise process the data in accordance with the Data Protection Legislation and as set out in this Policy. This may include sharing this information with third parties and providing it across border from the PRC. More information about sharing such information is set out below.

We may process any information we hold about you and your Client Business Personnel for a number of business purposes. Examples of the types of uses of such information are set out below:

- to undertake conflict search;
- to provide our services to you;
- to administer and operate your client account(s) and matters;
- to monitor and analyse the conduct of your client account(s) and matters;

- to assess any billing matters or credit decisions;
- to enable us to carry out statistical and other analysis and to meet our legal or regulatory obligations;
- for our reasonable commercial purposes (including in connection with our insurance, quality control and administration and assisting us to develop new and improved services);
- to confirm your or their identity and carry out background checks, including as part of our client due diligence for the purposes of anti-money laundering, combating terrorism financing, national security, compliance screening and to prevent fraud and other crimes;
- to follow up with you or them after you request information to see if we can provide any further assistance;
- to comply with any requirement of applicable laws or regulations;
- to fulfil our obligations under any reporting agreement entered into with any tax authority or revenue service(s) from time to time;
- to check your instructions to us;
- to circulate attendee lists to other attendees of our events;
- to monitor, record and analyse any communications between you or them and us, including phone calls to analyse, assess and improve our services to you, as well as for training and quality purposes;
- to prevent or detect abuse of our services or any of our rights (and attempts to do so), and to enforce or apply this Policy and/or any other agreement and to protect our (or others') property or rights;
- in the context of a sale or potential sale of a relevant part of our business, subject always to confidentiality obligations;
- if instructed to do so by you or them or where you or they give us consent to the use and/or processing involved; and
- to bring to your or their attention (in person or by post, email or telephone) information about additional services offered by us and/or the SH Group, which may be of interest to you or them, unless you or they indicate at any time that you or they do not wish us to do so.

Lawful grounds for using your information

We have described the purposes for which we may use information about you and your Client Business Personnel. We are permitted to process such information in this way, in compliance with the Data Protection Legislation, by relying on one or more of the following lawful grounds:

- you or they have explicitly consented to us processing such information for a specific reason;
- the processing is necessary to perform the agreement we have with you or them or to take steps to enter into an agreement with you or them;
- the processing is necessary for compliance with a legal obligation we have;
- the processing is necessary for us to respond to sudden public health incidents or to protect individuals' lives, health or properties under emergency conditions;
- the processing is necessary for us to implement news reporting, public opinion supervision and other such activities for the public interest, provided that such processing is carried out within a reasonable scope; or
- the processing is related to personal information which has already been publicly disclosed by yourself or themselves or by other lawful means, provided that such processing is carried out within a reasonable scope in accordance with the Data Protection Legislation and does not have a significant impact on your or their rights and interests.

Separate consent

Notwithstanding the foregoing, in any of the following scenarios, we may only process your or their personal information with separate consent:

- processing of sensitive personal information;
- sharing the personal information with other controllers. See "**Information Sharing - Sharing your information with others**" section below for more details;
- public disclosure of the personal information;
- use of your or their image or identifying information collected from public places for any purpose other than safeguarding public security; or
- providing the personal information across border from the PRC. See "**Information sharing - Providing your information across border**" section below for more details.

In relation to any processing of sensitive personal information or special categories of personal data, we will generally rely on obtaining specific

consent in order to process such information, although it may be necessary for us to use certain information in order to comply with our legal obligations as a regulated entity (such as in relation to an alleged offence). Where you or your Client Business Personnel have consented to our processing of such information, you or they may withdraw such consent at any time, by contacting us using the contact details set out in "**Contacting Us**" below. Please note, however, that in certain circumstances it may be still lawful for us to continue processing this information even where consent has been withdrawn, if one of the other legal bases described above is applicable.

Automated processing

We do not carry out automated decision-making or profiling in relation to our clients.

Information sharing

Sharing your information with others

We keep all client information confidential. However, in order to be able to service our clients' needs to the best of our ability, we may identify a member or members of the SH Group or other outside counsel, experts, agents, document management providers, consultants and/or foreign lawyers to work for you on your matter, and may therefore share any information you provide to us with such entities or persons and their agents, counterparties and support service or data providers, wherever located. If we are required to instruct such entities or persons on your behalf, we will seek your consent before doing so.

We may also provide third party service providers, as entrusted party, access to client information where they support or provide services to us. We will ensure that if we share information with, or provide access to, third party service providers, any such disclosure or access is at all times in compliance with Data Protection Legislation.

If you or your Client Business Personnel have provided information to a member of the SH Group, to the extent permitted by the Data Protection Legislation, those entities may also share that information with us.

Save for the SH Group or other outside counsel, experts, agents, document management providers, consultants and/or foreign lawyers, the recipients, or categories of recipients, of your information, or information relating to your Client Business Personnel, may be:

- any revenue service or tax authority, if obliged to do so under applicable regulations;
- your other advisers (including, but not limited to, accountants or other professional advisers) where authorised to do so by you;

- to the extent permitted by applicable laws and regulations, PRC and overseas regulators, courts and authorities in connection with their duties (such as crime prevention);
- fraud prevention agencies who will use it to prevent fraud and money-laundering and to verify your identity. We and fraud prevention agencies may also enable law enforcement agencies to access and use your information to detect, investigate and prevent crime;
- third party service providers who support or provide services to us;
- attendees of our events where we circulate names, corporate names and corporate email addresses on an attendee list for our events;
- anyone to whom we may transfer our rights and/or obligations under this Policy; and
- any other person or organisation after a restructure, sale or acquisition.

If we, or a fraud prevention agency, determine that you and/or your Client Business Personnel pose a fraud or money laundering risk:

- we may refuse to provide the services you have requested, or we may stop providing existing services to you; and
- a record of any fraud or money laundering risk will be retained by the fraud prevention agencies, and may result in others refusing to provide services, financing or employment to you or them.

Sharing third party information with us

If any information which you, your Client Business Personnel provide to us relates to any third party, by providing us with such information you or they confirm that you or they have obtained any necessary permissions from such persons to the reasonable use of their information in accordance with this Policy, or are otherwise permitted to give us this information on their behalf. You shall promptly provide us with documents evidencing such authorization or permission as requested by us from time to time.

Providing your information across border

Information about you, your Client Business Personnel in our possession may be provided to recipients in other countries or regions (particularly to the entities in the SH Group and their agents in different countries or regions) for any of the purposes described in this Policy by ways of, including but without limitations, transferring or storing the personal information outside the PRC, or granting the overseas recipient access to the personal information stored in the PRC.

You and your Client Business Personnel understand and accept that these countries or regions may have differing (and potentially less stringent) laws relating to the degree of confidentiality afforded to the information they hold and that such information can become subject to the laws and disclosure requirements of such countries, including disclosure to governmental bodies, courts, regulatory agencies and private persons, as a result of applicable governmental or regulatory inquiry, court order or other similar process. In addition, a number of countries have agreements with other countries providing for exchange of information for law enforcement, tax and other purposes.

When we provide your or your Client Business Personnel's personal information across border from the PRC, we will impose contractual obligations on the overseas recipients to ensure that the relevant personal information will be protected by the overseas recipient at a level at least up to the standards set by PIPL and only where:

- you and your Client Business Personnel have provided separate consent in relation to the cross border provision of personal information, or
- such provision of personal information across border is otherwise permissible under Data Protection Legislation (for example if we are required to provide such information by law).

Subject to the volume and nature of the relevant data export involving your or your Client Business Personnel's personal information, we will also meet at least one of the following requirements set by PIPL for exporting such information:

- passing the data export security assessment conducted by the Cyberspace Administration of China ("**CAC**");
- obtaining certification from a specialised institution under the applicable rules prescribed by CAC;
- entering into a standard form contract formulated by CAC with the overseas recipient, and where required by law, filing it with CAC; and
- satisfying other conditions under the applicable laws, administrative regulations or rules prescribed by CAC.

Protection of minors

Please note that normally Wei Tu does not intentionally collect or process personal information of minors under the age of 18. Wei Tu may provide legal services to minors in protection of their legal rights with the consent of their legal guardians. Personal information of minors must be provided by their legal guardian or by the minors themselves if accompanied by their guardians.

Your rights in relation to your information

You and your Client Business Personnel have a number of rights concerning the way that we use your information. You are responsible for ensuring that your Client Business Personnel are aware of these rights, which comprise:

- to request access to, or a copy of, any personal information we hold about you or them, except where the laws require us to keep such information confidential;
- to request the rectification of your or their personal information, if you or they consider that it is inaccurate or incomplete;
- to request the erasure of your or their personal information in any of the following scenarios:
 - The purpose of personal information processing has been achieved or cannot be achieved, or the personal information is no longer necessary to achieve such purpose;
 - The period of the retention of the personal information has expired;
 - You or they have withdrawn your or their consent;
 - Our personal information processing violates the laws and administrative regulations or breaches our contracts with you or them; or
 - Other circumstances provided by the applicable laws and administrative regulations;
- to restrict or object to our processing of your or their personal information;
- to ask us to provide the portal for transferring your or their personal information to another controller where technically feasible, but we may grant such request only if the conditions set by CAC have been met;
- where our processing of your or their personal information is undertaken based on your or their consent, to withdraw, at any time, any such consent but such withdrawal of consent shall not affect the effectiveness of our processing of the relevant information which had already been undertaken before you or they withdraw such consent;
- to request us to explain and elaborate this Policy and any other rules on the processing of your or their personal information; or
- to ask us to stop or start sending them marketing messages at any time.

For security reasons, we may ask you to verify your identity before processing your request. Any such request must be made in writing and we will endeavour to respond

within a reasonable period and in any event within 30 days in compliance with Data Protection Legislation. We will comply with our legal obligations as regards any individual's rights as a data subject.

If you would like to contact us in relation to any of the rights set out above please contact us using the contact details in the "**Contacting Us**" section below.

Retaining your information

We will only keep the information we collect about you and your Client Business Personnel on our systems or with third parties for as long as required for the purposes set out above or as required to comply with any legal obligations to which we are subject. This will involve us regularly reviewing our files to check that information is accurate and up-to-date and still required.

If you terminate your relationship with us, a matter comes to an end, we decline to act on a matter, or you decide not to go ahead with a matter, we may still keep your information.

Sending you marketing information

Wei Tu may use your information from time to time to send and inform you and your Client Business Personnel by letter, telephone, text (or similar) messages, email or other electronic means, certain newsletters, alerts and updates, and information about similar services (including those of third parties), which may be of interest to you or them.

You and your Client Business Personnel may, at any time, request that we cease or do not send such information by one, some or all channels, by contacting us using the contact details set out below or by clicking "unsubscribe" for the relevant communication.

Contacting us

If you or any of your Client Business Personnel wish to exercise any of the rights relating to your information set out above, or if you have any questions or comments about data protection, or you wish to raise a complaint about how we are using your information you can contact us using the following details, or any other details notified to you from time to time:

- Write to Wei Tu Law Firm at 903 - 904, R&F Center, No.10 Hua Xia Road Zhujiang New Town, Guangzhou 510623 PRC or email info@shlegalworld.com or call +86 20 8388 0590.

- Details of all our offices are available on our website, www.weitu-china.com.

If you and/or your Client Business Personnel have any concerns about our use of your or their information, you and they also have the right to make a complaint to CAC and their contact details are available here: <http://www.cac.gov.cn/>.

Policy update

We may make changes to this Policy from time to time and how we use your information in the future. If we do this, we will ensure that the version available on this website (www.weitu-china.com) is the current version. You acknowledge and confirm that if you do not agree to the updated version of this Policy, you should immediately inform us and request that we stop processing your or your Client Business Personnel's personal information; if you continue to provide such information to us or allow us to process such information, you are deemed to have agreed to accept the updated content.

Version: WT20240101V1

This Policy is written in Chinese and the English translation is for reference only. Should there be any inconsistency between the English and Chinese versions, the Chinese version shall prevail.