FRC (Hong Kong) Limited Privacy Statement

Last updated: September 2025

Introduction and purpose of this Privacy Statement

You are reading this privacy Statement to understand how FRC (Hong Kong) Limited, with registered office at 1603 Kowloon Plaza 485 Castle Peak Road, Hong Kong with company number 59610258, along with its affiliates and subsidiaries (hereinafter referred to as "**FRC (Hong Kong)**", "**FRC**", "**We**" or "**Us**") handles (or processes) your personal data/personal identifiable information (hereinafter referred to as "**Personal Data**"; "Data" or "PII")).

Although this document focuses on The Personal Data (Privacy) Ordinance (PDPO) because our headquarters are in Hong Kong, we are committed to following all privacy regulations in Hong Kong where we conduct market research. This includes, but isn't limited to, Asia-Pacific (APAC). Where local laws differ from the PDPO, we ensure compliance by, e.g., General Data Protection Regulation, offering specific opt-in choices or using approved data transfer methods.

This Privacy Statement ("**Statement** ") explains how FRC (Hong Kong) Limited processes your Data according to data protection laws, especially the PDPO. It describes how we use this Data, our security measures, and your rights as a data subject (research participants, website users, clients, suppliers, and business contacts).

It applies to Personal Data collected through:

- **Market Research Activities (MRA) (**e.g., (online) surveys, communities, panels, interviews and focus groups)
- **Business Activities/Operations (BA)** (e.g., own marketing, website interactions, contractual relationships, job applications)
- Social media presences (on LinkedIn, Instagram, X)

This Statement distinguishes between data processing for **Market Research Activities** (mainly for **participants**) and our **Business Activities/ Operations.**

"Participant" means anyone involved (engaged or interested) in Market Research Activities (e.g., survey respondents, panel members, focus group participants)

Other terms in this statement align with the definitions in The Personal Data (Privacy) Ordinance (PDPO):

- **'Process' and/or 'processing'** means any operation or set of operations performed on personal data/PII, such as collection, recording, storage, use, sharing, pseudonymization, anonymization, erasure, alteration, or destruction, as defined in section 4 of the PDPO.
- **'Personal Data/PII'** means any information that relates to you and could—directly or indirectly—identify you. This includes:
- Basic details (e.g., name, email, address, phone number);
- Digital identifiers (e.g., IP address, cookies, device ID);
- Sensitive data (e.g., health information, race, religious beliefs – where applicable);
- Other details like your opinions, location data, or even work history if linked to you.

We do not consider truly anonymous data (where no one can trace it back to you) as personal data.

Where to Find/Table of Contents

1. Who we are

FRC (Hong Kong) Limited is a regional market research company. We conduct consumer insights research for our clients. More details about our roles in data processing are below [cf. 2. Roles].

FRC (Hong Kong) Limited is committed to following all applicable data protection laws, including but not limited to The Personal Data (Privacy) Ordinance (PDPO). All of our entities follow the stringent PDPO requirements and other applicable privacy regulation to protect your personal data.

As members of the European Society for Opinion and Marketing Research (**ESOMAR**), we follow its ethical research standards, ensuring high-quality and trustworthy market research.

2. Our “Role” (Position) under Data Protection Laws

General:

FRC (Hong Kong) Limited's 'Role': Unless otherwise communicated, we may process your personal data as a **data controller**, **data processor**, or **joint controller**, depending on the specific circumstances.

- **Data Controller**: We **decide how and why** (Purpose and Mean) your personal data is processed. Equivalent terms include 'controller', 'responsible party', 'controlling organization', 'business' (CCPA/CPRA), and 'business operator.'
- **Data Processor** – When we process personal data on behalf of a client, following their instructions. Equivalent terms in other privacy laws include 'service provider', 'operator' and 'entrusted business operator.'
- **Joint Controller** – We jointly decide how and why your personal data is processed with another party (e.g., our clients).

These distinctions define our responsibilities toward you and other parties involved, such as our clients. They also determine how this **Privacy Statement** applies to our processing activities, as explained below.

2.1 (For Participants:) Our Role(s) in Market Research Activities (MRA):

In general, we conduct market research for our clients or on behalf of our clients, and our role may vary. We often act as a **Data Processor**, while our **client is the Data Controller**. This is common when we get your personal data directly from the client.

However, in some cases, we may act as an **independent data controller**, depending on the nature of the study and our contractual agreements.

2.1.1 When we act as a Data Processor:

We process your Personal Data only according to our clients' instructions. Our clients are the Data Controllers. We have a contract with our clients, including a Data Processing Agreement as required by law.

Our market research projects are usually conducted on behalf of companies/our clients with a Legitimate Interest in the results. To avoid affecting the study's objectivity, we may not reveal the client's name before the study. Instead, we'll tell you about the client's industry. You can ask for the client's name after the study, unless the client has a legitimate reason to keep it private (for example, to protect a new product launch).

Our clients are responsible for informing you how they will use your personal data. As a data processor, FRC (Hong Kong) Limited is not responsible if this information is incomplete. Our clients are solely responsible for explaining how they process and use your personal data. If their activities go beyond the market research purposes in this Statement, they will provide more details separately.

2.1.2 When we act as a Joint Controller:

If we and our clients **jointly determine** the purpose and essential means of processing your personal data, we act as **joint controllers** under data protection laws.

In such cases, we and our clients enter into a **Joint Controller Agreement (JCA)** in accordance with the PDPO. This agreement clearly defines each party's responsibilities for compliance to applicable privacy regulation, transparency (inform You of the necessary privacy information), and data protection.

Information about the processing of personal data, in accordance with applicable laws—particularly Part 6 of the PDPO—is provided jointly by both controllers. This information is made available to data subjects through privacy policies published on their official websites and, specifically, in this Statement

2.1.3 When we act as an (independent) Data Controller:

In certain cases, we act as **an independent Data Controller** when processing your personal data for Market Research Activities (MRAs). This applies, for example, when we approach, recruit, and invite you to participate in an MRA, such as using our **own participant member databases**, or other non-client databases in these cases, we independently decide how and why your personal data is processed.

We also act as an independent Data Controller in managing and maintaining our own participant member database, which individuals can register for or to whom we may send invitations to participate in Market Research Activities.

Information about the processing of Personal Data, as required by law, especially Part 6 of the PDPO, is provided in our privacy policy on our websites and in this Statement.

For more detailed information about how your personal data is handled in MRA, please refer to Section 4: Description of the Processing of Your Personal Data (Categories of Data, Purpose, General Legal Base, and Retention Period 4.1 and 4.2) of this privacy statement.

2.2 For Client/ Business partner/Applicants/others: Our Role in Business Activities/Operations

(Information for Visitors/Visitors of our Website, Newsletter Subscriber; Clients, Business contacts, Supplier, Applicant and other individuals who contact us outside of MRA)

When we carry out our business activities/operations and collect your personal data—whether as a visitor to our websites, an applicant, a subscriber to our newsletter, a client, a supplier, a business contact, or any other individual who reaches out to us—we process your personal data on behalf of FRC (Hong Kong) Limited. The entity within FRC (Hong Kong) Limited to whom you initially provide your personal data acts as the primary data controller.

Information about the processing of your personal data, in accordance with applicable laws—particularly Part 6 of the PDPO —is provided both in this Statement and in our company's Privacy Policy available on our website.

Additionally, it is possible for one entity of FRC (Hong Kong) Limited to receive services directly or indirectly from another entity within the group. For example, when a local entity conducts market research activities on behalf of a client and requires assistance from another entity within FRC (Hong Kong) Limited, the assisting entity acts as a sub-processor for the personal data. In such cases, an Intra-Group Agreement is in place, including a Data Processing Agreement to ensure compliance with applicable laws.

For more detailed information about how your personal data is handled in our BA, please refer to Section 4: BA-Description of the Processing of Your Personal Data of this privacy statement.

3. Who to contact if you have privacy questions?

3.1 For all privacy concerns:

Please contact our **Data Protection Officer (DPO)**:
Email: gloria.cheung@frchongkong.com

3.2 When we act as a Data Processor:

We will forward your request (e.g., access, deletion) to the relevant client (**Data Controller**) without undue delay. The **Data Controller/client** is legally obligated to respond to your request.

Please note: **Client Identity in research**:
You will usually receive the **Data Controller's contact details** at the start of the research.
In rare cases (e.g., to preserve research integrity and prevent bias), we may disclose the client **after the research concludes** upon request.
If you withdraw consent post-disclosure, we will delete your **Personal Data** immediately.

Our commitment:

- We aim to address all inquiries, regardless of our role (Controller/Processor), within **4 weeks**.
- Complaints will be escalated to the **Controller** and our **DPO** for resolution.
- For unresolved issues, you may lodge a complaint with your **local data protection authority**.

If you have any questions or concerns about this statement or the processing of your personal data, please contact the **FRC Data Protection Officer (DPO)** using the contact information provided below under "**9 FRC DPO**".

4. Processing of your Personal Data

Overall

Data protection laws require us to have a valid reason (legal base) for using your personal data. Depending on where you are and what we're doing with your data, these reasons may include:

- Your **Permission**/explicit **consent**: You've given us clear permission to use your data for specific purposes. This is important under laws like PDPO in Hong Kong, GDPR in Europe, CCPA in the USA, and similar laws in South Africa, Brazil, India, Canada, Japan, and Australia.
- To Fulfil a Contract (**Contractual Necessity**): We need your data to fulfil the obligations outlined in our contract with you, which includes the Terms and Conditions you agree to when you participate. For example, if you're a panel member, we need your contact details to send you surveys or research requests as part of the agreement defined in the Terms and Conditions.
- **It's Required by Law (Legal Obligations):** We might be required to use your data to follow legal obligations, like tax reporting or compliance with other local laws (e.g., GDPR, CCPA, POPIA, PIPEDA, and others).

We Have a Legitimate Reason (Legitimate Interests): We can use your data if we have a genuine and fair reason, as long as it doesn't interfere too much with your privacy. For example, we believe market research is a Legitimate Interest. We carefully balance our needs with your privacy rights and only use your data in fair and reasonable ways. Examples of Legitimate Interests: Improving our services, understanding customer trends, and developing new products to better meet your needs.

4.1 Market Research Activities (MRA) Data Processing: What Participants Need to Know

4.1.0 What We Use Your Data For (Purpose) in General

We use and process your personal data for market research purposes, which includes all Research related steps:

1. Sending you invitations, organizing and conducting research activities, and communicating with you about research opportunities. This may involve selecting participants based on criteria such as age, location, or interests.
2. Providing and maintaining the online research platform
3. Hosting the Data; Storing the research data securely
4. Handling data, such as transcribing interviews, summarizing responses, or translating answers.
5. Analyzing data and creating research reports for our clients.
6. Profiling may be used to group participants for research purposes, but this will not have any legal or significant effect on you (it is only for research quality and targeting, never for automated decision-making that affects your rights.)
7. **Use of anonymized research results:** We always share research results with the client who commissioned the study. These results may include pseudonymized and/or anonymized quotes or participant responses, but never any personal data that could directly identify you.

In some cases, anonymized research findings may also be used in marketing materials, trade publications, conferences, or other public communications. Any information used in this way is fully anonymized and carefully reviewed to ensure it cannot be linked back to any individual. For example, quotes will never include your name or any other identifying details without your explicit consent. A typical quote might appear as follows:

“I like this product because it’s easy to use.” (quote: woman, user, age 20–29)

4.1.1 Data Sources & The Types of Personal Data We Use:

Sources: We may collect your personal data from these sources:

- **Directly from you:** e.g., Become a member of our database and directly enter your information. Answer surveys, whether for recruitment or during a research project. Participate in interviews or focus groups. Contact us with inquiries or requests related to our research activities.
- **From our clients:** If our client provides us with your information for research purposes.
- **Public sources:** Such as public social media profiles or public directories.
- **Third parties:** Like panel partners or list providers, but only when this is allowed by law.

If your data is collected **from in-direct sources**, we will inform you at the time of first contact and disclose the source. Specifically, we will:

- Notify you during the initial contact (e.g., when inviting you to participate)
- Inform you about the source of your data and the specific purposes for processing
- Make it clear if your data came from a public source.
- Use your data solely for the purposes described

If you ask us to remove your personal data from our records, we will do so as soon as possible. If we have shared your personal data with others, we will also tell them to delete it.

Types of Personal Data We Collect in General

The types of personal data we collect depend on the research project. This may include:

- Contact Information: Your name, address, email, and phone number.
- Demographic Information: e.g., your age, gender, location, education, income, and employment details.
- Behavioural Data: e.g., your opinions, preferences, product usage, and purchasing behavior.
- Technical Data: e.g., your device's IP address, browser type, and cookies.
- Sensitive Data: sometimes, we may ask about things like your health or political views. We will only collect this kind of information if you give us clear permission (explicit consent) and if the law allows it.

We take extra precautions to protect sensitive data, including encrypting it and restricting access to only those who need it.

4.1.2 Our legal basis for using your Data in General

Unless otherwise stated and without a legal basis, FRC (Hong Kong) Limited will only **use** your personal data **for conducting market research**. We only process your personal data when we have a valid legal reason to do so. We will never use your data for advertising or any other purposes unless you have given clear consent. If we ever plan to use your data in a new way, we'll inform you in advance.

These legal bases may include:

Legal Basis MRA	**Description**
Consent *(and additional, explicit consent where required by law)*	*We ensure that when we rely on your consent for processing of your data, we or our clients have obtained your* ***informed, explicit, and unambiguous consent****.* *Explicit consent is required for collecting sensitive data, using images where you identifiable, or for cross-border transfers.* ***You can withdraw your consent anytime with effect for the future –*** *– see the "Your Rights" section for details.*
Contractual Necessity *(by accepting the Terms and Conditions provided before participating)*	*To participate in our research activities, we need to collect and use certain personal data — such as your contact details (e.g., name, email) and some basic demographic information (e.g., age, gender, location, or target group). This helps us manage your participation, ensure the quality and fairness of the research, and provide any incentives we've promised (such as prize draws or vouchers).*

Legal Basis MRA	Description
	By accepting the Terms and Conditions and joining our research, you agree to the processing of only the data that is strictly necessary for these specific purposes.
***Legitimate Interest** (only where permitted by local legislation)*	*We may process your personal data when we have **a Legitimate Interest** to do so — but only if that interest is not overridden by your rights and freedoms.* *These interests may include:* • *Improving our services and research methodologies* • *Keeping our systems secure and preventing fraud* • *anonymized or pseudonymized your data and performing data analytics and generating insights* • *Providing customer support or responding to your inquiries* • *Conducting limited direct marketing (only where legally permitted and with opt-out options)* *Before relying on this legal basis, we carefully assess the potential impact on your privacy.* *Where needed, we apply safeguards — like data minimization, access controls, and pseudonymisation — to protect your personal data.* ***You always have the right to object to this type of processing. See the "Your Rights" section for details.***
Legal obligations	*We may use your data if it's required by law—for example, to comply with reporting requirements or respond to official requests from authorities.*

4.1.3 Data Protection Measures:

We use the following measures to protect your personal data:

- **Pseudonymization:** We minimize the use of directly identifiable information wherever possible.

- **Data Minimization:** We only collect the personal data that we need for research.
- **Secure Deletion/Anonymization:** We make sure your data is securely deleted or anonymized when we no longer need it.

For more information on how we protect your data, please see section "*6 How We Keep Your Data Safe."*

4.1.4 How Long We Keep Your Data / Retention Periods in General

We keep your personal data only as long as necessary for the purposes for which it was collected, or until you ask us to delete it. This also depends on whether you withdraw your consent or object to us processing your data.

- **General Retention:** We will keep your personal data for no more than 2 years after the research project ends, or for the period required by law (for example, 8 years for financial data). We may keep it longer if needed for analysis, legal reasons, or other legitimate purposes.
- **Data Processed for Clients:** If we are processing your data for a client, they determine how long we keep the data. We can only keep the data as long as our agreement with the client lasts. After that, we must return or delete the data, according to the client's instructions.

After the retention period ends, we will securely delete or anonymize your data.

4.1.5 Overview What data we collect and why for MRA

This table outlines the types of personal data we may process, why we do so, the legal basis that allows it, and how long we keep your data. We always process your data responsibly and in compliance with applicable data protection laws, including those that apply to children's data.

Categories of Personal Data MRA	**Purpose MRA** *(see Section 4.1.0 for details)*	**Possible Legal Basis MRA**	**Retention Period MRA** *(as outlined in Section 4.1.5)*
Electronic Identification/Metadata *(e.g. address, user ID, device identifiers, browser details, geolocation, cookies)*	*(Includes: a) Managing research; b) Providing and maintaining the research platform; c) Hosting data; d) Data*	– Legitimate Interest *(security, fraud prevention, system admin)*	As outlined in Section 4.1.5 — generally not longer than **2 years** after the research ends

Categories of Personal Data MRA	**Purpose MRA** *(see Section 4.1.0 for details)*	**Possible Legal Basis MRA**	**Retention Period MRA** *(as outlined in Section 4.1.5)*
	handling; e) Analysis and creation of research reports) *This data helps recognize and authenticate users in digital environments, and provides context about other data without containing the content itself)*	– Consent *(non-essential cookies, tracking)*	
Contact Information *(e.g., name, email address, phone number)*	*– Manage your participation* *– Communicate with you and provide support* *– Deliver rewards or incentives*	– Contractual Necessity, – Consent, – Legitimate Interest: *(Customer support, communication)*	Generally not longer than 2 years after the research ends. We may keep it longer if needed for analysis, legal reasons, or other legitimate purposes.
Demographic Data *(e.g., age, date of birth, gender, nationality)*	*– Organize and analyse research* *– Create research reports* *– Segment target audiences*	– Contractual Necessity, – Consent	Generally not longer than 2 years after the research ends. We may keep it longer if needed for analysis, legal reasons, or other legitimate purposes.
Educational Qualifications *(e.g., degree, educational institution, professional skills)*	*– Research segmentation* *– Analytical profiling* *– Audience targeting*	– Contractual Necessity, – Consent	Generally not longer than 2 years after the research ends. We may keep it longer if needed for analysis, legal reasons, or other legitimate purposes.
Personal Interests & Lifestyle	*– Understand behavioural patterns* *– Build research profiles* *– Create aggregate insights*	– Contractual Necessity, – Consent	Generally not longer than 2 years after the research ends. We may keep it longer if needed for

Categories of Personal Data MRA	**Purpose MRA** *(see Section 4.1.0 for details)*	**Possible Legal Basis MRA**	**Retention Period MRA** *(as outlined in Section 4.1.5)*
*(e.g., Data types: Lifestyle and Preferences, Hobbies and Personal Interests * Interests and Activities Community involvement)*			analysis, legal reasons, or other legitimate purposes.
Financial Details *(e.g., bank account number, IBAN, payment details)*	*– Process incentive payments or prize rewards*	– Contractual Necessity, – Consent – Legal Obligation (*where applicable)*	Up to **7 years** where legally required, otherwise based on agreement
Contact History *(e.g., support requests, participation records)*	*– Customer service* *– Operational management* *– Resolve disputes or inquiries*	-Legitimate Interest *(Customer service, operational purposes)* – Consent (*Marketing-related communications)*	Generally not longer than 2 years after the research ends. We may keep it longer if needed for analysis, legal reasons, or other legitimate purposes.
Unique IDs (*e.g., survey identifiers, panel participant IDs)*	*Security measurements: Anonymizing or Pseudonymizing data for research* *Ensure data quality* *Maintain platform functionality*	– Contractual Necessity, – Consent, – Legitimate Interest	Generally not longer than 2 years after the research ends. We may keep it longer if needed for analysis, legal reasons, or other legitimate purposes.
In some circumstances **Public Information**	*For research and statistical goals (Desk research, social Media analysis), draw up collective profiles, profiling,*	– Legitimate Interest *(Research and analysis)*	Max. 18 months, or earlier if an objection is submitted.

Categories of Personal Data MRA	**Purpose MRA** *(see Section 4.1.0 for details)*	**Possible Legal Basis MRA**	**Retention Period MRA** *(as outlined in Section 4.1.5)*
(e.g., publicly available social media data or records)	*processing your answers to surveys and provide results to the client.*		
Photos, Images, or Sound Recordings (Audio-visuals) *(e.g., Audio-visual content that it's either created during research activities or uploaded/posted by the participant.*	**See Section 4.1.0 for details.** *Used during specific research activities or uploaded by you* *– May be part of interviews or diary studies*	– Contractual Necessity (*if stated as essential part of the Research)* – Explicit Consent (All identifiable recordings)	Generally not longer than 2 years after the research ends. We may keep it longer if needed for analysis, legal reasons, or other legitimate purposes.

In special cases, we comply with applicable local laws regarding children's personal data.

Children's Personal Data: *We allow children under the age of 16 to participate and process personal data in accordance with applicable local laws. We collect personal data from users under the age of 16 or the lower age limit only to*	**See Section 4.1.0 for details.** *Manage participation of minors where permitted* *– Ensure compliance with legal obligations*	– **Explicit consent** from both the child (if applicable) and their legal guardian	Same retention rules apply: no longer than **2 years** after research ends

the extent permitted and in compliance with legal requirements			

Additional Notes

- Unless we inform you otherwise and have a valid legal basis, **FRC (Hong Kong) Limited only uses your data for the purposes described above**.
- If we plan to use your personal data for new or additional purposes, we will notify you in advance and seek your **explicit consent** if required. For example: we will not use Your Personal Data for advertising purposes unless You have freely given Your explicit and prior consent.

4.2 Business Operations: Data Processing for Clients, Partners, and Applicants (Non-MRA)

This section explains how we **handle your Personal Data for general business purposes, outside** of specific market research activities (MRA).

4.2.0 What We Use Your Data For (Purpose) in General

These purposes include

- Communicating with clients and suppliers.
- Managing our contractual relationships.
- Marketing our services (where permitted by law).
- Running our internal operations efficiently.
- Managing applications (e.g., job applications).
- Ensuring security and preventing fraud.

If we intend to use your Personal Data for purposes not originally communicated, we will inform you in advance.
For example, we may use your data for direct marketing **where permitted by law and based on our Legitimate Interest**, but you will always have

the right to opt out at any time.
Where required, we will ask for your **explicit consent** before sending marketing communications..

4.2.1 Data Sources

We collect personal data from a few different places:

- **Directly from you**: When you contact us, fill out forms, or otherwise provide us with your information.
- **Publicly available sources**: We may use sources like LinkedIn or Indeed to find information relevant to our business activities/operations.
- **Third parties**: We may receive your data from other companies or organizations, but only when legally permitted.

Important: If we get your data from a source other than directly from you, we will let you know where we got it when we first contact you. If you want us to remove your data from our systems, we will do so promptly.

4.2.2 Our legal basis for using your Data

Data protection laws require us to have a valid legal reason for processing your personal data.

Here's what we rely on:

Legal Basis	**Description**
Consent *(where required by law)*	*If we rely on your consent to process your data (e.g., for sending you newsletters), we will always ask for your explicit and informed consent. You can withdraw your consent at any time. See the "Your Rights" section below for details on how to do this.* *We will only use your data if you have given us clear consent to do so for a specific purpose.* *(e.g., Newsletter subscriptions (you must opt-in and can unsubscribe easily).*

Legal Basis	Description
Contractual Necessity	*We need to process your data to fulfil our obligations under a contract we have with you. (e.g., Managing our business relationship with you.)*
Legitimate Interest	*We may process your data based on our legitimate business interests, as long as those interests don't override your rights and freedoms. We always consider the impact on your privacy (e.g., improving our services, enhancing security, and some direct marketing).* *We believe we have Legitimate Interests in:* • *Improving our services.* • *Making our systems more secure and preventing fraud.* • *Conducting direct marketing (where legally allowed and with opt-out options).* • *Providing excellent customer service and responding to your inquiries.* ***Your Right to Object:*** *You have the right to object to our processing of your data based on Legitimate Interests. Please contact us to exercise this right.*
Legal obligations	*If the processing is necessary to fulfil legal obligations*

4.2.3 Data Protection Measures:

We implement various safeguards to protect your data:

- **Pseudonymization**: Minimizing the use of identifiable data.
- **Data Minimization**: Collecting only essential data for research purposes.
- **Secure Deletion/Anonymization**: Securely deleting or anonymizing data once it is no longer needed.

(Refer to "6. **How We Keep Your Data Safe**" for further details)

4.2.4 Retention Periods:

Personal data is retained according to legal standards and business needs, with secure deletion or anonymization after the retention period.

If necessary, data may be retained for up to three additional years, in compliance with legal warranty obligations

Please note: Applicant data will be deleted after the completion of the recruitment process in accordance with legal requirements.

4.2.5 Overview What data we collect and why

Below is an overview of the categories of data we may process, their purposes, legal grounds, and retention periods.
In special cases, we comply with applicable local laws.

Categories of Personal Data	**Purpose** (Cf. **4.2.2. Purpose)**	**Legal bases**	**Retention Period BA** (Cf. **4.2.5 Retention Periods)**
Contact information *(e.g., Name, e-mail address, phone number or any other relevant contact details)*	*To contact you, provide information, direct marketing, advertising, CRM, website logins.*	*– Contract,* *– Consent,* *– Legitimate Interest*	*Data is kept while our agreement is active, or until you withdraw consent/object, plus up to three years where legally required*
Demographic data or basic personal information *(e.g., Age, date of birth, place of birth, gender, civil status, nationality)*	*Job applications,* *Statistics, CRM*	*– Contract,* *– Legitimate Interest* *(Customer relationship)*	*Data is kept while our agreement is active, or until you withdraw consent/object, plus up to three years where legally required*

Contact history *(e.g., mails, phone call logs, purchase history)*	*To manage business, client, and supplier relationships, and to support marketing efforts.*	*– Contract,* *– Consent,* *– Legitimate Interest*	*Data is kept while our agreement is active, or until you withdraw consent/object, plus up to three years where legally required*
Educational and professional background information. *(e.g., CV, education, degree, certificates, professional skills and activities.)*	*For job applications, research, and statistical goals.*	*– Contract,* *– Consent,* *– Legitimate Interest*	*Data is kept while our agreement is active, or until you withdraw consent/object, plus up to three years where legally required*
Public information. *e.g., Publicly available information, information on social networks.*	*Assessing qualifications for recruitment, verifying professional information.*	*– Legitimate Interest*	*18 months as of any objection has been filled.*
Financial details. *(e.g., Bank details, (branch identifiers, sort code, IBAN, BIC, account number.)*	*Accounting, invoicing, CRM.*	*– Contract,*	*In accordance with legal retention periods by national law (up to 10 years).*
Special categories of Personal Data: *(e.g., Information on race and origin, political opinions, religious or*	*Complying with legal requirements, managing relationships, providing services. We minimize processing this type of data.*	*– Explicit Consent, – Data made public by yourself.*	*Data is kept while our agreement is active, or until you withdraw consent/object, plus up to three years where legally required*

philosophical beliefs, trade union membership, physical or mental *health, genetic data, biometric data, sexual life or sexual orientation.)*			
***Unique ID's**:* *(e.g., Information that we collect in questionnaires or panels, participants unique identification number.)*	*statistical purposes, for anonymizing or Pseudonymizing data.*	*– Contract,* *– Consent,* *– Legitimate Interest*	*We keep your data until our agreement ends, you withdraw consent, or object. After that, we delete or anonymize it, unless the law requires us to keep it longer (up to three years).*
Electronic (online) identification & Meta data	*Verifying user identity, managing systems, ensuring security, operational efficiency.*	*– Contract,* *– Consent,* *– Legitimate Interest*	*We keep your data until our agreement ends, you withdraw consent, or object. After that, we delete or anonymize it, unless the law requires us to keep it longer (up to three years).*

Important note: In specific cases, we adhere to applicable local laws, which may require different handling of your data.

5. How We Keep Your Data Safe

How we protect your Personal Data

At FRC (Hong Kong) Limited, we take the security of your Personal Data seriously. We have implemented appropriate **technical and organizational measures** to protect your data against unauthorized access, loss, or misuse. These safeguards are designed based on the **sensitivity, format, location, and storage** of the data and include:

- **Encryption and Data Masking:** We protect your data when it is sent over the internet (for example, with SSL encryption) and when it is stored.

- **Access Controls:** Only authorized staff and trusted third parties who need your data for their work can access it.
- **Firewalls & Security Protocols** – Using industry-standard security measures to prevent unauthorized access.
- **Data Loss Prevention (DLP)** – We use AI-assisted tools to detect and prevent data leaks, such as scanning emails and attachments for sensitive information. Any suspicious activity is checked by our team.

Any processing of Personal Data in relation with security measurements is carried out under the following **legal bases**:

- **Legitimate Interest** – Ensuring data security.
- **Legal obligations** – Compliance with applicable data protection laws and or cybersecurity laws.
- **Contractual obligations** – Implementing security measures where required to protect confidential data.

All FRC (Hong Kong) Limited employees, contractors, and third parties handling your Personal Data are bound by **strict confidentiality agreements** and must follow our security policies. Access to data is limited to those who require it for legitimate business purposes.

6. Sharing and Transfers of Personal Data

We only share your Personal Data when necessary and legally permitted to fulfil the purposes outlined in this Statement.

When we share your data, we implement contractual safeguards and security measures to ensure compliance with data protection, confidentiality, and security standards. All third parties must meet our strict confidentiality and security requirements.

6.1. Who We Share Data With

- **Within the FRC (Hong Kong) Limited:** To enable efficient internal operations and business continuity. All entities adhere to the same high standards of data protection and confidentiality.
- **Our Clients (as Data Controller and Sponsor of the MRA)**: We conduct **Market Research Activities on behalf of clients**, who **are considered the "Data Owners**." Sharing your data with them is necessary to deliver our services. If you participate in a survey, poll, or community discussion, your **screen name and posts may be visible** to us, other participants, and the client. Any posts you make to a survey,

poll or discussion in the community will in principle only be associated with your screen name. If you post any personally identifiable information yourself, we may at our discretion remove this for your own security. We recommend that you choose a screen name which does not resemble your real name. Also, in this context it is possible that we share photos, image recordings, sound recordings or full datasets (e.g., answers to survey questions to help inform them about specific elements of their offer) we hold of you. Your contributions (e.g., survey responses, photos, recordings) may be shared as pseudonymized or anonymized data, and sometimes in full form if required by the research.

Important: Our Client may combine data collected from the Market Research Activity carried out by Us on behalf of our clients with other data that they may hold about you. This Statement does not describe our client's specific uses of your personal data, which information will be provided to you separately if this would deviate from the Market Research Purposes as set out above, but if you are not happy with your responses being used in this way, you should notify us prior to agreeing to participating to one of the Market Research Activities for which you are invited and for which you need to accept this Statement and any relevant terms and conditions of use. We can then determine with the client whether the use of your data can be limited and in that case whether it is possible to take part in the specific Market Research Activity.

- **Research Partners/Service Providers (Supplier/Sub-Processor):** We work with trusted external partners (e.g., moderators, interpreters, data processors) who help us run and support research. All partners are contractually bound to confidentiality, follow our strict data security requirements, and act only on our instructions.
- **Law Enforcement or Regulatory Authorities**: We may disclose Personal Data when required to comply with legal obligations or protect our legal rights.

6.1.1 Overview of Sharing Scenarios, Legal Bases, and Safeguards

Scenario	**Purpose**	**Legal Basis**	**Safeguards**
1. Internal – within FRC (Hong Kong) Limited	*To enable efficient business operations and support Market Research and Business Activities/Operations.*	*Legitimate interest in efficient business operations.*	*Intra-Company Agreement ensuring compliance with data protection standards. All entities adhere to the same data protection and security requirements.*

2. With Our Clients (*as Data Controllers and Sponsors of the MRA)*	*To conduct Market Research Activities (MRA) on their behalf. Clients receive insights based on research findings, including pseudonymized and/or anonymized data.* *May include voluntary contributions (e.g., photos, recordings, survey responses).*	*– Necessary for contract performance.* *– Legitimate Interest in delivering services.* *– Explicit consent when required.*	*Data Processing Agreement (DPA) or Joint Controller Agreement (JCA).* *EU Standard Contractual Clauses (SCC) for international transfers.*
3. With Law Enforcement or Regulatory Authorities	*To comply with legal obligations, respond to lawful requests, or protect legal rights*	*– Legal obligation.* *– Legitimate Interest in legal defence.*	*Disclosure limited to what is legally required. Confidentiality safeguards where applicable.*

6.2 No Unauthorized Data Sharing

- We do not sell, rent, or lease your data to third parties as defined under the PDPO
- We do not share Personal Data collected for one client with another. We maintain clear boundaries between client engagements to avoid cross-contamination of data.

6.3 Transfer of Data inside and outside Hong Kong

Cross-border Data transfer:

As a global network, your Personal Data may be transferred outside the country where it was originally collected.

We may transfer Personal Data to clients or third-party service providers located outside your country to facilitate Market Research and Business Activities/Operations.

Your Personal Data may be processed in jurisdictions with different data protection standards.
However, we comply with the high standards of the PDPO and other applicable privacy regulation and implement appropriate safeguards to protect your data, regardless of location.

- When transferring data outside Hong Kong, we ensure that Personal Data is handled securely and lawfully.

We carefully assess each transfer on a case-by-case basis and ensure that all necessary agreements and security measurements that your data remains protected. Additionally, we maintain internal data protection agreements across our organization to uphold the PDPO compliance and security standards.

Where required by applicable privacy laws, we will obtain your explicit consent before transferring your data outside the jurisdiction where it was collected. This applies to transfers for Market Research Activities (MRA).

7. Your Rights under Data Protection Law(s)

Under various data protection laws, including but not limited to the PDPO, you have certain rights regarding your Personal Data. Under data protection laws like the PDPO, you have specific rights regarding your personal data. Some of these rights may be limited or subject to exceptions, depending on local laws.

Right	**Description**	***Possible limitations/exceptions***
Right to Access	You can ask us what personal data we have about you and get a copy of it.	*We may deny access if it affects the rights and freedoms of others or if the request is clearly unreasonable.*
Right to Rectification	You can ask us to correct any information about you that is wrong or incomplete.	*None*
Right to Erasure (‘Right to be Forgotten’)	You can ask us to delete your personal data in certain situations.	*We do not have to delete your data if we need it to comply with a legal obligation, for public interest reasons, or for legal claims. If we delete your data, we will inform third parties processing your data about the request.*

Right	Description	*Possible limitations/exceptions*
Right to Restrict Processing	You can ask us to limit how we use your personal data in specific situations.	*We can continue processing your data if it is needed for legal claims or to protect the rights of others.*
Right to Data Portability	You can ask for your data in a format that you can easily use and transfer to another organization, where technically feasible.	*This only applies to data you gave us and that we process based on your consent or a contract.*
Right to Object	You can object to us using your data for Legitimate Interests, including direct marketing. If you object to direct marketing, we will stop.	*We can continue processing if we have compelling legitimate grounds that override your interests.*
Right to Withdraw Consent	If we use your data based on your consent, you can withdraw it at any time. Withdrawing your consent doesn't affect what we did with your data before you withdrew it.	*Withdrawal does not apply where processing is required by law.*
Rights Related to Automated Decision-Making	You have the right not to be subject to decisions based solely on automated processing, including profiling, that significantly affects you, unless the processing is necessary for a contract, authorized by law, or based on explicit consent.	*Does not apply if processing is necessary for a contract, authorized by law, or based on explicit consent.*

Important notes:

- **No "Automated Decision-Making"**: We do not use automated decision-making or profiling (as defined by data protection laws) when processing your Personal Data for market research activities. All processing involves human oversight.
- **Exercising Your Rights:** It is generally free to exercise your rights. However, if a request is clearly unfounded or excessive, we may charge a reasonable fee or decline the request.

- **Response Time:** We will respond to your request within 4 weeks /one month (for simple requests) or three months (for complex or multiple requests).
- **Exceptions:** Certain exceptions may apply when exercising these rights, meaning you may not be able to fully exercise them in all situations, and this may be further limited by national/local laws.

- **Right to lodge a complaint:** If you are unsatisfied with how we process your data, you have the right to file a complaint with the relevant data protection authority (Contact information see section 11).
  However, we encourage you to contact us first, so we can address your concerns directly.

8. Updates to this Statement

FRC (Hong Kong) Limited may modify and update this Statement at any time. The latest update date is displayed at the top of this Statement, and the most recent version will always be accessible on our websites. We encourage you to check our websites regularly to stay informed about our latest Statement and practices.

9. How to contact us

To exercise your rights or for more information, please contact us using the provided contact details. We will review your request and respond in accordance with applicable laws.

9.1 FRC Data Protection Officer (DPO)

9.1.1 FRC Data Protection Officer (DPO):

We have appointed a Data Protection Officer (DPO) to oversee compliance with data protection laws, including the PDPO. The DPO is supported by a data protection team responsible for implementing data protection measures across the organization. We also engage external legal advisors for additional support.

For privacy-related questions, data subject requests, or complaints, please contact the FRC (Hong Kong) Limited via:

- **Email**:
- **Phone**:
- **Postal Mail**:

9.1.2 Roles and Responsibilities

- **Processor/Joint Controller Scenarios**: The DPO acts on behalf of FRC (Hong Kong) Limited. When FRC (Hong Kong) Limited processes data for clients (e.g., Market Research Activities), the DPO serves as a primary contact but may redirect specific data subject requests to the client (controller) as needed. The DPO ensures that requests are addressed within the timeframes specified by the PDPO

10. Lead Supervisory Authority

In accordance with PDPO, we have designated the Privacy Commissioner for Personal Data as our Lead Supervisory Authority, as FRC (Hong Kong) Limited's main establishment is located in Hong Kong. The Lead Supervisory Authority is primarily responsible for overseeing our cross-border data processing activities. We encourage you to direct any complaints regarding FRC (Hong Kong) Limited's processing of your Personal Data to this authority.

Contact Details for the Privacy Commissioner for Personal Data:

- **Name**: Privacy Commissioner for Personal Data
- **Address**: Unit 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong
- **Telephone**: +852 2827 2827
- **Email**: communications@pcpd.org.hk
- **Website**: https://www.pcpd.org.hk/english/about_pcpd/commissioner/commissioner.html

You also have the right to lodge a complaint with your local data protection authority.

11. Translations of this Statement (alternative languages)

The primary language of this Privacy Statement is English.

For your convenience, AI-generated translations into other languages are provided below. Please note that these translations are provided as a courtesy and may not fully capture the nuances of the original text. In the event of any discrepancies between the translations and the English version, the English version shall prevail. We strive to ensure the accuracy of these translations, but we recommend consulting the English version for legal purposes.

Privacy Policy – FRC (Hong Kong) Limited