Absolute Internship Company Limited

Data Protection & Privacy Policy

Version: 2.0
Effective Date: [01/11/2025]
Last Updated: [01/11/2025]

1. Who we are and scope

Absolute Internship Company Limited, a company incorporated in Hong Kong (Company No. 1426978) and having its registered office at 9/F Amtel Building, 148 Des Voeux Road, Central, Hong Kong ("Absolute Internship", "AI", "we", or "us"). This policy explains how we handle personal data under Hong Kong's legislation:

- Hong Kong's Personal Data (Privacy) Ordinance, Cap. 486 (PDPO), and applicable guidance from the Office of the Privacy Commissioner for Personal Data (PCPD). ● Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR). ● Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD).

This policy applies to personal data processed in Hong Kong, Spain, and internationally when providing our services.

2. Contact

- **Data User/Controller**: Absolute Internship Company Limited
- **Registered address (Hong Kong)**: 9/F Amtel Building, 148 Des Voeux Road, Central, Hong Kong
- **Privacy contact/ role**: Data Protection Lead — info@absoluteinternship.com

Absolute Internship acts as the **Data Controller** for the personal data collected from Participants, applicants, and clients in connection with its Programs.

Where Absolute Internship collaborates with third-party entities — including Host Companies, accommodation providers, or technology partners — these entities may act as:

● **Data Processors**, when they process personal data on behalf of Absolute Internship and under its documented instructions, or
● **Joint Controllers**, where both parties jointly determine the purposes and means of processing.

In such cases, each party remains responsible for its respective obligations under applicable data protection laws.

This approach also aligns with the accountability principles under the PDPO and relevant PCPD guidance.

3. What we collect

Depending on your relationship with us (student, partner, company, employee, other), we may collect: Identification and contact details, account credentials, billing and transaction data, service usage and logs, communications, and limited HR/recruitment data. We collect only data that is adequate, relevant, and limited for stated purposes in our services in line with GDPR Article 5(1)(c) and (DPP1, DPP2).

We do not collect sensitive data (health, religion, etc.) unless strictly necessary and with your explicit consent.

4. How and why we use personal data (PDPO legal bases)

Under the PDPO, we must **collect for a lawful purpose, and use consistently with the original purpose** or where prescribed consent is obtained for new uses (DPP1, DPP3). Typical purposes include, but not limited to: providing services, account administration, billing, customer support, security and fraud prevention, analytics to improve services, legal compliance, and recruitment. Where we rely on **direct marketing**, we follow the GDPR and PDPO's direct-marketing rules (see section 9).

Legal bases (GDPR Art. 6) for the collection of data:

- Consent: when you voluntarily provide data or accept marketing communications.
- Contractual necessity: to perform a service you have requested.
- Legal obligation: to comply with tax, accounting, or employment laws.
- Legitimate interest: to improve our services, prevent fraud, and maintain security.

Under the PDPO, data is collected and used only for the original lawful purpose, unless prescribed consent is given for new uses.

5. How we collect data

We collect personal data through several legitimate and transparent channels, always in accordance with Regulation (EU) 2016/679 (GDPR), Organic Law 3/2018 (LOPDGDD), and Hong Kong's Personal Data (Privacy) Ordinance (PDPO).

Our goal is that you are always informed about how, when, and from where we obtain your personal information.

We may collect data in the following ways:

- Directly from you
- Automatically through our digital platforms
- From third parties: we may also use publicly available sources (e.g., LinkedIn, professional directories, or institutional websites) to verify or supplement existing information.

All third-party transfers or collections comply with data protection regulations, and we ensure that the source has lawfully obtained your consent or is otherwise authorised to share the data.

Legal reference: GDPR Article 14 - PDPO DPP3 – Use consistent with the original lawful purpose.

We do not buy, rent, or sell personal data from external databases.
If we ever receive your personal data from a third party and not directly from you, we will inform you within a reasonable period of time, explaining the source, purpose, and your rights under the law.

6. Retention

We keep personal data **no longer than is necessary** for the fulfillment of the purpose for which the data is or is to be used,required by applicable laws (GDPR Art. 5(1)(e) / DPP2). Once no longer needed, data is securely deleted or anonymised. We maintain and apply a **retention schedule**.

7. Security

We take **all reasonably practicable steps** to protect personal data against unauthorized or accidental access, processing, erasure, loss or use, including technical and organizational measures required by GDPR Art. 32 and DPP4 Where third parties process data for us, we establish data processing agreements ensuring compliance and security.

8. International transfers

Because Absolute Internship SL operates in both Spain and Hong Kong, some personal data may be transferred between jurisdictions or to third countries when necessary for service provision or operational purposes.

We ensure that all such transfers are performed in full compliance with applicable data protection laws.

For transfers from Spain or the European Union
We comply with Chapter V of the GDPR and Articles 44–49, as well as Title V of the LOPDGDD, ensuring that personal data leaving the European Economic Area (EEA) is subject to an adequate level of protection.

To achieve this, we may:

- Use the European Commission's Standard Contractual Clauses (SCCs) with recipients located outside the EEA.
- Transfer data only to countries officially recognised by the European Commission as providing an adequate level of data protection.
- Conduct Transfer Impact Assessments (TIAs) and apply technical and organisational safeguards, such as encryption, pseudonymisation, and strict access controls. ● Keep a record of international data transfers and periodically review the adequacy of implemented safeguards.

For transfers from Hong Kong

Although Section 33 of the Personal Data (Privacy) Ordinance (PDPO) which restricts cross-border transfers has not yet commenced, we follow the guidance of the Office of the Privacy Commissioner for Personal Data (PCPD) and apply equivalent standards.

Specifically, we:

- Use the PCPD's Recommended Model Contractual Clauses (RMCs) when sharing personal data with overseas recipients or processors, ensuring comparable levels of protection. ● Conduct risk assessments before any transfer and implement security measures such as encryption and access limitation.
- Maintain a register of regular cross-border transfers and applicable safeguards. ● For transfers between Hong Kong and Mainland China, we assess and, where appropriate, adopt the Guangdong–Hong Kong–Macao Greater Bay Area (GBA) Standard Contract or other legally recognised mechanisms.
- All international data transfers are documented and reviewed regularly to ensure ongoing compliance, accountability, and transparency under both the GDPR and the PDPO.

9. Direct marketing

We will only use or provide your personal data for **direct marketing** if we have complied with the PDPO's **notice and consent** regime — including giving you prescribed information, obtaining your consent, and honoring your opt-out at any time. We also comply with the **Unsolicited Electronic Messages Ordinance (UEMO)** when sending electronic marketing.

Our approach follows both European and Hong Kong data protection laws:

- GDPR Article 21 and LSSICE Article 21 (Spain/EU): we must obtain your prior and explicit consent before sending any electronic commercial communication (e.g., newsletters, promotional emails, or event invitations).
- PDPO Sections 35A–35M (Hong Kong): we are required to inform you before using your personal data for direct marketing, explain the intended purpose and the types of data used, and give you the right to opt out at any time.

We intend to use your name, contact details, service history, and preferences for **direct marketing** of our services. We will not use your personal data for direct marketing unless we have obtained your **consent** If you consent, you may **opt out at any time** via email. We may also provide your personal data to providers and partners for their direct marketing of services, but only with your consent or absence of objection. You can choose whether or not to receive our communications:

- When subscribing, registering, or completing forms on our website, you will have the option to give or withhold consent to receive marketing communications.
- You can withdraw your consent or opt out at any time by sending an email to: info@absoluteinternship.com

Once you withdraw consent, we will immediately update our records to ensure you no longer receive promotional messages.

However, you may still receive service-related communications (for example, billing, security, or operational notices) that are not considered marketing.

10. Your rights

You have the right to know whether Absolute Internship Company Limited is processing personal data that concerns you.

In accordance with the Personal Data (Privacy) Ordinance (PDPO) and the General Data Protection Regulation (GDPR), the Organic Law 3/2018 (LOPDGDD), you may exercise the following rights:

- Access: to request confirmation about whether we process your data and to obtain a copy of the information we hold about you.
- Rectification: to request correction of inaccurate or incomplete data.
- Erasure: to request the deletion of your data when it is no longer necessary for the purposes for which it was collected or when you withdraw your consent.
- Restriction: to request limitation of processing, in which case we will keep your data only for exercising or defending legal claims.
- Objection: to object to certain processing, including direct marketing. In this case, we will stop processing your data unless there are compelling legitimate reasons or necessary legal defences.
- Portability: to request that your data be provided in a structured, commonly used format or transferred to another data controller, where technically feasible.

- Withdraw consent: to withdraw your consent at any time, without affecting the lawfulness of processing carried out before withdrawal.

You may exercise these rights by contacting our Data Protection Officer (DPO): info@absoluteinternship.com

Please include a copy of your ID or any other valid document confirming your identity, and indicate clearly which right you wish to exercise.

If you believe that your rights have not been properly respected, you have the right to file a complaint with the relevant authority:

- In Hong Kong: Office of the Privacy Commissioner for Personal Data (PCPD)

11. Cookies and online tracking

We use cookies and similar technologies for essential functions, analytics, and — where applicable — marketing. You can manage cookies through your browser settings, and we will obtain consent where required by local law in the place of access. In Spain and the EU, cookies requiring consent are managed through a cookie banner, in accordance with LSSICE and AEPD guidelines.

In Hong Kong, we follow the PCPD guidance on online tracking.

12. Data breach handling

Below you can find our Data Breach Response Plan, which outlines the steps Absolute Internship will follow in the event of a personal data breach. **If a breach occurs, we will:**

- Contain the incident and secure systems.
- Assess the risks and affected data subjects.
- Notify the PCPD and affected individuals as appropriate, and communicate mitigation steps.
- Keep records and conduct a post-incident review.

Under GDPR, serious breaches are reported to the AEPD within 72 hours.
Under PDPO, notification to the PCPD is recommended “as soon as practicable” when there is a real risk of harm.

13. Children

Where personal data is collected from a minor under the age of eighteen (18), Absolute Internship will ensure that consent is validly obtained in accordance with Article 8 of the GDPR and Article 7

of the Spanish Organic Law 3/2018 (LOPDGDD).
In Spain, valid consent for the processing of personal data in connection with digital or online services generally requires the individual to be at least fourteen (14) years of age. If the Participant is under 14, consent must be provided or authorised by the holder of parental responsibility.

In other jurisdictions where a higher age threshold applies, Absolute Internship will comply with the applicable local requirement.

Absolute Internship reserves the right to request verification of parental consent where appropriate.

14. Third-party links and services

Our services may link to sites or services operated by third parties with their own privacy practices. We are not responsible for the privacy practices of third parties. Please, review those policies before providing personal data.

15. Changes to this policy

We may update this policy to reflect operational, legal or regulatory changes. We will indicate the "Effective date" and, for material changes, provide a clear notice.

16. Governing Law

This Privacy Policy is governed by Spanish law, specifically the GDPR, LOPDGDD, and LSSICE.

For international activities, including those carried out in Hong Kong, Absolute Internship Spain S.L. also ensures compliance with the Personal Data (Privacy) Ordinance (PDPO).

In case of dispute, the parties submit to the courts of Barcelona (Spain), without prejudice to any mandatory provisions of local law.

Annex A — PDPO Mapping (summary)

Topic	PDPO reference	How we address it
Collection — fair and lawful purpose notice	**DPP1**	Provide clear notices stating purposes, classes of transferees, and whether provision is voluntary/obligatory.

Accuracy and retention	**DPP2**	Maintain accuracy checks and retention schedule; delete when no longer necessary.

Use consistent with purpose	**DPP3**	No new use unless **prescribed consent** obtained.
Security and processors	**DPP4/4(2)**	Technical/organizational measures; processor contracts.
Openness	**DPP5**	Publish this policy and internal manuals for staff.
Access/correction	**DPP6**	Data Access and Correction Request procedures.
Direct marketing	**ss.35A–35M**	Prescribed notice and consent; opt-out honored.
Electronic marketing	**UEMO Cap. 593**	Include unsubscribe; comply with DNC registers where applicable.
Cross-border transfers	**s.33 (not yet commenced)** + PCPD RMCs	Use PCPD RMCs/assessments; implement safeguards.
Data breach	PCPD Guidance	Notify **as soon as practicable** when risk of harm; keep records.

Annex B — GDPR / LOPDGDD Mapping (summary)

Topic	**Legal Reference (GDPR / LOPDGDD / LSSICE)**	**How we address it**

Lawful, fair and transparent processing	GDPR Art. 5(1)(a), Art. 6; LOPDGDD Art. 6–8	Personal data is processed lawfully, fairly and transparently. All processing activities are based on a valid legal ground such as consent, contractual necessity, legal obligation, or legitimate interest. Clear privacy notices are provided to all data subjects.
Purpose limitation	GDPR Art. 5(1)(b)	Data is collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
Data minimisation	GDPR Art. 5(1)(c)	Only data that is adequate, relevant and limited to what is necessary is collected and processed for each purpose.
Accuracy	GDPR Art. 5(1)(d)	Procedures are in place to maintain data accuracy and allow individuals to request correction of inaccurate or outdated information at any time.
Storage limitation (retention)	GDPR Art. 5(1)(e); LOPDGDD Art. 32	A retention schedule defines how long each category of data is kept. Once data is no longer needed, it is securely deleted or anonymised.
Integrity and confidentiality (security)	GDPR Art. 5(1)(f), Art. 32	Technical and organisational measures such as encryption, access controls, firewalls and processor agreements are implemented to ensure confidentiality, integrity and resilience of data processing systems.
Accountability and record keeping	GDPR Art. 5(2), Art. 24, Art. 30	Records of processing activities are maintained, and compliance responsibilities are documented to demonstrate accountability.
Data Protection Officer (DPO)	GDPR Art. 37–39; LOPDGDD Art. 34–37	
Data subjects' rights	GDPR Arts. 12–23; LOPDGDD Title III	

A Data Protection Officer has been appointed to monitor compliance, advise on data protection obligations, and act as a contact point for supervisory authorities and individuals.		
	Procedures exist to ensure individuals can exercise their rights of access, rectification,	erasure, restriction, objection, portability, and withdrawal of consent. Requests are handled within the legally established timeframes.
Children's data GDPR Art. 8; LOPDGDD Art. 7		
Parental or guardian consent is required for processing the personal data of minors under 14 years of age.		
	Data processors and third parties GDPR Art. 28–29 Data processing agreements are signed with all processors and partners to ensure compliance with GDPR and LOPDGDD requirements.	
International data transfers GDPR Chapter V (Arts. 44–49)	Transfers outside the EEA are based on EU Standard Contractual Clauses (SCCs) or adequacy decisions. Transfer	impact assessments and appropriate safeguards are applied.
	Privacy by design and by default GDPR Art. 25 Data protection principles are integrated into the design of new systems, projects and processes, ensuring privacy is considered by default.	
Data breach notification		Individuals may file complaints with the Spanish Data Protection Agency (AEPD) or contact the DPO for assistance in resolving any issues.
Electronic marketing and cookies	GDPR Arts. 77–79; LOPDGDD Art. 63	
	A documented incident response plan is in place. The AEPD and affected individuals are notified within 72 hours where required.	
Complaints and supervision GDPR Arts. 33–34; LOPDGDD Art. 33		
LSSICE Arts. 21–22	Prior consent is obtained before sending electronic commercial communications or using non-essential cookies. All marketing emails include an unsubscribe option.	