ASPEN PHARMACARE HOLDINGS LIMITED
AND ITS SUBSIDIARIES

("ASPEN", "THE GROUP" OR "ASPEN GROUP OF COMPANIES")

GENERAL PRIVACY NOTICE

---

1. INTRODUCTION

1.1. Purpose

This privacy notice explains how Aspen ("company", "we", or "us") collects, uses, and discloses personal data through our websites, direct interactions, and instances where other Aspen Privacy Notices does not apply, including how individuals may exercise their rights. We are committed to respecting your privacy and protecting your personal data under relevant data protection laws. This notice does not apply to employees, job applicants, or scenarios where more specific notices apply (such as pharmacovigilance). If you are interacting with us in an employment or candidate capacity or through other specialised programmes, please refer to the specific notice that applies to your relationship with us.

1.2. Scope

We conduct business across various jurisdictions and may localise this notice following local requirements. We do not knowingly collect personal data from children without obtaining parental consent or otherwise having another lawful basis. We do not intend this website for children. Where we discover that we have inadvertently collected personal data relating to minors, we will delete or anonymise it as soon as reasonably practicable.

1.3. Accountability

We encourage you to read this notice thoroughly. If you have any questions, please contact us using the details below. It is our policy to integrate privacy considerations from the outset and align with data protection by design and by default.

1.4. Legal and regulatory compliance.

We aim to comply with all relevant data protection laws that apply to our operations. We will update and refine our internal processes and documentation based on changes in applicable laws. Where local law imposes additional or stricter obligations, we will honour those requirements in the relevant jurisdiction.

2. FUNDAMENTAL PRINCIPLES

2.1. Processing limitation

2.1.1. We rely on lawful grounds such as contract, legitimate interests (provided your interests or fundamental rights do not override these), compliance with legal obligations, or (where required) your consent. Although we may seek consent where appropriate, we generally avoid using consent as the primary basis for processing unless it is legally required. We process personal data for various purposes, including:

2.1.1.1. Conducting our business activities (such as manufacturing, marketing and selling our medicines, managing payments, and administering contracts)

2.1.1.2. Executing agreements (such as due diligence checks or supplier screening)

2.1.1.3. Enabling website functionality (such as using cookies to improve user experience)

2.1.1.4. Fulfilling compliance obligations (such as responding to lawful requests)

2.1.1.5. Conducting marketing and communications (unless you opt-out in terms of relevant data protection laws)

2.1.1.6. Handling internal support (such as technical assistance)

2.1.1.7. Defending against legal claims (such as litigation or regulatory investigations)

2.1.2. If we intend to use personal data for a new purpose incompatible with the original one, we will endeavour to obtain consent or rely on another valid legal basis, where applicable.

2.2. **Data minimisation**

Our policies require that we only collect and retain data necessary for specific purposes, which is consistent with the data minimisation principle. We will endeavour to not request more information than is reasonably required, and limit data retention to what is needed to achieve lawful and legitimate objectives.

2.3. **Purpose specification**

2.3.1. We may collect personal data from a range of sources, including:

2.3.1.1. Directly from you (such as when you fill out forms)

2.3.1.2. Automatically from your device (for example, through cookies or similar technologies)

2.3.1.3. From publicly available sources (to the extent that applicable data protection laws allow)

2.3.1.4. From our employees (for example, if someone has listed you as an emergency contact)

2.3.1.5. From third parties (such as analytics providers or social media platforms, to the extent that applicable data protection laws allow)

We may also process aggregated or anonymised data to the extent that it is not personal data because no one can re-associate it with an individual. We will inform you if certain data is mandatory under law or contract. Failure to provide such data may prevent us from delivering our products or services.

2.4. **Data quality**

To ensure that the personal data we hold is accurate and up to date, please notify us if your information changes. Maintaining accurate data is important for you and Aspen, and helps us comply with our legal obligations. If we discover that personal data is inaccurate or no longer needed, we will endeavour to rectify, delete, or anonymise it as appropriate.

2.5. Openness and transparency

We provide notices and disclosures that explain our data practices, including any relevant cookies or analytics technologies. If we collect your personal data indirectly, we will inform you within a reasonable period, to the extent applicable data protection laws require. You may opt out of marketing or withdraw consent anytime by contacting us or using the unsubscribe link (where provided).

2.6. Security safeguards

Our policies require that we maintain technical and organisational measures to protect personal data from unauthorised disclosure or misuse. We endeavour to restrict access to authorised personnel and/or bind them with confidentiality obligations. We routinely assess our security posture to identify and mitigate potential risks.

2.7. Privacy by design and by default

We endeavour to embed data protection into our business processes. We routinely review our systems and procedures for compliance, carrying out impact assessments if a process poses a high risk to individuals.

2.8. Data subject participation

Subject to local law, you have rights such as accessing your data, rectifying inaccuracies, requesting erasure, restricting or objecting to processing, and seeking data portability. You may withdraw consent if processing is based on consent and to not be subject to decisions solely based on automated means, if such decisions significantly affect you. We may verify your identity before processing such requests. If you are dissatisfied with our response, you may complain to the relevant authority.

2.9. Handling special categories of personal data

We do not ordinarily collect special categories of personal data (such as health or biometric data) unless relevant laws mandate it or with your explicit consent. We only disclose such data when strictly necessary.

2.10. Automated decision-making

We do not generally engage in automated decision-making that produces legal or similarly significant effects. If we do so in the future, we will provide clear notice, including an explanation of the logic involved and your right to request human intervention, contest decisions, or express your views.

3. INTRA-GROUP TRANSFERS

3.1. Intra-group data processing

We may share personal data among entities within our group for internal business purposes (such as centralised IT services or payroll). All entities must comply with this privacy statement and any additional data protection obligations. Where required, we conduct data protection impact assessments before introducing new intra-group processing activities that may pose a high risk to individuals.

3.2. Cross-border transfers

If we transfer personal data to countries outside the one in which you reside, we implement appropriate safeguards (such as standard contractual clauses or binding corporate rules) to ensure compliance with international data transfer requirements. You may contact us for further details of these safeguards.

4. THIRD-PARTY DATA PROCESSORS

4.1. Due diligence

We may disclose or share personal data with third-party providers, business partners, advisors, affiliates, or social media platforms, but only for lawful, legitimate purposes. Our policies require that we conduct due diligence on these third parties to assess their security measures and other procedures for complying with data protection standards.

4.2. Contractual safeguards

Third parties processing data on our behalf do so under written contracts outlining their obligations, including confidentiality, security, and adherence to our instructions. They may not use personal data for any purpose other than the one agreed, and they must promptly inform us of any data breaches or inability to comply with contractual terms.

4.3. Monitoring and auditing

We may periodically review third-party relationships to confirm their ongoing compliance. In the event of a merger, acquisition, or sale of our assets, we may transfer your personal data to the acquiring entity under the same terms unless otherwise notified. Where our website links to external sites or resources, we recommend reviewing their respective privacy notices, as we do not control third-party practices.

5. ENFORCEMENT AND COMPLIANCE

5.1. Internal reviews and training

We maintain protocols and internal policies to manage data security and protect personal data. Our employees receive training on data protection responsibilities. We periodically review our practices to assess compliance with legal and regulatory obligations.

5.2. Communication and awareness

This notice is easily accessible to stakeholders on our website and has been drafted in plain language so that our procedures are clear and easily understood.

5.3. Incident handling and notifications

We have internal protocols to identify, investigate, contain, and report personal data breaches. We will notify the relevant supervisory authority within the required period if a breach is likely to result in a risk to individuals' rights or freedoms. Where needed, we will also notify affected individuals without undue delay.

5.4. Addressing non-compliance

Any breach of this notice or relevant data protection laws may result in disciplinary action, termination of contractual relationships, or reporting to law enforcement, depending on the severity and applicable legal requirements. We foster a culture of accountability and encourage reporting any concerns so that we can address them promptly.

5.5. Policy review and updates

We review and update this statement at appropriate intervals to reflect changes in our data processing practices, legal requirements, or industry standards. The most updated version of this notice is the one accessible via our website. You may request previous versions of this statement by email or via our website contact form.

6. HOW TO CONTACT US

6.1. If you have any questions about this notice or wish to exercise your rights, please access our contact details here.

6.2. You may also complain to your local or national data protection authority if you believe we have processed your personal data unlawfully.