集团隐私政策

Group Privacy Policy

凯莱英医药集团（天津）股份有限公司（以下简称“**本公司**”、“**我们**”）作为一家致力于为全球制药、生物技术提供专业合同研发与生产服务（Contract Development and Manufacturing Organization, CDMO）的企业，深知个人信息与数据安全对于客户、合作伙伴、员工及所有相关方的重要性。我们始终将尊重并保护您的隐私视为企业运营的核心准则之一。

本《隐私政策》（以下简称“**本政策**”）旨在以清晰、透明的方式，向您阐明我们在业务活动中如何收集、使用、存储、共享、转让、删除及保护您的个人信息，并详细说明您依法享有的各项权利。我们严格遵循《中华人民共和国个人信息保护法》、《中华人民共和国数据安全法》、《中华人民共和国网络安全法》以及《信息安全技术个人信息安全规范》（GB/T 35273）等适用的法律法规、国家标准及监管要求，承诺采取业界领先的安全措施，持续优化信息安全系统，监测并处置各类信息安全威胁，不断完善数据治理体系，切实保障您的个人信息安全。

请您在访问我们的官方网站、使用我们的服务、参与我们的项目合作或与我们进行任何形式的业务互动之前，仔细阅读并充分理解本政策。如您对本政策内容或我们的个人信息处理活动有任何疑问、意见或建议，请通过本政策第十条所列联系方式与我们取得联系。

Asymchem Laboratories (Tianjin) Co., Ltd. (hereinafter referred to as “the Company”, “we” or “us”), as a professional Contract Development and Manufacturing Organization (CDMO) dedicated to serving the global pharmaceutical and biotechnology, fully recognizes the critical importance of personal information and data security to our clients, partners, employees, and all relevant stakeholders. We uphold the respect for and protection of your privacy as a core principle of our corporate operations.

This Privacy Policy (hereinafter referred to as “this Policy”) is designed to clearly and transparently inform you of how we collect, use, store, share, transfer, delete and protect your personal information in the course of our business activities, and to detail the rights you are entitled to under applicable law. We strictly adhere to the *Personal Information Protection Law of the People’s Republic of China*, the *Data Security Law of the People’s Republic of China*, the *Cybersecurity Law of the People’s Republic of China*, and the *Information Security Technology—Personal Information Security Specification* (GB/T 35273), along with other applicable laws, regulations, national standards, and regulatory requirements. We are committed to implementing industry-leading security measures, continuously enhancing our information security systems, monitoring and addressing various information security threats, and further strengthening our data governance framework to effectively safeguard your personal information.

We kindly request that you read and thoroughly understand this Policy before visiting

our official website, using our services, participating in our projects, or engaging with us in any form of business interaction. Should you have any questions, comments, or suggestions regarding the content of this Policy or our personal information processing activities, please contact us via the channels listed in Article X of this Policy.

第一条 适用范围与定义

1.1 适用范围

本政策适用于凯莱英医药集团（天津）股份有限公司及其所有子公司（以下统称“**本集团**”）在全球范围内开展的所有业务活动，特别是与 CDMO 服务相关的研发、临床试验支持、生产制造、质量控制、供应链管理及客户服务等环节。

1.2 定义

- **“个人信息”：**指以电子或其他方式记录的，与已识别或可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

- **“敏感个人信息”：**指一旦泄露或非法使用，容易导致自然人的人格尊严受到侵害或人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

- **“您”/“个人信息主体”：**指其个人信息被本集团处理的自然人，具体包括但不限于：（1）我们的客户及其授权代表；（2）参与由我们支持的临床试验的试验参与者；（3）我们的员工、求职者、实习生及顾问；（4）我们的股东；（5）我们的供应商、运输代理商、合作伙伴、承包商及其员工；（6）访问我们办公场所、研发中心或生产设施的访客；（7）我们网站及数字平台的用户；（8）与我们就业务、投诉或合作事宜进行联系的任何个人。

Article I: Scope of Application and Definitions

1.1 Scope of Application

This Policy applies to all business activities conducted globally by Asymchem Laboratories (Tianjin) Co., Ltd. and its subsidiaries (collectively, “the Group”), particularly those related to CDMO services, including research and development, clinical trial support, manufacturing, quality control, supply chain management, and customer service.

1.2 Definitions

- **“Personal Information”:** Refers to any information, recorded electronically or otherwise, that is related to an identified or identifiable natural person, excluding information that has been anonymized.

- **“Sensitive Personal Information”:** Refers to personal information which, if leaked or used illegally, is likely to infringe upon an individual's dignity or jeopardize their personal or property safety. This includes biometric data, religious beliefs, specific identities, health and medical information, financial accounts, location tracking data, and the personal information of minors under the age of fourteen.

- **“You” / “Data Subject”:** Refers to the natural person whose personal information is processed by the Group. This specifically includes, but is not limited to: (1) Our clients and their authorized representatives; (2) Trial participating in clinical trials supported by us; (3) Our employees, job applicants, interns, and consultants; (4) Our shareholders; (5) Our suppliers, shipping agents，partners, contractors, and their employees; (6) Visitors to our offices, R&D centers, or production facilities; (7) Users of our websites and digital platforms; (8) Any individual who contacts us regarding business, complaints, or cooperation matters.

第二条 个人信息的收集与使用

我们遵循“合法、正当、必要、诚信、公开、透明”的原则，并恪守“最小必要”准则，仅在实现特定业务目的所必需的范围内收集和处理个人信息。

2.1 我们收集的个人信息类型

根据您与我们的互动性质，我们可能收集以下类别的个人信息：

- **基本身份信息**：姓名、性别、出生日期、国籍、婚姻状况、联系方式（电话、电子邮件、地址、紧急联系人电话）等。

- **官方身份证明**：身份证、护照、工作证等。

- **职业与教育背景**：职位、工作单位、部门、员工编号、毕业院校、学历、专业资质、工作经验等。

- **财务与交易信息**：银行账户、发票信息、付款记录、税务识别号等（用于合同履行与财务结算）。

- **通信与互动记录**：与我们的邮件、通话、会议记录及在线表单提交内容。

- **设备与网络信息**：IP 地址、浏览器类型、操作系统、设备标识符、Cookie 信息及网站访问日志。

- **位置信息**：在您访问我们的实体场所时，可能记录的签到信息或大致地理位置。

- **其他信息**：在特定场景下，经您同意后收集的其他必要信息。

特别提示：作为 CDMO 企业，我们通常不会主动收集生物识别、健康生理、宗教信仰、性取向等个人敏感信息。仅在法律、法规或合同明确要求的特定场景下，并在获得您或相关方（如伦理委员会、申办方）的明确授权后，才会在严格保密和最小必要的前提下处理此类信息——例如，为支持临床试验、药物警戒（如不良事件报告）等医药研发与监管活动，或在员工考勤及高安全等级区域出入管理中（如经员工明示同意后，使用指纹或人脸识别进行身份验证）。

2.2 收集与使用的目的

我们处理您的个人信息主要用于以下合法目的：

- **履行合同义务：**为您提供 CDMO 服务，包括项目沟通、样品接收、产品运输、报告交付、发票开具及款项结算。
- **人力资源管理：**招聘、员工入职、在职管理、薪酬福利及离职手续办理。
- **合规与法定义务：**满足药品监管（如 GMP、GCP）、税务、审计及反洗钱等法律法规的要求。
- **安全保障：**管理对办公及生产区域的物理访问，以及维护 IT 系统与网络安全。
- **业务沟通与客户服务：**回应您的咨询、处理投诉、发送服务相关通知。
- **网站与系统运营：**优化用户体验、进行流量分析、诊断技术问题。
- **内部管理与运营：**进行必要的业务分析、风险管理及内部审计。
- **紧急情况下的必要处理：**为应对突发公共卫生事件，或者在紧急情况下为保护自然人的生命健康和财产安全所必需。

除非获得您的另行同意，我们不会将您的个人信息用于上述目的之外的用途。

Article II: Collection and Use of Personal Information

We adhere to the principles of “lawfulness, fairness, necessity, good faith, openness, and transparency”, and strictly comply with the “data minimization” principle, collecting and processing personal information only to the extent necessary to achieve specific business purposes.

Depending on the nature of your interaction with us, we may collect the following categories of personal information:

- **Basic Identity Information:** Name, gender, date of birth, nationality, marital status, contact details (telephone, email, address, emergency contact phone

number), etc.

- **Official Identification Documents:** National ID card, passport, work permit, etc.

- **Professional and Educational Background:** Job title, employer, department, employee ID, educational background, education level, professional qualifications, work Experience, etc.

- **Financial and Transactional Information:** Bank account details, invoice information, payment records, tax identification number, etc. (for contract fulfillment and financial settlement).

- **Communication and Interaction Records:** Content from emails, phone calls, meeting notes, and submissions via online forms.

- **Device and Network Information:** IP address, browser type, operating system, device identifiers, cookie information, and website access logs.

- **Location Information:** Check-in records or approximate geographic location when you visit our physical premises.

- **Other Information:** Other necessary information collected with your consent in specific scenarios.

Special Note: As a CDMO, we generally do not proactively collect sensitive personal information such as biometric data, health/physiological information, religious beliefs, or sexual orientation. Such information is processed only in specific scenarios explicitly required by law, regulation, or contract—and solely after obtaining your explicit consent or the authorization of relevant parties (e.g., an ethics committee or sponsor)—under strict confidentiality and on a data-minimization basis. These include supporting clinical trials and pharmacovigilance activities (e.g., adverse event reporting), as well as employee attendance and access control to high-security areas (e.g., using fingerprint or facial recognition for identity verification with the employee's explicit consent).

2.2 Purposes of Collection and Use

We process your personal information for the following lawful purposes:

- **Fulfilling Contractual Obligations**: To provide CDMO services, including project communication, sample receipt, product shipping, report delivery, invoicing, and payment settlement.

- **Human Resources Management**: For recruitment, onboarding, ongoing employment management, compensation & benefits, and offboarding procedures.

- **Compliance with Legal and Regulatory Obligations**: To meet requirements

from drug regulatory authorities (e.g., GMP, GCP), tax authorities, auditors, and anti-money laundering regulations.

- **Security Safeguards**: To manage physical access to our offices and production sites, and to maintain the security of our IT systems and network.
- **Business Communication and Customer Service**: To respond to your inquiries, handle complaints, and send service-related notifications.
- **Website and System Operations**: To optimize user experience, conduct traffic analysis, and diagnose technical issues.
- **Internal Management and Operations**: For necessary business analysis, risk management, and internal audits.
- **Processing necessary in emergencies**: To respond to public health emergencies, or where essential in urgent situations to protect the life, health, or property safety of natural persons.

Unless we obtain your separate consent, we will not use your personal information for any purpose beyond those listed above.

第三条 个人信息的共享、转让与披露

3.1 集团内部共享

为协同提供高效服务，您的个人信息可能会在本集团内部各关联公司之间共享，但仅限于实现本政策所述目的所必需的范围。

3.2 向第三方披露

我们仅在以下情况下向外部第三方披露您的个人信息：

- **服务提供商**：委托专业的 IT 服务商、物流供应商、会计师事务所等处理相关事务。我们将通过签订数据处理协议，合同中包含保密条款等形式，确保其仅按我们的指示处理数据，并承担同等的保密与安全义务。
- **法律与监管要求**：为遵守适用的法律法规、响应政府或司法机关的合法要求，或为保护本集团、客户、公众的重大合法权益而必须披露。
- **业务转让**：如发生合并、分立、收购或资产转让等情形，我们将确保个人信息的处理继续受本政策约束，并向您告知相关情况。

我们**不会**出于广告营销等目的，将您的个人信息出售或出租给任何无关第三方。

Article III: Sharing, Transfer, and Disclosure of Personal Information

3.1 Internal Sharing within the Group

To provide efficient and coordinated services, your personal information may be shared among the Group's affiliated companies, but solely to the extent necessary to achieve the purposes stated in this Policy.

3.2 Disclosure to Third Parties

- **Service Providers:** We engage specialized IT service providers, logistics vendors, accounting firms, etc., to handle related tasks. We will ensure, through data processing agreements, confidentiality clauses and other relevant terms are incorporated into the contract, that they process data only on our instructions and assume equivalent confidentiality and security obligations.

- **Legal and Regulatory Requirements:** To comply with applicable laws and regulations, to respond to lawful requests from government or judicial authorities, or where disclosure is necessary to protect the significant legal rights and interests of the Group, our clients, or the public.

- **Business Transfers:** In the event of a merger, division, acquisition, or asset transfer, we will ensure that the handling of personal information remains bound by this Policy and will inform you of the relevant situation.

We **will not** sell or rent your personal information to any unrelated third party for advertising or marketing purposes.

第四条 个人信息的跨境传输

原则上，我们在中华人民共和国境内收集和产生的个人信息，将存储于境内。因 CDMO 业务的全球化特性，在获得您明确同意或为履行与您的合同所必需的情况下，您的个人信息可能会被传输至境外。在此类情形下，我们将采取包括但不限于签订标准合同条款等措施，确保境外接收方提供同等水平的保护。

Article IV: Cross-border Transfer of Personal Information

In principle, personal information collected and generated within the territory of the People's Republic of China will be stored within the country. Due to the global nature of CDMO business, your personal information may be transferred overseas with your explicit consent or where necessary for the performance of a contract with you. In such cases, we will implement measures, including but not limited to executing standard contractual clauses, to ensure that the overseas recipient provides a comparable level of protection.

第五条 个人信息的保护、存储与问责机制

5.1 个人信息的保护、存储与安全事件响应

我们已建立了一套融合技术和管理手段的综合数据安全体系，以防止您的个人信息遭到未经授权的访问、公开披露、篡改、毁损或丢失。具体措施包括但不限于：

- **技术措施**：数据加密（传输与存储）、严格的访问控制与权限管理、防火墙、入侵检测系统、安全审计日志等。

- **管理措施**：制定并实施全面的信息安全管理制度，对员工进行定期的数据安全与隐私保护培训，并与接触个人信息的员工签署保密协议。

尽管我们已付出最大努力，但任何信息系统都无法保证绝对安全。如不幸发生个人信息安全事件，我们将立即启动应急预案，迅速遏制事态，并按照法律法规的要求，及时向监管部门报告，并在必要时通知受影响的个人信息主体。

我们仅在实现本政策所述目的所必需的期限内，或在法律法规、行业规范（如GMP/GCP）要求的保存期限内保留您的个人信息。保存期限届满后，我们将对您的个人信息进行删除或匿名化处理，使其无法再识别到特定个人。

5.2 违规行为的纪律处分与问责机制

本公司对任何违反本隐私政策的行为秉持“零容忍”原则。为确保政策的有效执行，我们已建立明确、分级且具强制力的纪律处分制度：

- **核心依据**：所有纪律处分均以《凯莱英医药集团（天津）股份有限公司价值观和行为准则》《数据安全与隐私合规管理办法》及与第三方签订的《数据处理协议》/合同保密条款为根本依据。

- **处分对象**：涵盖全体员工、管理层、临时工、实习生，以及所有第三方合作者（包括供应商、服务商、合作伙伴等）。

- **分级处分种类**：

    - **一般违规**：如未按规定进行数据访问审批、轻微操作失误等，将给予通报批评或合规再培训。

    - **严重违规**：如未经授权访问、复制或传输敏感个人信息，将视情节给予降职、暂停合作资格或经济处罚。

    - **重大违规**：指故意泄露、出售、滥用个人信息，或因严重失职导致大规模数据泄露，对公司声誉、客户权益或公共利益造成实质性损害的行为。对此类行为，公司将立即解除劳动合同或终止商业合作，并保留追究其民事及刑事责任的权利。

- **执行保障**：所有违规事件均由审计部牵头调查，所有违规事件应根据其性质由人力资源部（针对员工）或采购/BD 商务/项目协调管理办公室（针对

第三方）协同处理，处分决定需经运营办代表复核，确保程序公正、尺度统一、结果公平。

Article V: Protection, Storage, and Accountability Mechanisms for Personal Information

5.1 Protection, Retention, and Response to Security Incidents

We have established a comprehensive data security system integrating technical and managerial measures to prevent unauthorized access, disclosure, alteration, damage, or loss of your personal information. Specific measures include, but are not limited to:

- **Technical Measures**: Data encryption (in transit and at rest), strict access controls and permission management, firewalls, intrusion detection systems, and security audit logs.

- **Managerial Measures**: Formulation and implementation of a comprehensive information security management system, regular data security and privacy training for employees, and confidentiality agreements signed with employees who handle personal information.

While we have made our best efforts, no information system can guarantee absolute security. In the unfortunate event of a personal information security incident, we will immediately activate our emergency response plan to contain the situation and, in accordance with legal requirements, promptly report to the relevant regulatory authorities and, where necessary, notify the affected data subjects.

We will retain your personal information only for the period necessary to fulfill the purposes outlined in this Policy, or for the duration required by laws, regulations, or industry standards (e.g., GMP/GCP). Upon expiration of the retention period, we will either delete or anonymize your personal information so that it can no longer identify a specific individual.

5.2 Disciplinary Actions and Accountability for Violations

The Company maintains a “zero-tolerance” policy towards any violation of this Privacy Policy. To ensure effective enforcement, we have established a clear, tiered, and mandatory disciplinary system:

- **Core Basis**: All disciplinary actions are grounded in the *Asymchem Laboratories (Tianjin) Co., Ltd. Code of Conduct and Values*, the *Data Security and Privacy Compliance Management Measures*, and the *Data Processing Agreements/confidentiality clause* signed with third parties.

- **Subjects of Discipline**: This covers all employees, management, temporary staff, interns, and all third-party collaborators (including suppliers, service providers, and partners).

- **Tiered Disciplinary Actions**:
    - **Minor Violations**: E.g., failure to follow data access approval procedures or minor operational errors, resulting in public criticism or mandatory re-training.
    - **Serious Violations**: E.g., unauthorized access, copying, or transmission of sensitive personal information, leading to demotion, suspension of cooperation, or financial penalties, depending on the severity.
    - **Major Violations**: Defined as the intentional leakage, sale, or misuse of personal information, or gross negligence leading to a large-scale data breach that causes substantial harm to the Company's reputation, client rights, or public interest. In such cases, the Company will immediately terminate the employment contract or business cooperation and reserve the right to pursue civil and criminal liability.
- **Enforcement Assurance**: All violation incidents are investigated by the Audit Department. Depending on the nature of the incident, disciplinary actions shall be jointly handled by Human Resources (for employees) or Procurement / Business Development / Project Coordination & Management Office (for third parties). All disciplinary decisions must be reviewed by a representative from the Office of Operation Management to ensure procedural fairness, consistent application of standards, and equitable outcomes.

第六条 隐私合规与集团风险管理体系的整合

本公司已将隐私保护全面嵌入集团层面的风险管理与合规管理体系，实现从战略到执行的一体化治理：

- **预防机制：**通过隐私信息权限的控制，签署保密协议等措施预防隐私泄露。
- **风险评估工具：**我们采用标准化的《个人信息处理活动影响评估（PIA）模板》，在新项目启动、系统上线或业务模式变更前，系统性识别、分析和评估潜在的隐私风险，并制定相应的缓解措施。
- **管理措施整合：**本集团已建立完善的隐私合规管理体系。隐私合规目标已被纳入各业务单元的年度 KPI 考核体系，作为各级管理人员的重要考核指标。各部门负责人对其管辖范围内的数据处理活动负有直接管理责任，重大 IP 泄密事件作为一票否决项纳入各级管理人员考核评价，确保责任落实到位。
- **审计与监督：**集团内部审计部门不定期开展专项隐私合规审计，并可根据业务变化或风险事件触发临时审计。此外，我们定期聘请独立的第三方机构进行外部评估，确保我们的实践符合国际标准（如 ISO 27001）及最新监管要求。

- **持续改进：**所有审计发现、违规事件及监管反馈均被录入集团统一的风险登记册，并作为下一年度隐私培训、制度修订和资源投入的重要输入，形成闭环管理。

Article VI: Integration of Privacy Compliance into the Group's Risk Management System

The Company has fully integrated privacy protection into its enterprise-wide risk management and compliance system, achieving integrated governance from strategy to execution:

- **Preventive Measures**: Privacy breaches are prevented through controls over access to personal information, the execution of confidentiality agreements, and other appropriate safeguards.

- **Risk Assessment Tools**: We employ a standardized *Privacy Impact Assessment (PIA) Template* to systematically identify, analyze, and evaluate potential privacy risks before launching new projects, deploying systems, or changing business models, and to formulate corresponding mitigation measures.

- **Integrated Management Measures**: The Group has established a comprehensive privacy compliance management system. Privacy compliance objectives have been incorporated into the annual KPI evaluation framework of all business units and serve as a key performance indicator for managers at all levels. Department heads bear direct managerial responsibility for data processing activities within their scope of authority. Any major intellectual property or personal information breach is treated as a "one-vote veto" item in the performance evaluations of managers at all levels, ensuring clear accountability and effective implementation of responsibilities.

- **Audits and Oversight**: The Group's Internal Audit Department conducts periodic specialized privacy compliance audits and may trigger ad-hoc audits based on business changes or risk events. Furthermore, we regularly engage independent third-party institutions for external assessments to ensure our practices align with international standards (e.g., ISO 27001) and the latest regulatory requirements.

- **Continuous Improvement**: All audit findings, violation incidents, and regulatory feedback are logged into the Group's unified risk register and serve as key inputs for next year's privacy training, policy revisions, and resource allocation, forming a closed-loop management system.

第七条 您的权利

根据相关法律法规，您对您的个人信息享有以下权利：

- **知情权：**您有权以清晰、公开、及时的方式获知我们如何收集、使用、存储、共享、转让及保护您的个人信息，包括处理目的、所涉信息类

别、保存期限以及个人信息处理者的身份和联系方式。

- **访问权**：您可以请求查阅、复制我们所持有的关于您的个人信息。
- **更正权**：您可以要求我们更正或补充不准确、不完整的个人信息。
- **删除权**：在法定情形下（如我们处理目的已实现、您撤回同意等），您可以要求我们删除您的个人信息。
- **限制处理权**：在特定情况下（如您对信息准确性提出质疑期间），您可以要求我们暂停或限制对您个人信息的处理。
- **撤回同意权**：当我们的处理活动是基于您的同意时，您有权随时撤回该同意。撤回同意不影响此前基于同意所进行的处理活动的合法性。
- **数据可携权**：在技术可行且不侵犯他人权益的前提下，您可以请求将您的个人信息以结构化、通用的格式转移给您指定的其他数据控制者。

为保障安全，我们在响应您的上述请求前，可能会要求您提供身份证明文件以核实您的身份。您可通过本政策第十条所列联系方式提交您的请求。我们将在收到您有效请求后的十五个工作日内予以答复。在法律法规允许的特定情形下（如涉及国家安全、公共利益、司法程序或商业秘密），我们可能无法完全满足您的请求，届时我们将向您说明理由。

Article VII: Your Rights

In accordance with relevant laws and regulations, you are entitled to the following rights regarding your personal information:

- **Right to be Informed**: You have the right to be clearly, openly, and timely informed about how your personal information is collected, used, stored, shared, transferred, and protected, including the purposes of processing, categories of data involved, retention periods, and the identity and contact details of the data controller.
- **Right of Access**: You may request to review and obtain a copy of the personal information we hold about you.
- **Right to Rectification**: You may request that we correct or complete any inaccurate or incomplete personal information.
- **Right to Erasure**: Under statutory circumstances (e.g., when our processing purpose has been fulfilled or you withdraw your consent), you may request that we delete your personal information.
- **Right to Restriction of Processing**: In specific situations (e.g., while you are

contesting the accuracy of the information), you may request that we suspend or restrict the processing of your personal information.

- **Right to Withdraw Consent**: Where our processing activity is based on your consent, you have the right to withdraw that consent at any time. Withdrawal of consent does not affect the lawfulness of processing based on consent prior to its withdrawal.

- **Right to Data Portability**: Where technically feasible and without infringing on the rights of others, you may request that your personal information be transferred to another data controller you designate in a structured, commonly used, and machine-readable format.

For security purposes, we may require you to provide proof of identity to verify your request before responding. You may submit your request via the contact information provided in Article X of this Policy. We will respond within fifteen (15) business days of receiving your valid request. Under specific circumstances permitted by law (e.g., involving national security, public interest, judicial proceedings, or trade secrets), we may be unable to fully comply with your request, in which case we will provide you with our reasons.

第八条 对未成年人信息的保护

本政策所称“未成年人”系指依据适用法律被认定为不具备完全自主同意能力的自然人。根据《中华人民共和国个人信息保护法》，该年龄标准为**未满十四周岁**；而在其他司法管辖区（如欧盟成员国），相关法律（例如《通用数据保护条例》）可能将该年龄设定为**十三至十六周岁之间**，具体以当地法律规定为准。

我们不会在未事先获得其父母或法定监护人**可验证的明示同意**（如书面或其他符合监管要求的形式）的情况下，主动收集、使用、共享、转让或以其他方式处理上述年龄标准以下未成年人的个人信息。

如您发现我们在未取得有效监护人同意的情况下持有未成年人的个人信息，请立即通过本政策第十条所列联系方式与我们联系。我们将依法尽快核实并删除相关数据。

Article VIII: Protection of Minors' Information

For the purposes of this Policy, "minors" refer to natural persons who, under applicable law, are deemed incapable of providing valid consent independently. Under the *Personal Information Protection Law of the People's Republic of China*, this age threshold is set at **under fourteen years old**. In other jurisdictions (e.g., EU member states), relevant laws such as the General Data Protection Regulation (GDPR) may set this threshold between **thirteen and sixteen years old**, depending on the specific national implementation.

We will not knowingly collect, use, share, transfer, or otherwise process personal

information of individuals below the applicable age threshold without first obtaining **verifiable explicit consent** from their parent or legal guardian (e.g., in writing or through other means compliant with regulatory requirements).

If you become aware that we are processing personal information of a minor without valid parental or guardian consent, please contact us immediately via the channels specified in Article X. We will promptly verify and delete such information in accordance with applicable legal obligations.

第九条 政策的更新

我们保留不时更新本政策的权利。任何重大变更都将通过在公司官网显著位置发布公告等方式提前通知您。更新后的政策自公布之日起生效。若您继续使用我们的服务，即视为您接受修订后的政策。

Article IX: Policy Updates

We reserve the right to update this Policy from time to time. Any material changes will be notified to you in advance by posting a prominent announcement on our company's official website. The updated Policy will take effect from the date of publication. Your continued use of our services after the update constitutes your acceptance of the revised Policy.

第十条 联系方式

如您对本政策有任何疑问、意见，或希望行使您的个人信息权利，请通过以下方式联系我们：

- **电子邮箱**：privacy@asymchem.com.cn

我们承诺在收到您的有效请求后十五个工作日内予以回复。

Article X: Contact Information

If you have any questions, comments, or suggestions regarding this Policy, or if you wish to exercise your rights over your personal information, please contact us through the following channels:

- **Email**: privacy@asymchem.com.cn

We commit to replying to your valid request within fifteen (15) business days.

第十一条 决策与监督

本政策已经本公司董事会下属的战略委员会审议通过，自颁布之日起生效。战略委员会负责本政策的解释、修订与监督执行，并定期向董事会汇报政策履行情况。

本政策未尽事宜，按有关法律、法规、规范性文件执行。

本政策以中文编制。如两个版本有任何不相符之处，应以中文版本为准。

Article XI: Governance and Oversight

This Policy has been reviewed and approved by the Strategy Committee of the Company's Board of Directors and is effective from the date of issuance. The Strategy Committee is responsible for the interpretation, revision, and oversight of this Policy's implementation, and will regularly report on its performance to the Board of Directors.

Any matters not covered herein shall be governed by applicable laws, regulations, and normative documents.

This Policy is originally drafted in Chinese. In the case of any discrepancies, the Chinese version of the Policy shall prevail.