

东方日升隐私安全政策

Privacy Security Policy

■ 声明和承诺 Our Statement and Promise

本公司重视客户的个人信息与隐私保护, 承诺按照适用的法律法规及行业最佳实践, 透明地收集、使用、存储和处理客户数据, 并为客户提供充分的控制权。为此, 我们制定了以下隐私安全政策。

Risen Energy values the protection of customers' personal information and privacy. We are committed to collecting, using, storing, and processing customer data transparently in compliance with applicable laws, regulations, and industry best practices, while ensuring customers have full control over their data. Below, we outline our privacy and security policy:

■ 隐私安全政策 Privacy Security Policy

• 法令遵循 Compliance

我们遵循适用的法律法规和国际标准, 包括但不限于《网络安全法》、《个人信息保护法》等, 以确保个人信息的合法、合规处理。

We strictly comply with relevant laws and regulations, including the "Cybersecurity Law of the People's Republic of China" and the "Personal Information Protection Law of the People's Republic of China," to ensure the lawful and compliant handling of personal information.

• 制定隐私管理系统 Privacy management system

我们制定了专门的隐私管理系统约束公司及供应商的行为, 对个人信息的收集、保存、调阅和销毁作出明确的规定。如因特殊需求需要收集员工个人信息时, 公司需要明确向员工告知其个人信息的内容和用途, 必须在征得其同意的情况下才能使用。

We have established a privacy management system to standardize the behaviors of Risen Energy and our suppliers, clearly outlines the procedures for collecting, preserving, accessing, and destroying personal information. When collecting employee information, we inform employees of the specific contents and purposes of the collection, and obtain their consent prior to actual use.

• 专人负责 Data security management team

我们成立了一个由业务部门、流程与信息中心、风控中心等多个部门组成的数据安全管理工作组, 统筹协调数据安全管理的各项工作, 确保各环节的高效运作。

To ensure effective information security management, we have formed a data



security management team comprising representatives from the Information Center, Risk Control Center, and other relevant departments.

- **风险与合规管理 Risk and compliance management**

我们将隐私政策纳入集团范围的风险与合规管理体系中，进行全面的风险评估和管理，及时发现和应对潜在的隐私安全风险。

We integrate our privacy policy into our overall risk management system and conduct comprehensive risk assessments to identify potential privacy security risks promptly.

- **零容忍政策 Zero tolerance policy**

我们实行零容忍政策，对任何违反隐私政策的行为采取严厉的纪律处分，包括但不限于口头警告、书面警告、不良绩效评估、降级或解雇等。

We have a zero-tolerance policy and take disciplinary action for any violation of our privacy policy, including verbal warnings, written warnings, negative performance appraisals, demotion, dismissal, and other measures.

■ **信息收集及使用范围 Nature and Use of Information Collected**

- **信息用途 Use of the collected information:**

我们可能出于以下目的收集、处理和使用个人信息：业务需求、商业销售、安全管理、求职面试、法律需要、保护东方日升法律权利需要以及其它东方日升运营管理措施必要。

We may collect, process, and use personal information for various purposes, including business operations, commercial sales, security management, job interviews, legal requirements, protection of the company's legal rights, and other operational management needs.

- **信息类别 Nature of information captured:**

- 人员资料，包含姓名、性别、服务机构及职称、身份证

Basic information, including name, gender, service organization and title, ID card

- 人员联系方式，包含电话及邮件

Contact information, including mobile and e-mail

- 其他为保护安全所必要之资料

Other information necessary for the protection of security

- 求职者资料，包含姓名、性别、生日、身份证或其他证件号码及照片等

Job applicant information, including name, gender, date of birth, ID card or other ID number and photo, etc.

- 求职者专长及教育、工作经验，包含语言能力及其他专业技能证书

Job applicant's professional and education background, work experience, including language proficiency and other professional skills certificates



- 求职者联系方式，包含电话及邮件
Job applicant's contact information, including mobile and e-mail
- 其它公司认为有必要搜集的信息
Other information that we consider necessary

• 信息搜集的告知 Notice of Information Collection

我们将告知资料所有人以下信息：

We will inform data providers about the following details:

- 所获取信息的性质
The nature of the information obtained
- 信息的使用方式
How the information will be used
- 信息在公司档案的保存时间
Duration of Retention
- 信息保护方式
Protection Measures
- 我们将为资料所有人提供以下选项，使其可以决定如何收集、使用、保留和处理私人数据：
We offer data providers the following choices to determine how their private data will be collected, used, retained, and processed:
 - ✓ 请求查阅或复制
Request for access or copying
 - ✓ 收取信息需经过同意，并提供退出选项
Consent and opt-out
 - ✓ 请求更正不正确的信息
Request for correction
 - ✓ 请求删除储存于公司内部或网站的信息
Request for deletion stored by the company or on our website
 - ✓ 在必要且技术可行之条件下，请求以电子及机器易读取形式将资料转移给第三方
Request for data transfer to a third party in an electronic and machine-readable format, if necessary and technically feasible

■ 客户权利 Customer Rights

本公司确保客户在数据生命周期各阶段拥有以下权利：



Our company ensures that customers have the following rights throughout the data lifecycle:

- **选择权 Choice**
客户可自主决定其数据如何被收集、使用、保留和处理。
Customers can decide how their data is collected, used, retained, and processed.
- **同意机制 Consent**
数据收集前需客户明确的“选择加入 (Opt-in) ” 同意。
Explicit opt-in consent is required before data collection.
客户可随时选择退出 (Opt-out) 其数据的使用。
Customers can opt-out of the use of their data at any time.
- **访问与更正 Access and Correction**
客户有权请求访问公司持有的其数据。
Customers can request access to their data held by the company.
客户有权请求更正不准确的数据。
Customers can request correction of inaccurate data.
- **数据传输与删除 Data Portability and Deletion**
客户有权要求其数据被转移至其他服务提供商。
Customers can request their data to be transferred to other service providers.
客户有权请求删除其数据。
Customers can request deletion of their data.

■ 数据存储与保护 Data Retention and Protection

- **信息保存期限 Data Retention Period:**
我们会在客户账号保持活跃期间，持续保存客户信息，以确保服务的连续性并符合适用的法规要求。如果客户主动申请删除或注销其在我们系统中的账号，所有相关的个人信息将按照我们的数据删除流程从系统中永久移除。
We retain customer information for as long as the account remains active in our system to ensure service continuity and compliance with applicable regulations. If a customer actively requests to delete or deactivate their account, all associated personal information will be permanently removed from our system in accordance with our data deletion procedures.
- **数据保护措施 Data Protection Measures:**
技术保护：使用加密技术，例如传输层安全协议(TLS)，在传输过程中保护您的个人数据。当我们储存您的个人数据时，我们使用的是具有有限访问权限的计算机系统，并且这些系统是部署在受物理安保措施保护的设施内。
Technical Protection: We use encryption technologies, such as Transport Layer Security (TLS), to safeguard your personal data during transmission. When storing



your personal data, we utilize computer systems with restricted access, deployed in facilities protected by physical security measures.

- 安全事件处理：为防止信息安全事件的发生，我们制定了完善的预警机制和应急预案。若发生个人信息安全事件，我们将严格按照法律法规的规定，及时向客户告知。

Security Incident Handling: To prevent information security incidents, we have established comprehensive early warning mechanisms and contingency plans. In the event of a personal information security incident, we will notify customers promptly in strict accordance with applicable laws and regulations.

- 第三方审计：我们每年进行至少一次第三方审计和内部审计，评估隐私政策的合规情况，并及时进行必要的改进和调整，以确保个人信息的安全和合法使用。

Third-party audits: We conduct third-party audits and internal audits at least once a year to assess our compliance with the privacy policy. We make improvements and necessary adjustments to ensure the safe and lawful use of personal information.

- 安全意识培训：员工必须经过安全信息培训并签署保密协议。针对 IT 人员至少一年开展二次安全培训，内容涉及集团信息安全应急响应制度、信息安全框架解析、信息安全意识、钓鱼演练等。

Security awareness training: Employees are required to participate in security information training and sign confidentiality agreements. IT staff undergo security training sessions at least twice a year, covering topics such as information security emergency response policy training, information security framework analysis training, information security awareness, and phishing drills.

■ 数据二次用途监控 Monitoring of Secondary Data Use

我们公司严格限制客户数据仅用于其最初收集的目的，并通过内部数据治理体系持续监测客户数据是否被用于二次用途的比例。目前，在未获得客户明确同意的情况下，不会将客户数据用于任何二次用途。我们承诺保持透明，如果未来发生二次用途的情况，将公开披露相关比例，并确保完全符合适用的数据保护法规。

Our company strictly limits the use of customer data to the purposes for which it was originally collected. We currently monitor the proportion of customer data used for any secondary purposes through our internal data governance system. At present, no customer data is used for secondary purposes without explicit consent. We are committed to transparency and, should such data use occur in the future, we will publicly disclose the proportion and ensure it complies with applicable data protection regulations.

当前比例 / Current Percentage: [0%]



■ 第三方信息披露政策 Third-Party Disclosure Policy

公司承诺在与任何第三方（包括供应商、合作伙伴、公共机构等）交换客户信息时，严格遵守适用法律法规，仅在业务必要或符合法律要求的情况下披露，并采取最小化和安全性原则。所有接收方必须遵守同等的数据保护标准，未经客户同意，公司不会将其个人信息用于与原收集目的无关的用途。

We are committed to strictly complying with applicable laws and regulations when exchanging customer information with any third party (including suppliers, partners, and public authorities). Information will only be disclosed when legally required or strictly necessary for business purposes, following the principles of data minimization and security. All recipients must adhere to equivalent data protection standards, and the company will not use or share personal information for purposes beyond the original intent without customer consent.

我们坚信，通过以上管理方针的全面实施，我们能够有效保护客户的个人信息安全和隐私权益，为客户提供可信赖的服务和保障。

We firmly believe that by fully implementing the above management policy, we can effectively safeguard our clients' personal information security and privacy rights. This commitment enables us to provide our clients with trustworthy services and protection.

