高景太阳能
Gokin Solar

隐私保护政策

Privacy Protection Policy

目录 / Table of Contents

高景太阳能股份有限公司（以下简称“高景太阳能”或“公司”）尊重并保护员工、求职者、客户、供应商、承包商、合作伙伴及其他相关个人的隐私和个人信息权益。本政策旨在建立覆盖个人信息全生命周期的统一原则和管理要求，防止未经授权的访问、使用、披露、篡改、丢失或滥用，并支持公司业务的合规、稳健运行。

Gokin Solar Co., Ltd. (hereinafter referred to as “Gokin Solar” or “the Company”) respects and protects the privacy and personal information rights of employees, applicants, customers, suppliers, contractors, business partners, and other individuals. This Policy establishes consistent principles and requirements across the personal information lifecycle, prevents unauthorized access, use, disclosure, alteration, loss, or misuse, and supports compliant and resilient business operations.

本政策依据业务所在地适用的隐私、个人信息保护、网络安全和数据安全法律法规制定，并参考《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》、欧盟《通用数据保护条例》（GDPR）以及 ISO/IEC 27001、ISO/IEC 27701 等国际标准的相关原则。适用法律规定更严格要求的，从其规定。

This Policy is developed in accordance with applicable privacy, personal information protection, cybersecurity, and data security laws in the locations where the Company operates. It also refers to principles in the Personal Information Protection Law, Data Security Law, and Cybersecurity Law of the People’s Republic of China, the EU General Data Protection Regulation (GDPR), and international standards including ISO/IEC 27001 and ISO/IEC 27701. Where applicable law imposes stricter requirements, those requirements prevail.

本政策适用于高景太阳能股份有限公司及其控股子公司、各生产基地和经营单位，以及代表公司处理个人信息的董事、高级管理人员、员工、实习生、劳务用工人员和第三方。公司要求供应商、服务商、承包商及其他受托处理方遵守适用法律、合同约定和与本政策一致的隐私保护要求。

This Policy applies to Gokin Solar Co., Ltd., its controlled subsidiaries, production bases, and operating entities, as well as directors, senior management, employees, interns, contract workers, and third parties processing personal information on the Company's behalf. Suppliers, service providers, contractors, and other processors are required to comply with applicable law, contractual obligations, and privacy requirements consistent with this Policy.

3. 定义　Definitions

3.1 个人信息　Personal Information

以电子或其他方式记录的、与已识别或者可识别的自然人有关的各种信息，不包括依法匿名化处理后的信息。

Any information, recorded electronically or otherwise, relating to an identified or identifiable natural person, excluding information that has been lawfully anonymized.

3.2 敏感个人信息　Sensitive Personal Information

一旦泄露或被非法使用，容易导致自然人的人格尊严受到侵害或者人身、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、行踪轨迹以及未成年人信息等。

Personal information that, if leaked or unlawfully used, may readily harm personal dignity or endanger personal or property safety, including biometric data, religious beliefs, specific identity information, medical and health data, financial accounts, location tracking, and information concerning minors.

3.3 处理　Processing

对个人信息的收集、存储、使用、加工、传输、提供、公开、删除等活动。

Any operation performed on personal information, including collection, storage, use, alteration, transmission, provision, disclosure, and deletion.

4. 职责　Responsibilities

4.1 高级管理层　Senior Management

负责监督公司隐私保护治理，推动必要资源配置，并审议重大隐私风险和重大个人信息安全事件。

Oversee privacy governance, support the allocation of necessary resources, and review material privacy risks and significant personal information security incidents.

4.2 信息安全、法务合规及风险管理相关职能　Information Security, Legal, Compliance, and Risk Functions

按照职责分工统筹隐私合规与信息安全管理，组织制度建设、风险评估、合规审查、技术与管理控制、事件响应、培训和监督检查，并为业务部门提供专业支持。

Coordinate privacy compliance and information security according to assigned responsibilities; organize governance documents, risk assessments, compliance reviews, technical and organizational controls, incident response, training, and inspections; and provide professional support to business functions.

4.3 业务部门及各生产基地　Business Functions and Production Bases

落实“谁收集、谁负责，谁使用、谁负责”的管理原则，在开展处理活动前明确目的、范围、法律依据、保存期限和安全措施，维护数据清单并及时报告风险与事件。

Apply the principle that the function collecting or using information is accountable for that activity. Before processing begins, define the purpose, scope, legal basis, retention period, and safeguards; maintain relevant inventories; and promptly report risks and incidents.

4.4 全体工作人员　All Personnel

遵守本政策及相关制度，仅在授权和履职所必需的范围内处理个人信息，妥善保护账号、终端和文件，并及时报告可疑事件。

Comply with this Policy and related procedures, process personal information only within authorized and job-related limits, safeguard accounts, devices, and records, and promptly report suspected incidents.

5. 管理流程　Management Process

识别处理活动与法律依据→告知并在需要时取得同意→最小化收集→安全使用、存储与传输→管理第三方和跨境活动→响应个人权利请求→到期删除或匿名化→监测、审计与改进。

Identify processing and legal basis → provide notice and obtain consent where required → minimize collection → securely use, store, and transmit → manage third parties and cross-border

activities → respond to data subject requests → delete or anonymize at expiry → monitor, audit, and improve.

6. 隐私保护要求　Privacy Protection Requirements

6.1 合法、正当、透明与目的限制　Lawfulness, Fairness, Transparency, and Purpose Limitation

公司仅基于明确、合理且与业务直接相关的目的处理个人信息，并依据适用法律确定处理依据。收集前以清晰、易懂的方式告知个人处理者身份、目的、方式、种类、保存期限、共享对象、权利行使方式及其他法定事项；目的、方式或种类发生实质变化时，依法重新告知并取得必要授权。

The Company processes personal information only for specific, reasonable purposes directly related to business needs and establishes a lawful basis under applicable law. Before collection, individuals are clearly informed of the controller's identity, purposes and means of processing, data categories, retention period, recipients, methods for exercising rights, and other legally required matters. Material changes to purposes, means, or categories require renewed notice and authorization where legally required.

6.2 最小必要与准确性　Data Minimization and Accuracy

公司将个人信息的种类、数量、访问范围和保存期限限制在实现处理目的所必需的范围内，不进行过度收集。业务部门采取合理措施保持信息准确、完整并及时更新；不准确的信息应根据处理目的予以更正或删除。

The Company limits the categories, volume, access scope, and retention of personal information to what is necessary for the stated purpose and avoids excessive collection. Business functions take reasonable steps to keep information accurate, complete, and current; inaccurate information is corrected or deleted as appropriate to the processing purpose.

6.3 敏感个人信息与未成年人信息　Sensitive Information and Minors

处理敏感个人信息应具有特定目的和充分必要性，开展影响评估，采取更严格保护措施，并依法取得单独同意或满足其他法定条件。处理未成年人信息时，依法取得监护人同意并采取与其年龄、风险相适应的保护措施。

Sensitive personal information is processed only for a specific purpose and where strictly necessary, subject to an impact assessment, enhanced safeguards, and separate consent or another lawful condition where required. Information concerning minors is processed with legally required guardian consent and safeguards appropriate to age and risk.

6.4 访问控制与安全保障　Access Control and Security

公司按照数据分类分级和最小权限原则实施身份认证、权限审批、日志记录、加密或脱敏、备份恢复、终端与网络防护、物理安全等控制。权限定期复核，并在岗位变动或离职时及时调整或撤销。公司定期开展风险评估、漏洞管理、应急演练及必要的合规审计。

The Company applies data classification, least privilege, authentication, access approval, logging, encryption or masking, backup and recovery, endpoint and network protection, and physical safeguards. Access is reviewed periodically and promptly modified or revoked following role changes or termination. Risk assessments, vulnerability management, emergency exercises, and appropriate compliance audits are conducted regularly.

6.5 保存、删除与匿名化　Retention, Deletion, and Anonymization

公司根据处理目的、合同要求和法定期限确定保存期限。目的已实现、保存期限届满、授权被撤回且无其他处理依据，或法律要求删除时，公司依法删除或匿名化；技术上暂时难以删除的，除存储和采取必要安全保护措施外停止其他处理。

Retention periods are defined according to processing purposes, contractual needs, and legal requirements. Information is deleted or anonymized when the purpose has been achieved, retention expires, authorization is withdrawn and no other lawful basis exists, or deletion is legally required. Where immediate deletion is technically impracticable, processing is restricted to storage and necessary security safeguards.

6.6 共享、委托处理与第三方管理　Sharing, Processing by Vendors, and Third-Party Management

向第三方提供个人信息或委托处理前，公司开展必要性和风险评估，履行告知、同意或其他法定义务，并通过合同明确处理目的、期限、方式、信息种类、安全措施、事件报告、审计和返还/删除要求。未经批准，受托方不得转委托、改变目的或超范围处理。

Before sharing personal information or engaging a processor, the Company assesses necessity and risk, meets notice, consent, or other legal obligations, and contractually defines purposes, duration,

methods, data categories, safeguards, incident reporting, audit rights, and return or deletion requirements. A processor may not sub-process, change purposes, or exceed the agreed scope without approval.

6.7 跨境提供　Cross-Border Transfers

个人信息跨境提供应基于真实、明确且必要的业务目的，履行适用的安全评估、认证、标准合同、告知和单独同意等要求，并采取措施确保境外接收方达到适用法律规定的保护水平。

Cross-border transfers must serve a genuine, specific, and necessary business purpose and comply with applicable security assessment, certification, standard contract, notice, and separate consent requirements. Measures are taken to ensure that overseas recipients provide the level of protection required by applicable law.

6.8 个人信息安全事件　Personal Information Security Incidents

发现或怀疑发生泄露、篡改、丢失、未经授权访问或其他安全事件时，相关人员应立即报告并采取控制措施。公司按照应急机制开展分级响应、调查、影响评估、证据保存、补救和复盘，并依法向监管机构和受影响个人通知；法律允许不通知的，应记录判断依据。

Any actual or suspected leak, alteration, loss, unauthorized access, or other security incident must be reported immediately and contained. The Company activates a risk-based response covering investigation, impact assessment, evidence preservation, remediation, and lessons learned, and notifies regulators and affected individuals where legally required. Where notification is lawfully omitted, the basis for that decision is documented.

6.9 培训与隐私设计　Training and Privacy by Design

公司定期开展隐私与信息安全培训，对处理大量、敏感或高风险个人信息的岗位实施针对性培训。新系统、新产品、新场景或重大变更在设计和上线前应评估隐私影响，将最小化、默认保护和安全控制嵌入业务流程。

The Company provides periodic privacy and information security training, with role-specific training for personnel handling large volumes of sensitive or high-risk information. New systems, products, processing scenarios, and material changes are assessed before design approval and launch so that minimization, privacy-protective defaults, and security controls are embedded in business processes.

7. 申诉与个人权利请求　Grievances and Data Subject Requests

在适用法律规定的范围内，个人有权查询、复制、更正、补充或删除其个人信息，撤回同意，限制或反对处理，要求解释处理规则，注销账户，或依法行使可携带等其他权利。公司建立身份核验、登记、评估、处理和反馈机制，并在法定期限内回应；拒绝请求时说明理由及救济途径。

Subject to applicable law, individuals may access, copy, correct, supplement, or delete their personal information; withdraw consent; restrict or object to processing; request an explanation of processing rules; close an account; or exercise portability and other legal rights. The Company verifies identity, registers, assesses, handles, and responds to requests within applicable time limits. Where a request is denied, the reason and available remedy are explained.

利益相关方可实名或匿名通过以下渠道提出申诉、投诉或举报：

电子邮箱 shenjibu@gokin.com；

举报电话/短信 15692038078；

公司及各基地官方微信公众号“联系我们—举报渠道”；

各基地举报信箱或邮寄至广东省珠海市金湾区三灶镇湖滨路 1566 号高景太阳能股份有限公司审计委员会（收）。

Stakeholders may raise grievances, complaints, or reports openly or anonymously through the following channels: email at shenjibu@gokin.com; hotline/SMS at +86 15692038078; WeChat QR Code; the “Contact Us - Reporting Channel” on the official WeChat accounts of the Company and its production bases; reporting mailboxes at each production base; or correspondence to the Audit Committee of Gokin Solar Co., Ltd., No. 1566 Hubin Road, Sanzao Town, Jinwan District, Zhuhai, Guangdong, China.

公司对举报人、申诉人、证人及协助调查人员的信息严格保密，禁止任何形式的打击报复。善意提出关切或行使个人信息权利不会影响其雇佣、采购、商业合作或其他合法权益。具体受理和保护要求按照《高景太阳能申诉、投诉与举报管理政策》执行。

The Company keeps information concerning reporters, complainants, witnesses, and persons assisting an investigation confidential and prohibits retaliation in any form. Raising a concern in good faith or exercising privacy rights will not adversely affect employment, procurement, business

relationships, or other lawful interests. Detailed handling and protection requirements follow the Gokin Solar Grievance, Complaint and Reporting Management Policy.

8. 监督、审查与持续改进　Oversight, Review and Continual Improvement

公司通过风险评估、内部检查、审计、事件分析和整改跟踪监督本政策落实，并根据法律法规、监管要求、业务变化、技术发展和行业实践适时更新。本政策原则上每年至少审查一次，重大变化或重大事件发生后及时开展专项审查。本政策由高级管理层、董事长签批。

The Company monitors implementation through risk assessments, internal inspections, audits, incident analysis, and corrective-action tracking and updates this Policy in response to legal, regulatory, business, technological, and industry developments. The Policy is reviewed at least annually in principle and promptly following material changes or significant incidents. This policy was approved by the senior management and the chairman.