天合光能股份有限公司

个人信息保护管理制度

主导部门	**风险控制管理部**		
支持部门	**流程数字化部、全球法务部**		
制度审批	**GRC**		
制度分级	**二级**	**制度版本**	**V02**
文档编号	**TSL-CM-008**	**生效日期**	**2026-08-13**

1. 目的

为尊重、保护个人隐私权，保证个人信息收集、存储、使用、加工、传输、提供、公开、删除等活动的目的与个人信息主体的意愿一致并符合法律法规的要求，不超目的、超范围处理个人信息，特制定本制度。

2. 范围

本制度适用于天合光能股份有限公司（以下简称公司）及其下属各分子公司的个人信息保护合规管理相关内容。对于非中国大陆主体，可以在本制度制定的原则基础上，结合所适用法律法规的具体规定，对应执行。

本制度依据公司运营所在地所适用的个人信息保护要求（包括但不限于《中国个人信息保护法》《欧洲通用数据保护条例》《美国加州消费者保护法案》等法律和规范要求）制定。

公司应通过协议等方式，要求所有接触、处理、使用、运营和保管天合光能个人信息的供应商、承包商、顾问或销售商等第三方按照本制度所述的要求执行。

3. 定义

名称	定义
个人信息	*以电子或者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，不包括匿名化处理后的信息。*
敏感个人信息	*一旦泄露或者非法使用，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、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。*
个人信息主体	*可通过个人信息识别的特定的自然人，包括客户、供应商、员工等。*
个人信息处理者	*收集、存储、使用、加工、传输、提供、公开、删除个人信息的机关、企业、事业单位、社会团体等组织。*
处理	*处置个人信息的过程，如包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除及其它处置行为。*
收集	*获取个人信息的行为。*
使用	*运用个人信息的行为。*
加工	*对个人信息进行一系列的处理活动，包括收集、判别、筛选、分类、排序、分析、再造、存储、传递、检索和显示等。*
提供	*个人信息处理者委托第三方处理个人信息及其它因某种利益处理个人信息的行为。*
个人信息处理活动记录（RoPA）	*是“Records of Processing Activities”的缩写，即处理活动记录。*

4. 管理内容

4.1 个人信息保护基本方针、目标及原则

4.1.1 个人信息保护基本方针

(1) 治理完善，筑牢保护防线

公司坚持建立健全个人信息保护治理体系，将个人信息保护要求纳入公司整体管理体系和业务运营流程，明确个人信息保护相关组织架构、职责分工和管理机制，确保个人信息保护责任有效落实。公司通过持续完善制度体系、管理流程和监督机制，推动个人信息保护工作规范化、体系化运行。

(2) 经营合规，规范处理活动

公司遵循合法、正当、必要和诚信原则开展个人信息处理活动，严格依据适用法律法规及内部管理要求，对个人信息的收集、存储、使用、共享、删除及跨境传输等全过程进行管理。公司坚持向个人信息主体充分履行告知义务，保障个人信息处理活动透明、可控。

(3) 稳健发展，防控合规风险

公司坚持以风险管理为导向，持续识别、评估和降低个人信息处理过程中的合规风险和安全风险。公司通过开展个人信息保护影响评估、风险评估、安全控制措施建设以及第三方管理等方式，提升个人信息保护能力，防范个人信息泄露、滥用及其他安全事件。

(4) 创造价值，共建合规信任

公司将个人信息保护作为企业可持续发展的重要组成部分，通过持续开展监督检查、内部审核、管理评审和员工培训，不断提升个人信息保护管理水平。同时，公司积极回应个人信息主体、客户及合作伙伴对隐私保护的期待，通过透明、负责的个人信息处理实践，建立长期信任关系。

4.1.2 个人信息保护目标

(1) 提升个人信息保护合规管理水平

建立完善个人信息保护制度体系与运行监督体系，有效开展个人信息处理活动风险控制，适时更新个人信息保护目标。

(2) 遵守个人信息保护法律法规与公司规章

严格遵守个人信息保护相关法律法规、行业准则与公司内部规章制度，年度实现重大个人信息合规事故为 0，不得因违规处理个人信息致使公司产生较大损失（包括行政处罚、赔偿金、滞纳金等）。

(3) 保障数据主体合法权益

规范个人信息收集、存储、使用、传输、共享、删除等全生命周期处理活动，建立标准化数据主体权利响应流程，实现数据主体权利请求妥善处置办结率 100%，充分保障数据主体知情权、访问权、更正权、删除权、撤回同意等各项法定权利有效落地。

(4) 保护企业声誉和品牌价值

培育形成个人信息保护合规文化，不得因个人信息违规处理行为，违背诚信经营原则并引发重大负面舆情。

4.1.3 个人信息保护基本原则

(1) **权责一致原则**：对其个人信息处理活动及对个人信息主体合法权益造成的损害承担责任。

(2) **目的明确原则**：具有合法、正当、必要、明确的个人信息处理目的。

(3) **选择同意原则**：向个人信息主体明示个人信息处理目的、方式、范围、规则等，征求其授权同意或具备其他合法性依据。

(4) **最少够用原则**：除与个人信息主体另有约定或具备其他合法性依据外，只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时根据约定删除或匿名化处置个人信息。

(5) **公开透明原则**：以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督。

(6) **确保安全原则**：具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性。

(7) **主体参与原则**：向个人信息主体提供能够访问、更正其个人信息，以及撤回同意、注销账户等方法。

4.2 个人信息全生命周期管理

4.2.1 个人信息的收集、使用

(1) 公司收集的个人信息类型通常包括人员姓名、照片、身份证号、联系电话、电子邮件、通讯地址等信息，具体取决于特定的应用场景及处理目的。公司在收集个人信息前，应当向个人信息主体明确告知所获取信息的性质及收集个人信息的目的、方式、范围和可能涉及的第三方。

(2) 所有个人信息收集行为必须具有合法、正当、明确、合理的目的，并通过合法途径进行收集。

(3) 所有个人信息收集行为，应具备合法性依据，并告知信息处理目的、处理方式、处理的个人信息种类、保存期限等信息，信息收集范围应限定在实现处理目的的最小范围内。具体合法性依据不尽相同，取决于个人信息的处理主体、处理目的、处理方式及适用法律的规定。符合下列情形之一的，公司方可处理个人信息：

(a) 取得个人的同意；

(b) 为订立、履行与客户/供应商的合同所必需，处理个人信息；

(c) 为订立、履行与个人签署的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需，处理个人信息；

(d) 为履行法定职责或者法定义务所必需；

(e) 为应对突发公共卫生事件，或者紧急情况下为保护个人的生命健康和财产安全所必需；

(f) 其他相关法律规定的合法性依据。

(4) 敏感个人信息的收集与处理

(a) 只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，方可收集、处理敏感个人信息；

(b) 收集、处理敏感个人信息应当取得个人的单独同意或具备其他合法性依据；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定；

(c) 应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响；依照法律规定可以不向个人告知的除外。

(5) 不得将个人信息用于违法犯罪活动、个人信息交易等不符合法律法规规定的用途。

(6) 收集、处理个人信息相关情形发生变更的，应当重新取得个人同意或具备其他合法性依据。

4.2.2 个人信息的提供

(1) **委托处理个人信息**。公司委托第三方处理个人信息的，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。未经公司同意，个人信息处理的受托人不得转委托他人处理个人信息。受托人应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息。

(2) **个人信息的转移**。公司因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应当向个人告知接收方的名称或者姓名和联系方式，并取得个人的单独同意。接收方应当继续履行个人信息处理者的义务。

(3) **向第三方披露、共享个人信息**。

(a) 公司向其他第三方披露、共享其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意或具备其他合法性依据。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。变更原先的处理目的、处理方式的，应当依法重新取得个人同意或具备其他合法性依据。

(b) 当已向第三方披露、共享的个人信息发生信息修改、授权撤回，或收到个人信息主体提出的异议时，公司应当及时将该等变更情况通知接收该个人信息的相关第三方。

(4) **个人信息的公开**。公司除取得个人信息主体的单独同意，或具备法律法规明确规定的其他合法性依据外，不得公开其处理的个人信息。

4.2.3 个人信息的跨境传输

在不违反原收集、处理及使用个人信息目的的必要范围内，公司对外跨境传输个人信息的，应取得个

人的单独同意或具备其他合法性依据，并遵循本制度、公司《数据跨境合规管理制度》及对应运营、交易所在地适用的个人信息跨境传输相关法律及政策要求，采取适当的保障措施。

4.2.4 个人信息的存储及删除

(1) 个人信息的存储时限应满足国家法律法规与行业主管部门有关规定要求，并符合个人信息处理目的所需的最短时间要求。

(2) 当发生以下情形之一的，公司应当采取合理的方式确保个人信息无法恢复和再利用：

(a) 处理目的已实现、无法实现或者为实现处理目的不再必要；

(b) 个人信息存储期限已届满；

(c) 公司违反适用法律规定或违反合同约定处理个人信息；

(d) 适用法律规定的其他情形。

(3) 适用法律规定的存储期限未届满，或者删除个人信息从技术上难以实现的，公司应当停止除存储和采取必要的安全保护措施之外的处理。

(4) 处理个人信息过程中生成的各类临时文件，应按照本制度第 4.2.4 条的规定进行存储和管理；临时文件到期后，应及时完成删除或销毁操作。

4.3 个人信息处理活动记录（RoPA）

4.3.1 个人信息处理活动记录（RoPA）涉及个人信息的类型、来源等信息的调研与记录，并根据业务功能和授权情况区分个人信息的处理目的、使用场景，以及共享、是否涉及出境等情况，包含个人信息处理活动各环节相关的信息系统。

4.3.2 当发生下述情形时，个人信息处理部门应新建、更新个人信息处理活动记录：

(1) 在特定业务场景下，将组织所在地境内收集和产生的个人信息提供给境外机构、组织或个人等情况前；

(2) 个人信息的收集、处理、转让、共享或披露的业务目的、范围、模式及委托的第三方及第三方的数据处理目的或其发生重大变更时；

(3) 涉及个人信息收集或处理的新产品、新服务、新功能上线时；

(4) 发生重大个人信息安全事件后；

(5) 法律、法规、政策及外部环境等出现重大变化时；

(6) 数据库层面已经脱敏的个人信息需重新识别和使用时；

(7) 对政府、监管部门、司法部门提供或披露个人信息前，对个人信息进行审阅。

4.4 个人信息主体权利响应

4.4.1 公司应当依法保障客户、供应商、员工等个人信息主体的合法权益，包括：

(1) 请求获取如何处理其个人信息的权利；

(2) 请求查阅、复制个人信息；

(3) 请求更正、补充个人信息；

(4) 请求删除个人信息；

(5) 请求撤回同意（Opt-out）；

(6) 请求获取个人信息副本；

(7) 在符合相关法律法规及国家网信部门规定条件的前提下，将个人信息转移至个人指定的其他个人信息处理者。

(8) 个人信息主体可发送邮箱至 datacompliance@trinasolar.com 提交请求。

4.4.2 个人信息安全事件的发现和报告：员工、供应商和外部第三方发现或怀疑已经发生或可能发生个人信息泄露、丢失、越权访问、恶意使用、系统攻击等安全事件（合称“个人信息安全事件”）时，应立即通知合规管理部、信息安全部，也可以通过公共邮箱 datacompliance@trinasolar.com 进行上报。

4.5 管理监督

4.5.1 公司对违反个人信息保护的行为“零容忍”。任何违反适用法律、本制度及公司其他个人信息保护相关的制度与流程，造成公司受到任何行政处罚、争议、经济损失、品牌声誉影响或其他负面影响的，应根据《天合光能员工手册》《业务违规及问责管理制度》规定，视违规行为等级及情节轻重处以口头或书面警告、解除劳动合同、追回违规所得、要求赔偿损失等处罚；构成犯罪的，公司将依法移交主管部门追究其法律责任。

4.5.2 公司应根据相关适用法律法规、政策等要求及公司业务运营情况，定期对本制度合规性进行内部和第三方审计，并及时进行调整及更新。

5. 附则

5.1 修订记录

编码	版本	拟制/修订责任人	生效日期	修订内容及理由
TSL-CM-008	V01	信息安全部、合规管理部	2024-08-12	新版本发布
TSL-CM-008	V02	风险控制管理部	2026-08-13	新增个人信息保护基本方针及目标、个人信息处理活动记录等要求

5.2 特别说明

本制度由风险控制管理部负责解释与更新。本制度有效期两年。新制度发布后，旧制度自动废止。