OSS数据安全和个人信息保护协议

深圳古瑞瓦特新能源有限公司（“**古瑞瓦特**”）作为光伏设备研发制造商，向注册OSS平台的古瑞瓦特经销商、分包商等合作伙伴提供与其设备有关的数据在线查看服务。特别是，在获得用户同意后，古瑞瓦特允许OSS平台用户（“**数据接收方**”或“**接收方**”）查看其终端客户通过Shine Phone App、瑞光宝盒App等收集的注册信息、设备基础信息、设备工作信息等数据及个人信息，以协助其提供后续设备运维服务。通过使用OSS平台服务，数据接收方同意遵守如下数据安全和个人信息保护协议。

对于古瑞瓦特向数据接收方分享的终端客户数据及个人信息，数据接收方与古瑞瓦特分别构成独立的个人信息处理者。数据接收方陈述并保证，在根据主协议处理个人信息时，应自行负责遵守任何和所有适用隐私法律和有关数据保护主管部门或其他主管部门的相应意见。

1. 个人信息处理

1.1. 在不限制本协议及协议其他条款关于接收方义务约定的情况下（包括但不限于保密义务），接收方应：（i）遵守所有适用的个人信息保护法律法规的要求; （ii）仅为向终端客户提供运维服务目的的处理个人信息。

1.2. 接收方保证仅许可获得适当授权的员工获取并读取个人信息及其他数据，该等授权应仅限于履行服务之必要的范围。对此，接收方应当采取一切必要措施保证被授权获取个人信息的员工的适当性和可靠性，包括保证任何人员（由接收方所雇佣或委派的人员）已经接受相关培训以了解在适用的个人信息保护法律法规和本附件下的个体责任和义务，并签署保密函等文件。接收方应禁止并阻止第三方未经本附件授权进行任何披露、访问或任何其他类型的个人信息处理行为。

1.3. 接收方应当确保持续实施并不断发展与潜在风险成比例的技术性和组织性措施，以便适当保护个人信息，特别是考虑到技术发展水平的变革以及通过定期测试和控制措施的实施。接收方采用的安全措施包括但不限于以下内容：（i）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；（ii）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；（iii）采取监测、记录网络运行状态、网络安全事件的技术措施,并按照相关规定留存相关的网络日志不少于六个月；（iv）采用数据分类、重要数据备份、加密和去标识化等安全技术措施；（v）合理确定个人信息处理的操作权限，并定期对接收方的员工进行安全教育和培训；（vi）制定并组织实施个人信息安全事件应急预案；（vii）根据适用法律的要求，实施网络安全等级保护制度，并按照法律法规和国家标准开展等级测评或向公安机关备案。

1.4. 如果数据接收方直接向个人收集个人信息，数据接收方保证：如果个人信息的处理在法律上需要数据主体的同意，则接收方应详细说明、获取并保存此等同意。接收方应确保此等同意是适当的，并且从数据主体处获得充分的同意，该等同意应包含适用的个人信息保护法律法规所要求的所有信息，并由接收方根据适用的个人信息保护法律法规保存。一经公司要求，接收方应向公司提供此等同意的证据，且不得无故拖延。如果接收方基于除数据主体的同意之外的合法性基础（如为订立、履行合同所必需；为履行法定职责或法定义务所必需；为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；为公共利益实施新闻报道、舆论监督等）收集、使用个人信息，并且接收方代表公司收集使用此类个人信息，则接收方应详细说明且记录无需取得数据主体同意的法律依据及个人信息收集的合法性证明，并履行其他相关法律义务（包括但不限于告知数据主体），且应确保此等依据是适当的。一经公司要求，接收方应向公司提供此等个人信息处理的合法性证明，且不得无故拖延。

1.5. 数据接收方保证其将仅遵守最小必要原则，仅将个人信息用于服务所需的必要目的。

2. 保障与控制

2.1. 接收方应保证执行、维持和落实安全措施，防止接收方及/或其代表处理个人信息过程中发生个人信息安全事件或网络安全事件。安全措施应当实时符合所有适用的个人信息保护法律法规以及相关行业标准。

2.2. 一旦发生以下情况，古瑞瓦特有权在合理通知之后对接收方的安全措施进行审计：（i）任何个人信息安全事件或网络安全事件；或（ii）古瑞瓦特发现或怀疑接收方或任何接收方代表可能存在不符合本协议的情况，包括但不限于任何实际或疑似未能实施符合适用的个人信息保护法律法规或者相关行业标准的安全措施。接收方应当以最佳方式协助和配合古瑞瓦特开展审计，包括但不限于组织人员召开会议、提交相关材料或记录等。

3. 个人信息安全事件和网络安全事件

3.1. 一旦出现个人信息安全事件或网络安全事件，接收方在发现或意识到个人信息安全事件或网络安全事件后二十四（24）小时内通知古瑞瓦特（“**事件通知**”）。该事件通知应至少包含个人信息安全事件或网络安全事件的描述、接收方采取补救该个人信息安全事件或网络安全事件的措施、联络人联系方式。

3.2. 数据接收方应合理配合和协助古瑞瓦特的调查、执行、监控、文件准备、通知和关于个人信息安全事件或网络安全事件的报告。

4. 个人信息的保存，销毁以及返还

4.1. 数据接收方保证在与数据处理有关的服务履行完毕后，根据法律法规要求及最小必要原则将所有个人信息安全删除。若古瑞瓦特要求，数据接收方还应提供其满足删除义务的证明。

4.2. 接收方保证个人信息只在中国境内处理和使用。任何个人信息及其他数据的转移均应遵守适用的个人信息保护法律法规，并且遵守适用法律中规定的特殊要求，例如数据主体的单独同意、按照国家网信部门制定的标准合同与境外接收方订立合同、按照国家网信部门的规定经专业机构进行个人信息保护认证、向个人告知境外接收方的相关信息（境外接收方的名称或者姓名、联系方式）及个人信息的处理目的、方式及种类、数据出境安全评估（如适用）和个人信息保护影响评估等。

5. 数据保护赔偿

数据接收方应作为独立的个人信息处理者对其开展的个人信息处理活动承担全部责任，古瑞瓦特对数据接收方的个人信息处理活动不承担任何责任。

如数据接收方违反本协议，古瑞瓦特有权采取终止服务等措施。接收方应对古瑞瓦特及其高管、董事和员工进行赔偿，使其免受因：（i）接收方在履行本附件过程中非法获不当地处理或使用数据，导致违反适用的个人信息保护法律法规或（ii）古瑞瓦特或其关联古瑞瓦特根据本附件规定的条件使用该等服务而引起的任何和所有索赔、花费、损害、罚款、损失、责任、成本、开销和律师费（包括来自于数据主体、数据保护机关或其他监管机关）。该赔偿义务在本附件因任何原因解除或期限届满后仍然有效。该责任的承担不影响古瑞瓦特进一步主张其他合法权利。

6. 定义

“**个人信息**”指的是任何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。

“**个人信息安全事件**”指的是实际发生或合理推断可能发生的以下情况：(1) 对个人信息未经授权的访问、使用、处理或盗窃；(2) 获准使用此类个人信息的人员，出于实际的或出于合理怀疑的盗窃或欺骗或者被证实的盗窃之原因，在授权范围外使用个人信息的；(3) 对个人信息未经授权的披露或修改；(4) 意外或非法破坏个人信息；或(5)个人信息丢失，包括但不限于因前述第(1)-(4)款中提及的事项或由于缺乏足够的安全措施，或接收方或其代表的渎职而导致。

“**网络安全事件**”是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件，包括有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件。

“**适用的个人信息保护法律法规**”指的是关于处理个人信息的不时生效的中国法律、法规、规范性文件等，包括但不限于《中华人民共和国民法典》、《中华人民共和国网络安全法》、《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》、《儿童个人信息网络保护规定》和任何适用的中国法，以及对前述法律法规进行不时修订的法律法规以及所有与个人信息安全相关的法律法规。

“**处理**”指的是任何对个人信息进行的收集、存储、使用、加工、传输、提供、公开、删除等，无论是否通过自动化处理的方式。

“**安全措施**”指的是目的是为了确保个人信息的机密性、完整性和可用性的技术、物理及行政管理措施，包括但不限于政策、程序、组织架构、硬件和软件功能和物理安全措施。