Sunny Optical Technology (Group) Co., Ltd.

Data Privacy and Security Policy

I. Vision and Guidelines

Sunny Optical Technology (Group) Co., Ltd. (hereinafter referred to as "the Group") is a globally leading comprehensive optical components and products manufacturer. In the course of production and operations, the Group handles business data, management data, and personal privacy information, and strictly complies with domestic and international laws, regulations, standards, and relevant policy requirements governing the full-lifecycle security management of data privacy, to realize the Group's vision of becoming a global exemplar of data privacy and security compliance.

The Group upholds the principle of establishing and implementing data privacy full-lifecycle security management that exceeds the requirements of laws, regulations, and standards, respects the rights of individuals to access, rectify, and delete their personal data privacy, progressively achieves standardized data privacy management, reduces the adverse impacts of data breaches or personal privacy compromises and the harm caused to employees, customers, and relevant stakeholders, and continuously strives to fully achieve data privacy and security compliance.

II. Management Objectives

To protect the data and personal privacy rights and interests of the Group, employees, customers, and relevant stakeholders, standardize data and personal privacy processing activities, promote the rational use of data and personal privacy, and promptly identify and address security risks in data and privacy processing, so as to achieve data privacy and security compliance.

III. Scope of Application

This Data Privacy and Security Policy applies to:

1. All operating premises and business activities of the Group worldwide;

2. All departments and employees of the Group, and all third-party personnel who may access the Group's data and personal information (including but not limited to suppliers, partners, service providers, contractors, and temporary staff);

3. All data and personal information involved in the Group's daily operations and management;

4. All stages of the full lifecycle of data and personal information, from collection, storage, use, transmission, sharing, disclosure, to destruction.

IV. Management Requirements

(1) Laws, Regulations, Standards, and Policy Requirements

The Group organizes professionals to collect and analyze data privacy and security-related laws, regulations, standards, and policy requirements from major countries worldwide, as the fundamental basis for formulating regulatory management systems and internal control standards. The Group regularly conducts data privacy compliance assessments, and responsible units shall effectively rectify any non-compliance with laws, regulations, or standards, to continuously meet the requirements of laws, regulations, standards, and relevant policies.

(2) Data Privacy Security Management Organization

The Group establishes the Information Security Working Group, responsible for data privacy security management and protection. It holds regular meetings annually, reporting to the Group's management on security governance, cybersecurity, data security, personal privacy protection, and security operations. The Information Security Working Group is designated to coordinate data privacy protection, and proactively responds to data privacy regulatory requirements from external government agencies.

The Group designates the Information Security Management Representative as the Data Protection Officer (DPO), serving as the designated person responsible for privacy matters. The Group's Information Security Working Group is responsible for comprehensively coordinating the planning, implementation, oversight, and continuous improvement of data privacy protection. The DPO reports directly to the Group's management, ensuring that data privacy protection work has sufficient independence and authority.

The Group embeds the data privacy policy framework into the Group's risk management and compliance management system, incorporating data privacy risk management into the Enterprise Risk Management (ERM) framework as an important component of the Group's overall risk identification, assessment, monitoring, and reporting, ensuring that

data privacy risks are aligned with the Group's overall risk management strategy, and achieving deep integration of data privacy compliance and Group compliance management.

The Group regularly conducts internal audits of privacy policy compliance, organized by the Group's Information Security Working Group through dedicated audits. These audits comprehensively examine the implementation and effectiveness of privacy policies against applicable laws, regulations, and the Group's privacy policy requirements, forming internal audit reports submitted to management for review. Corrective measures are developed and verified for any identified non-conformities.

The Group conducts third-party privacy policy compliance audits at least once every two years, engaging independent external third-party agencies to assess the applicability, adequacy, and implementation effectiveness of privacy policies, and issuing third-party audit reports to ensure that privacy policy compliance is independently verified. Third-party audit results serve as an important basis for policy revision and continuous improvement.

(3) Data Privacy Full-Lifecycle Security Management

The Group formulates security management systems such as *the Data Security Management Procedures* to implement security management across the full lifecycle of data privacy, including collection, storage, use, processing, transmission, provision, disclosure, and deletion. The Group implements classified and tiered management of data privacy, adopting corresponding security management and technical protection measures based on different categories and levels, including role-based access control, de-identification/anonymization/encryption, to ensure the confidentiality, integrity, availability, and non-tamperability of data privacy.

(4) Data Privacy Protection for Employees, Customers, and Relevant Stakeholders

The Group commits to minimizing the collection of employee, customer, and relevant stakeholder information (including sensitive personal information) necessary for the Group's daily operations and management. The Group clearly lists the types of personal information collected in an easily understandable manner (e.g., using tables), specifying the source, collection purpose, collection method, and usage of each item. Through pop-

ups or links, the Group ensures that operations are completed with the data subject's informed and explicit consent.

Before collecting and processing personal data, the Group must obtain the data subject's opt-in consent, meaning the data subject must actively and explicitly express consent before personal data can be collected and processed. The Group shall not obtain consent through pre-selected boxes, default opt-ins, or silence. For sensitive personal information (such as biometric data, health information, etc.), the Group must obtain the data subject's separate explicit consent.

When sharing data with third parties (such as partners, service providers, etc.), in addition to obtaining the data subject's explicit consent, the Group will inform the data subject of the type of recipient and the purpose of sharing, sign confidentiality agreements, and conduct regular security reviews, to maximize the protection of employee, customer, and relevant stakeholder data privacy and security.

The Group affirms that data subjects have the rights to access, rectify, delete, and data portability. Data subjects may obtain their personal data at any time, have the right to transmit such data to other data controllers, and may initiate data portability requests by directly contacting the Information Security Working Group or sending emails to designated mailboxes. The Group commits to responding in a common, interoperable data format within the statutory timeframe. The Group promises that even if users exercise their privacy rights (including data portability), the quality of services they receive will not be subject to any discriminatory effects, and supports the implementation of data portability requests with clear, concise, and unambiguous language in prominent positions on websites or applications, answering user inquiries and guiding them through the relevant processes.

The Group does not retain employee, customer, and relevant stakeholder data privacy beyond the necessary period. The retention period is limited to the achievement of the usage purpose, after which data privacy will be promptly deleted. The Group monitors the use of personal data privacy in real time to ensure that personal data is used only for the primary purpose explicitly consented to by the individual, and no data privacy is used for secondary purposes.

The Group commits that without the data subject's separate consent, personal data will not be used for secondary purposes unrelated to the original collection purpose. If monitoring reveals that data has been used for other purposes, the Group will record the proportion, type of use, and compliance basis, and ensure that such use complies with legal and regulatory requirements or the data subject's authorization.

(5) Data Privacy Security Assessment and Continuous Improvement

The Group regularly organizes internal and external data privacy security assessments, develops corrective and preventive measures for identified gaps, and leverages supervisory audit opportunities from external third-party agencies (such as ISO 27001, TISAX) to verify the achievement of the above measures, ensuring the maintenance and continuous improvement of data privacy and security compliance.

Furthermore, the Group conducts systematic and periodic assessments of privacy policy compliance through internal audits and third-party privacy policy compliance audits, ensuring that the effective implementation and continuous improvement of privacy policies form a closed-loop management.

(6) Data Privacy Security Incident Emergency Response

The Group proactively monitors and responds promptly to information security incidents, maintains transparency with stakeholders when incidents occur, and continuously protects the Group's information security and stakeholder interests. The Group formulates *the Business Continuity and Emergency Response Management Procedures*, establishes an information security incident emergency response mechanism, forms an information security incident emergency response team, defines emergency policies and strategies for security incidents, and in the event of data privacy policy changes or data privacy breaches, adheres to the principles of openness and transparency, notifying affected data subjects in a timely manner according to the severity level of the incident.

The Group deploys intrusion prevention systems, situational awareness systems, and other tools to conduct 24/7 uninterrupted monitoring of networks, systems, and applications. The Group regularly backs up critical data and system configurations, maintains operational manuals for the step-by-step recovery of services after system crashes, and periodically tests backup availability. The Group develops business continuity plans, regularly organizes emergency drills simulating real attack scenarios,

tests the entire process from detection, response to communication, and properly retains monitoring reports, incident reports, drill records, and training records, promptly updating and improving emergency response and disaster recovery plans.

The Group expressly declares that all employees, contractors, and temporary staff have the responsibility to promptly report any discovered or suspected information security incidents, vulnerabilities, or abnormal activities. The Group provides multi-channel, convenient reporting paths including direct reporting to supervisors, email, and hotline, offers anonymous reporting options, and strictly prohibits retaliation, reprimand, or discrimination against any person who reports security incidents, vulnerabilities, or suspicious activities in good faith. For employees who successfully prevent significant losses or discover critical vulnerabilities through reporting, the Group will provide public recognition or material rewards.

(7) Data Privacy Security Education and Training

The Group organizes information network security and data privacy protection education and training at least once a year to enhance employees' awareness of network security and data privacy protection, and periodically organizes technology and product exchange seminars on network security and data privacy security to improve the professional awareness and technical capabilities of professionals in network security and data privacy protection.

(8) Compliant Cross-Border Data Privacy Flow

The Group strictly complies with domestic and international legal requirements such as *the Measures for Security Assessment of Cross-border Data Transfer*, and regularly reviews and assesses cross-border data privacy transfer situations each year. Before cross-border data privacy transfer, the Group informs data subjects and obtains their explicit consent, defines the compliance path for cross-border data transfer, and ensures the secure and compliant cross-border flow of data privacy.

(9) Product Data Privacy Protection

When developing, operating, and managing products, services, and systems, the Group strictly follows the requirements of its ISO/IEC 27001 Information Security Management System certification, and has formulated and published *the Information System Security Management Procedures*, and *Malicious Activity Prevention and Control Procedures*, to

maximize the protection of the data privacy and security of the Group, customers, and relevant stakeholders.

(10) Data Privacy Policy Violation Disciplinary Action

Data privacy and security is the Group's solemn commitment to employees, customers, and relevant stakeholders, and the lifeline of enterprise development. The Group commits to a zero-tolerance stance toward violations of data privacy policies. Any violation will be held accountable according to the severity of the circumstances, in conjunction with Human Resources, Legal, and other departments, referencing the *Sunny Optical Technology Employee Reward and Punishment Management Measures* or relevant laws and regulations, demonstrating the Group's determination and responsibility in data privacy protection through concrete actions.

(11) Data Privacy Subject Rights Exercise Channels

The Group fully respects the personal rights and interests of employees, customers, and relevant stakeholders. Data subjects may decide how their personal data is collected, used, retained, and processed in accordance with the law. The Group provides opt-in and opt-out options for individuals, and provides clear and convenient channels to respond to data access requests from employees, customers, and relevant stakeholders for correction or deletion. Any organization or individual has the right to file complaints or reports with relevant functional departments regarding any unlawful data privacy processing activities. The Group will respond to data subject requests within the specified timeframe (e.g., 15 working days) in accordance with laws, regulations, and policy requirements, and promptly inform relevant data subjects of the processing results.

The Group's data privacy subject rights exercise channel: bgs@sunnyoptical.com

V. Supplementary Provisions

(1) This Policy shall be implemented from the date of issuance, published upon CEO approval, and is interpreted and revised by the Group's Information Security Working Group.

(2) The Group reviews this Policy annually and revises it as needed based on changes in laws and regulations and business development needs, ensuring that the Policy's applicability and effectiveness continue to meet compliance requirements.

(3) This Policy, together with the Group's other information security and data management-related policies, constitutes the Group's data privacy and security governance system. In case of any conflict, this Policy shall prevail.