SUNMI

SUNMI GDPR WHITE PAPER

Shanghai Sunmi Technology Co., Ltd.

Address: 6th Floor, 388 Songhu Road, Yangpu District, Shanghai.

Website: https://www.sunmi.com/zh-CN/

Contents

1. Overview

1.1. Scope of Application

The information in this document applies to the products or services provided by SUNMI to users or customers located in the European Economic Area, the United Kingdom and Switzerland.

1.2. Purpose

This document is intended to help customers or users of SUNMI know:

- Basic requirements for GDPR data compliance;
- Data processing roles and obligations of SUNMI in different business models;
- What measures has SUNMI taken for GDPR compliance.

1.3. Definitions

- Personal data means any information relating to an identified or identifiable natural person (**data subject**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- Processor means a natural or legal person, public authority, agency or other body

which processes personal data on behalf of the controller.

2. Overview of General Data Protection Regulation (GDPR)

2.1. Introduction to GDPR

General Data Protection Regulation (GDPR) is one of the most rigorous privacy and data protection regulations in the world, which requires compliance from organizations that process the personal data of any person in the European Union, regardless of where they are located. Effective on May 25, 2018, GDPR has far-reaching implications for data protection worldwide.

2.2. Basic Principles & Core Requirements of GDPR

(1) Basic Principles

- Lawfulness, fairness, and transparency: personal data must be processed in a lawful, fair, and transparent manner.
- Purpose limitations: personal data must be used for legitimate purposes that are explicitly spelled out to a data subject when their information is collected.
- Data minimization: personal data collection should be limited to what is necessary.
- Accuracy: personal data must be updated and accurately kept.
- Storage limitation: personal data can be stored only for no longer than necessary for the purpose for which the personal data are processed.
- Integrity and confidentiality: personal data must be processed using security measures, including technical and organizational measures to prevent unauthorized or unlawful processing and against accidental loss, destruction or damage.
- Accountability: have appropriate measures and records in place as proof of the compliance with the data processing principles.

(2) Data Security

Securely process data using “appropriate technical or organizational measures”, among which technical measures include permission management and data encryption, etc. Organizational measures include setting a complete organizational structure and regular employee training, etc.

(3) Privacy by Design (PbD) Approach

PbD aims to protect individual privacy by incorporating privacy design from the beginning of the development of products, services, business practices, and physical infrastructure.

(4) “Consent” is strictly defined in GDPR, such as:

- A consent must be “freely given, specific, informed and explicit”.
- A consent shall be “presented in a manner which is clearly distinguishable from the other matters, using clear and simple language”.
- The data subject shall have the right to withdraw his or her consent at any time, and their decisions shall be respected.
- Parental consent is mandatory before obtaining the consent from children younger than 13 years old.
- Written consents are required to be retained.

(5) Data Protection Officer (DPO)

Appointing an actual Data Protection Officer is only required by the GDPR if you meet one of the following three criteria:

- Public authority.
- Large scale, regular monitoring: the processing of personal data is the core activity of an organization who regularly and systematically observes its “data subjects” (such as Google).
- The core activities consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences (such as healthcare institutions) referred to Article 10.

A DPO can be named even if organizations are not required to by law.

(6) Protect Data Subject Rights

One of the aims of the General Data Protection Regulation (GDPR) is to empower individuals and give them control over their personal data. The GDPR has a chapter on the rights of data subjects (individuals) which includes the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and the right not to be subject to a decision based solely on automated processing.

3. SUNMI's Role in Data Processing in Different Cooperation Modes

In different cooperation modes between SUNMI and its customers, SUNMI has different roles in data processing and different data protection obligations, which can be roughly divided into the following three modes[1]:

(1) When SUNMI is only a device provider, where SUNMI customers adopt a private cloud deployment mode, that is, data is stored in the server of SUNMI customers, SUNMI does not process any customer or corresponding end user data, and does not need to undertake data compliance obligations under GDPR.

(2) When SUNMI is entrusted by a customer to provide customized devices, and is entrusted by the customer to assist it in providing corresponding device products and services to end users, SUNMI is a data processor to assist SUNMI's customer in processing end user data, and shall bear the obligations of a data processor under GDPR.

(3) When SUNMI directly provides products or services to SUNMI end users, where SUNMI acts as the data controller to process the end user's email address and other information, and SUNMI shall bear the obligations of the data controller under GDPR.

---

[1] Actual situations, which may be more complex and changeable, are simplified into three modes here for ease of understanding.

4. What Measures SUNMI Has Taken for GDPR Compliance

SUNMI has taken a series of measures and made preparations to meet the compliance requirements of GDPR in the following aspects:

4.1. Data Protection Measures

SUNMI has taken measures to protect data as required by GDPR Principles, including:

- **Transparency:** SUNMI informs users through the privacy policy on how SUNMI handles user data when users use relevant products or services provided by SUNMI. Please refer to the Legal Document page of SUNMI for more details. SUNMI will also notify users to read the latest privacy policy using pop-up notices once it makes changes or updates to the privacy policy.
- **Purpose limitation:** SUNMI is committed to processing user data for the purposes stated at the time of data collection, or in the case prescribed by law.
- **Data minimization:** SUNMI makes every effort to adhere to the principle of data minimization in the whole process of product development, such as: data collection minimization: the need for the collection of specified fields will be evaluated in the collection stage; Data storage time minimization: data is stored only for the shortest time necessary to fulfill a specific purpose.

4.2. Technical and Organizational Security Measures

SUNMI has taken a series of technical and organizational data protection measures, including:

(1) Technical Measures

- SUNMI is certified by ISO/IEC 27001 Information Security Management and has taken technical measures involved.
- Terminal security: SUNMI extends its security management of devices to the entire lifecycle to ensure that the device complies with PCI, UnionPay, CC and other standards and specifications from the manufacturing final assembly,

delivery, repair, to decommissioning and other aspects.

- Permission control: SUNMI verifies the identity of the device which accesses to SUNMI backend system to make sure it is authorized, thus to eliminate the risks brought by unauthorized accesses. Permission control and technical measures also have been set in SUNMI to ensure that only necessary employees have access to the data required within their areas of responsibility.
- Systematic data protection measures: SUNMI has taken specific measures like configuring security policies based on service and privacy protection requirements, such as operating system configuration, network configuration, security protection, and database encryption policies, and has set appropriate access control policies and password policies.

(2) Organizational Measures

- **Establish Information Security Committee:** SUNMI has set up an Information Security Committee, which is responsible for a series of organizational activities such as building the information security management system.
- **Establish a Cross-departmental Data Compliance Team:** SUNMI's Legal Department, R&D Center, Commercial & Operation Department and the data compliance consultant jointly set up a Data Compliance Team which is responsible for the company's overall data compliance.
- **Appointment of DPO**: a DPO has been appointed to take a holistic view of the company's data processing, implement new policies related to data synchronization, and follow up the overall data compliance efforts of the company.
- **Strengthen employees' data security awareness:** SUNMI regularly organizes training on staff information and data security, also conducts emergency drills to enhance the emergency response capabilities of all employees in terms of security.
- **Develop appropriate data protection policies:** ***Personal Information***

Security Management System, Data Security Assessment System, Data Security Management Standards and other internal management systems.

- **Establish a data security emergency response system:** a data security emergency response system has been established to deal with possible data leaks among other security issues.

4.3. Adopt Privacy by Design (PbD) Approach

SUNMI takes potential data compliance risks into consideration during function review and server deployment scheme design among other phases in product R&D and service provision, thus to create the design scheme in a comprehensive way.

4.4. Obtain Informed Consent

SUNMI makes every effort to implement the process of informed consent in its products or services, for example:

- When a user activates a SUNMI device for the first time, SUNMI will show the user the ***SUNMI Device Privacy Policy*** and obtain the user's consent.
- When a user registers a SUNMI account, SUNMI will show the user the ***SUNMI Account Privacy Policy*** and obtain the user's consent.
- When a user uses specific services provided by SUNMI, SUNMI will also show the corresponding privacy policies to the user and obtain the consent of the user.

4.5. Cross-border Data Flows

To reduce cross-border data security risks and compliance risks, the personal information and data of users, who have used SUNMI devices, websites among other SUNMI services, can be stored in the servers SUNMI deployed locally or servers managed by customers. SUNMI localized deployment solutions includes: for users in the European Economic Area, the UK and Switzerland, users' personal information will be stored on servers within the European Union; For customers who need private deployments, the users' personal information will be stored on servers specified by customers.

4.6. Protect Data Subject Rights

SUNMI is commited to protecting the rights of data subjects, including:

(1) Informing data subjects of their specific rights and how they can exercise their rights in the privacy policy.

(2) Data subjects can exercise some rights directly on the interactive interface provided by SUNMI, such as accessing and changing some personal information, closing accounts, etc.

(3) SUNMI has specialized personnel to maintain and support the exercise of data subject rights. The Data Compliance Team and relevant business departments will also provide legal and technical support.

5. Conclusion

Protecting data security and user privacy has always been a top priority in the design of SUNMI products. SUNMI will constantly gain insights into legal updates, and optimize internal data compliance processes, iterate product designs, and strive to provide users with products featuring better compliance and tighter security.

This white paper is for informational purposes only and does not have legal force or constitute legal advice.

6. Revision History

Date	Version	Summary
2024-02-01	1.0	