AURORE BONAVIA
AVOCAT EN PROPRIÉTÉ INTELLECTUELLE

Shanghai Sunmi Technology Co., Ltd.
Building 7, Chuangzhi Tiandi, 388 Songhu Road,
Yangpu District, Shanghai

Paris, 21 April 2026

Subject: GDPR Legal Opinion Shanghai SUNMI Technology Co., Ltd.

Shanghai SUNMI Technology Co., Ltd. (the "Company"), incorporated under Chinese law, has an establishment in France and is planning to go public on the Hong Kong Stock Exchange ("the listing"). In this context, the company needs to analyze the compliance of its activities with Regulation (EU) 2016/679 of April 27, 2016 (GDPR) and applicable French national provisions, in particular Law No. 78-17 of January 6, 1978, as amended, as well as the doctrine of the CNIL(National Commission for Information Technology and Civil Liberties)

Documents received from Shanghai SUNMI Technology Co., Ltd:

- GDPR White Paper,
- internal GDPR Data Management Manual,
- Emergency plan in the event of a data breach,
- Processing activity log – data controller (RoPA Controller),
- Processing activity register – processor (RoPA Processor),
- DPIA template (Data Protection Impact Assessment),
- Organizational chart for parent company and EU subsidiaries,
- Official appointment of the DPO and compliance team,
- Letter of appointment of the European representative (Art. 27 GDPR),
- AWS GDPR Data Processing Addendum (DPA),
- Data Processing Agreement (Controller-to-Processor) with Wolt – version 1 and amended version 04.28,
- Standard Contractual Clauses (Modules 2 and 3),
- Transfer Impact Assessments (TIA) completed or templates,
- Appendix III containing the list of subcontractors and organizational measures (with the mention "N/A" for certain partners),
- Information Security Addendum – Clean and HB reply versions with CCV,
- Specific security addenda (Information Security Addendum Terminals – Applied, variants with SUNMI returns),
- Vendor Questionnaire on Information Security and Privacy – ENTEL risk analysis,

EI Aurore Bonavia
Avocat au Barreau du Val d'Oise - Toque 56
SIRET 814 105 748 00044 – TVA intracommunautaire FR40 814 105 748
4 Boulevard Jean Jaurès – 95300 Pontoise
Tél. : 01.85.38.01.45 – Fax : 01.85.38.01.46
contact@aurorebonavia-avocat.fr - https://aurorebonavia-avocat.fr

- The Chinese legal opinion regarding the DATA protection of Shanghai SUNMI Technology Co., Ltd in China,
- SUNMI commercial presentation (SUNMI – BIoT for Business 4.0),
- Access to the SUNMI website and its online policies;
- Additional appendices 6, 7, and 8 detailing technical and organizational measures, digital service mapping, and internal processes,
- GDPR questionnaire updated by SUNMI on August 15, 2025.

1) Background

The purpose of this consultation is to provide a detailed legal opinion on the compliance of the establishment of Shanghai SUNMI Technology Co., Ltd. and its subsidiary "SUNMI Franc SAS" In France with European and French data protection rules, and to identify any corrective actions to be implemented.

The analysis was conducted taking into account:

- The Regulation (EU) 2016/679 (GDPR), in particular Articles 3 (territorial scope), 5 to 6 (principles and legal bases for processing), 24 to 32 (responsibility, security), 33 to 34 (notification of breaches), 44 to 49 (international transfers) and 82 (liability and redress);
- The Law No. 78-17 of January 6, 1978, as amended (the French Data Protection Act), and its implementing decree No. 2019-536 of May 29, 2019, in particular those specifying or supplementing the GDPR in French law;
- Guidelines and recommendations of the French Data Protection Authority (CNIL), as well as relevant opinions of the European Data Protection Board (EDPB);
- Rules derived from Directive 2002/58/EC, known as the ePrivacy Directive, transposed into French law, for the part relating to cookies and other trackers (Article 82 of the aforementioned law).

The scope of this consultation covers:

- The review of internal documents provided by the company, including internal policies, processing records, retention periods, data breach management procedures, impact assessments (DPIAs) and organizational charts;
- Analysis of contracts and clauses relating to data protection (DPA, SCC, TIA) and obligations arising from security agreements with partners (AWS, Wolt, CCV, ENTEL);
- Verification of legal notices, privacy policies, and other information provided to data subjects, including via the website and applications operated in France;
- Monitoring cookie and tracker management practices in accordance with CNIL and GDPR requirements;
- Identifying and assessing any transfers of personal data to third countries, in particular to China, and verifying the compliance mechanisms in place (SCC, TIA, additional measures);

- Assessment of technical and organizational security measures, both internal and contractually required by partners, including GDPR governance (appointment of a DPO, European representative, management of subcontractors).

The analysis also includes operational information provided in the updated GDPR questionnaire and technical appendices, as well as relevant elements from the Chinese legal opinion when these directly concern the French establishment or processing operations targeting the European Union market.

2) Presentation of the company and processing operations

a) Identification of the entity analyzed

The entity subject to this analysis is Shanghai SUNMI Technology Co., Ltd., a company incorporated under Chinese law with its registered office at 6th Floor, 388 Songhu Road, Yangpu District, Shanghai, China.

The French subsidiary, registered in the Lyon Trade and Companies Register under number 847 892 460, with its registered office at 186 avenue Thiers – 69006 Lyon, operates in Europe Union under the company name "SUNMI FRANCE SAS."

It constitutes, within the meaning of Article 3, §1 of the GDPR, an establishment in the European Union, which means that the GDPR applies directly to all of its processing of personal data, including that carried out on behalf of the parent company.

In addition, it has other subsidiaries in the Europe: one in the United Kingdom, one in the Netherlands, one in Poland, and one in Russia. The legal opinion concerns only the subsidiary SUNMI France SAS, as it is the largest among the subsidiaries in European Union with around 35 employees currently.

b) Main activity

SUNMI Group is a global player specializing in the design and supply of smart terminals and BIoT (Business Internet of Things) solutions for professionals in retail, catering, logistics, hospitality, and other sectors.

The offering is divided into several ranges, including:

- Smart mobile terminals (V, L, M Series) integrating payment, printing, barcode and RFID scanning, order management and voice broadcasting functions.
- Versatile payment terminals (P Series) that accept chip card, magnetic stripe, NFC, and QR code payments and can be used at the counter or on the go.
- Fixed and desktop POS terminals (T, D, S Series), integrating software and hardware solutions for sales management and customer experience improvement.

- Interactive kiosks and terminals (K Series) for self-ordering, registration, or information retrieval, reducing operating costs and improving service flow.
- Network peripherals and accessories (routers, cloud printers, cash drawers, scanners), designed to connect and optimize the entire point-of-sale ecosystem.

c) Channels operated

Distribution and customer interaction channels include:

- A global website (www.sunmi.com) accessible from the European Union, offering product pages, customer support, a developer area, and an online store;
- Mobile applications associated with SUNMI products, downloadable from major platforms (Google Play, Apple App Store);
- Proprietary software solutions (SUNMI OS, SUNMI Cloud, SUNMI Digital Store) for equipment management, hosting, and updates;
- Official accounts on professional and consumer social media (LinkedIn, YouTube, WeChat);
- Contractual relationships with distributors, integrators, and technical partners (e.g., AWS, Wolt, CCV, ENTEL) involving customer and user data flows.

According to the map provided in Appendix 7, certain SUNMI platforms and mini-programs are not specifically aimed at the French market (no French language, no delivery or dedicated service) and are therefore not included in the compliance analysis. Only channels accessible from France and likely to process data of individuals located in the EU are included.

d) Types of processing identified

According to internal documents and available commercial information, the main categories of personal data processing carried out by the French subsidiary (SUNMI France SAS) include:

- Customer relationship management and sales prospecting: collection of identification and contact information (B2B and B2C customers), monitoring of exchanges, sending of marketing communications;
- Product supply and maintenance: processing of data necessary for terminal activation, software configuration, remote troubleshooting, and system updates;
- Technical support and after-sales service: recording and tracking customer requests, managing technical incidents, communicating product-related information;
- Digital marketing: use of cookies and trackers for audience measurement and content personalization; use of data from online interactions;
- Human resources management: processing of administrative and professional data of employees and candidates (recruitment, payroll, training);
- Supplier and partner management: processing of contractual and contact data of service providers and distributors;

- Technical subcontracting services: hosting and processing of customer data on behalf of partners under signed DPAs and SCCs.

  According to the information provided in the updated GDPR questionnaire, the company does not currently process data falling under Article 9 of the GDPR. However, certain product ranges (payment terminals or kiosks) could technically allow the collection of biometric data, which would then require the implementation of specific safeguards and the collection of separate explicit consent.

3) Compliance status – data protection obligations

a) Legal basis for processing

(Articles 5 and 6 of the GDPR; Article 5 of Law No. 78-17 of January 6, 1978, as amended)

A review of the available information and documents provided (in particular the GDPR White Paper and the internal compliance manual) shows that "the company" carries out several categories of processing, the legal bases for which are as follows:

- **Performance of a contract** (Art. 6, §1, b GDPR): for processing necessary for the provision of SUNMI products and services, including delivery, activation, maintenance, and technical support;
- **Compliance with a legal obligation** (Art. 6, §1, c GDPR): for certain processing required by tax, accounting or payment security legislation ;
- **Legitimate interest** (Art. 6, §1, f GDPR): for purposes such as information system security, fraud prevention, B2B commercial prospecting or continuous product improvement;
- **Consent** (Art. 6, §1, a GDPR): for sending marketing communications to individual customers (B2C) and for the use of cookies or trackers that are not strictly necessary, in accordance with Article 82 of the French Data Protection Act.

Observation:

Appendices 10 ("RoPA data processing" – role of processor) and 11 ("RoPA controller" – role of controller) have been provided but appear to be largely incomplete at this stage.

They do reflect the structure required by Article 30 of the GDPR (purposes, legal bases, categories of data, retention periods, transfers, security measures), but the fields have not been filled in systematically.
As it stands, it is therefore impossible to assess the correspondence between each processing operation, its purpose and its legal basis, which constitutes a case of incomplete documentation rather than non-compliance.

b) Processing of sensitive data

(Article 9 GDPR; Article 6 of Law No. 78-17)

The information gathered indicates that SUNMI's main activity does not routinely involve the processing of so-called "sensitive" data (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, biometric data , or genetic data), except for the potential processing of biometric data on certain payment terminals or kiosks.

The DPAs and security addenda provide for enhanced protection clauses in the event of sensitive data (e.g., PCI PTS, pseudonymization).

c) Transfer of data outside the EU
(Articles 44 to 49 of the GDPR; Articles 112 to 114 of Law No. 78-17)

The registers and TIA confirm transfers to China (parent company) and potentially to other third countries via technical service providers (e.g., AWS, Wolt).

- AWS: main storage in the EU (Frankfurt), but SCC clauses activated for maintenance outside the EEA,
- Wolt and other partners: SCCs signed (Modules 2 and 3) + partial TIA

SUNMI has further confirmed that "In their major markets — China, the U.S., and Europe (including the U.K.) — data is collected and stored in accordance with the China Personal Information Protection Law, the GDPR, and the CCPA. In order to support their regional sales teams in Europe, certain customer services are handled by their domestic team, which collects certain customer contact information with proper consent, authorization, assessment, and protection measures in place. Saved from the aforementioned contact information, there was no other cross-border transfer of data between China, the U.S., and Europe (including the U.K.) during the Track Record Period and up to the Latest Practicable Date."

Contractual clauses requiring assessment of local laws and notification in the event of access requests from foreign authorities

Observation:

Annex 8 shows that certain commercial data may be accessed by the parent company based in China. Such accessibility constitutes, within the meaning of the GDPR, a transfer of personal data to a third country (Articles 44 et seq.).
If standard contractual clauses (SCCs) and organizational security measures are already in place, no specific assessment report ("Transfer Impact Assessment" or TIA) has been provided for China. However, since the Schrems II ruling (CJEU, July 16, 2020, case C-311/18), such an assessment is required to demonstrate the effectiveness of the safeguards offered during the transfer, taking into account local law and the risks of access by public authorities.

This lack of documentation does not call into question the overall compliance of the

structure, but it is a priority area for improvement in order to strengthen the legal security of international transfers.

d) Subcontracting and joint liability
(Articles 26 and 28 of the GDPR; Article 28 of Law No. 78-17)

SUNMI may act both as a data controller (for its own commercial and contractual purposes) and as a data processor (when processing data on behalf of a customer).

- Subcontracting:

- When the French subsidiary processes data on behalf of a customer, a subcontracting agreement in accordance with Article 28 of the GDPR must be concluded.
- This contract must specify the purpose, duration, nature, and means of processing, as well as the security, confidentiality, and assistance obligations of the processor.
- The documents provided do not confirm the systematic existence of these clauses for all European customers.

- Joint responsibility:

- Where the company jointly determines the purposes and means of processing with another party (e.g., a technology partner or integrator), a joint responsibility agreement (Article 26 of the GDPR) must be established and made available to the data subjects.
- No explicit mention of such agreements was found in the documentation provided.

Observation:

The subcontracting agreements analyzed (DPAs with AWS and Wolt) essentially comply with the requirements of Article 28 of the GDPR: mandatory clauses on security, assistance to the data controller, cooperation, and auditing. The security addenda negotiated with certain service providers (e.g., CCV, ENTEL) further strengthen the level of compliance, in particular by requiring annual audits, strict notification deadlines in the event of an incident, enhanced access controls, and the maintenance of recognized certifications (ISO 27001, PCI DSS, PCI PTS).

However, the internal documentation (Appendix III (5) – register of subcontractors) still contains some fields that are not filled in ("N/A"). However, Article 30 of the GDPR requires that registers be complete and regularly updated. Certain contractual relationships, particularly with CCV, also involve monitoring second-level subcontractors ("sub-processors"), which must be included in the internal documentation.

Overall, the subcontracting agreements comply with legal requirements and provide a satisfactory level of security.

e) Storage and retention period
(Article 5, §1, e GDPR; Article 4 of Law No. 78-17)

Data must be stored in a form that allows the identification of the data subjects for a period not exceeding that necessary for the purposes of the processing.

Best practices require the formalization of a retention period reference document, appended to the processing register, and the technical implementation of these periods (automatic deletion or anonymization).

Existing measures: internal table of retention periods; contractual obligations to delete or return data at the end of the contract (CCV, ENTEL).

Observation:

Appendix 11 – Table for recording data retention periods does not yet systematically specify the applicable legal periods or the criteria triggering erasure, as required by Article 5.1.e of the GDPR. Some lines in the table are filled in, but others remain incomplete ("N/A," periods to be defined).
However, the technical appendices confirm that the company's systems allow for the secure deletion of data. On the other hand, the traceability of these operations (proof of effective erasure via logs) is not expressly documented.

This finding does not call into question the organization's substantial compliance: the technical capacity for deletion exists and is operational.

f) Impact assessments
(Article 35 GDPR; Articles 90 and 91 of Law No. 78-17)

Certain processing operations may present a high risk to the rights and freedoms of individuals, in particular:

- Processing of financial data via payment terminals,
- Processing of location or usage data collected by devices,
- Data interconnection via SUNMI Cloud and associated applications.

The CNIL has drawn up a list of processing operations that systematically require a DPIA (https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-requise.pdf).

The company has provided a DPIA template (Appendix 13: DPIA template), demonstrating its anticipation of regulatory requirements. At this stage, no completed DPIA report has been provided.

The processing records (Appendices 10 and 11) and technical documentation reveal certain

processing operations which, if actually deployed in France or intended for the European public, could fall within the category of high-risk processing within the meaning of the GDPR and the list published by the CNIL (e.g., financial data processed via payment terminals, location data collected by certain devices, centralization of data via SUNMI Cloud).

Observation:

The company already has a compliant methodological tool (DPIA model). At this stage, no non-compliance has been identified as the processing operations in question have not yet been deployed in France.

.

g) Rights of data subjects
(Articles 12 to 23 of the GDPR; Articles 48 to 63 of Law No. 78-17)

Data subjects have the following rights: access, rectification, erasure, restriction, portability, and objection.

The SUNMI website has a privacy policy and a contact form.

In addition, the DPAs concluded with certain partners (e.g., AWS, Wolt – Appendix 4 and subcontracting agreements) provide for a contractual obligation to assist in responding to requests for rights, which demonstrates that this requirement is taken into account in relations with subcontractors.

Observation:

The privacy policy and a contact form are easily accessible on the website, enabling data subjects to exercise their rights (Articles 12 to 23 of the GDPR). Subcontracting agreements (AWS, Wolt) also provide assistance in the event of requests to exercise rights. However, no internal register for tracking requests has been provided to date, which makes it impossible to verify the traceability of responses (Article 12.3 of the GDPR).

h) Data security and breach management
(Article 32 GDPR; Articles 99 to 102 of Law No. 78-17; Decree No. 2019-536)

Measures from Annex 6 and the security addenda:

• ISO 27001, PCI DSS, PCI PTS certifications
• Separation of environments (development/production)
• Physical and logical access controls
• Logging and monitoring
• AES encryption, DES/HTTPS, hash + salt
• incident management with strict deadlines (notification within 24 hours for critical incidents)
• Secure deletion at the end of contracts or when equipment is returned
• Regular employee training
• SBOM and Cyber Resilience Act compliance for certain partners

Note:

The security measures described in Appendix 6 and in the contractual addenda (ISO 27001, PCI DSS, PCI PTS, encryption, logging, separation of environments, training, incident management within 24 hours, secure erasure, etc.) demonstrate a high level of maturity and, in some cases, go beyond the minimum requirements of the GDPR. These contractual standards are a reinforcement rather than a constraint.

4) ePrivacy and cookie compliance

(Article 5(3) of Directive 2002/58/EC, known as the "ePrivacy" Directive; Article 82 of Law No. 78-17, as amended; CNIL recommendations of September 17, 2020)

a) Legal framework

Cookies are text files, often encrypted, stored in the user's browser.

They are created when the browser loads a given website: the site sends information to the browser, which then creates a text file. Each time the user returns to the same site, the browser retrieves this file and sends it to the website server.

They may include "http" cookies, "flash" cookies, invisible pixels or "web bugs," and any other identifier generated by software or an operating system (serial number, MAC address, unique device identifier, or any set of data used to calculate a unique fingerprint of the device, for example, through "fingerprinting").

Cookies are governed, first and foremost, by Directive 2002/58/EC, amended in 2009 (or the "E-privacy" Directive), in Article 5.3, which states that:

- Obtain the user's prior consent before storing information on their device or accessing information already stored on it;
- Unless these actions are strictly necessary for the provision of an online communication service expressly requested by the user or have the sole purpose of enabling or facilitating electronic communication.

This provision has been transposed into Article 82 of the French Data Protection Act and refers to the provisions of Articles 4 (11) and 7 of the GDPR, which specify that consent must be freely given, specific, informed, unambiguous, and the user must be able to withdraw it at any time with the same ease with which it was given.
A distinction is made between cookies that are exempt from obtaining user consent and cookies that must necessarily be accepted by the user.

The CNIL emphasizes that, in order to be exempt from consent, these trackers must: they must:

- Have a purpose strictly limited to measuring the audience of the website or application (performance measurement, detection of navigation problems, optimization of technical performance or ergonomics, estimation of the power of the servers required, analysis of the content consulted), on behalf of the publisher exclusively;
- Not enable global tracking of the browsing behavior of individuals using different applications or browsing different websites;
- Be used solely to produce anonymous statistical data;
- Not lead to cross-referencing of data with other processing operations or to the transmission of data to third parties.

We can therefore list the following cookies:

- Cookies that store the choices made by users regarding the storage of cookies;
- Cookies intended for authentication with a service, including those intended to ensure the security of the authentication mechanism, for example by limiting robotic or unexpected access attempts;
- Cookies intended to remember the contents of a shopping cart on a commercial website or to bill the user for the products and/or services purchased;
- Cookies for personalizing the user interface (choice of language or presentation of a service) when such personalization is an intrinsic and expected element of the service;
- Cookies that enable load balancing of equipment contributing to a communication service;
- Cookies that allow paid sites to limit free access to a sample of content requested by users (predefined quantity and/or for a limited period);
- Audience measurement cookies, subject to compliance with the conditions mentioned above.
  However, cookies that require prior consent from users include:
- Cookies related to personalized advertising operations;
- social media cookies, in particular those generated by their share buttons.

Consent must be obtained prior to the placement and/or reading of cookies. Thus, as long as the person has not given their consent, cookies cannot be placed or read on their device.

If the purposes change, consent must be obtained again.

The validity of consent is linked to the quality of the information received, which must be:

- Visible, highlighted, and complete;
- Written in simple, understandable terms;
- Enable users to be fully informed, in particular about the different purposes of cookies and the identity of the data controller(s).

Therefore, you must:

- Inform the user of all the purposes for which cookies are used, which may be brief and detailed in the privacy policy; and of the list of data controllers;
- Allow the user to give consent through a clear affirmative action: silence no longer constitutes acceptance;
- Allow the user to make a choice by purpose;
- Allow the user to exercise their choices with the same degree of simplicity;
- Allow the user to change their mind.

As a professional and data controller, you must respect users' choices.

On September 17, 2020, the CNIL adopted guidelines on the application of Article 82 of the French Data Protection Act, relating in particular to cookies (Deliberation No. 2020-091) and a recommendation on the use of cookies and other trackers (Recommendation – Decision No. 2020-092 of September 17, 2020).

Firstly, the CNIL reaffirmed certain principles:

- Regarding user consent:
  - Simply continuing to browse a website can no longer be considered a valid expression of the internet user's consent;
  - Individuals must consent to the placement of trackers through a clear affirmative action (such as clicking "I accept" in a cookie banner). If they do not do so, no trackers that are not essential to the functioning of the service may be placed on their device.
- Users must be able to withdraw their consent easily and at any time;
- Refusing trackers must be as easy as accepting them.
- Regarding information for individuals:
  - They must be clearly informed of the purposes of the trackers before consenting, as well as the consequences of accepting or refusing trackers.
  - They must also be informed of the identity of all parties using trackers subject to consent.
- Organizations using trackers must be able to provide, at any time, proof of the valid collection of free, informed, specific, and unambiguous consent from the user.

The CNIL recommends that the consent collection interface should not only include an "accept all" button, but also a "reject all" button.
It also recommends that websites retain consent to cookies for a certain period of time (six months is recommended), as well as refusals.
Finally, if cookies enable tracking on websites other than the one visited, the user's consent must be obtained on each of the websites concerned.

On February 10, 2022, the CNIL issued a decision stating that the use of Google Analytics is contrary to the GDPR in the absence of an adequacy decision. This decision is in line with its European counterparts.

As a reminder, the CJEU invalidated the Privacy Shield, an adequacy decision that ensured an adequate level of protection for data transfers outside the EU.

However, with the entry into force of the European Commission's new adequacy decision on the EU-US cross-border agreement ("Data Privacy Framework") on July 10, 2023, transfers to certified US entities can be made freely.

With this decision, the Commission has decided that the changes made by the United States to its national legislation now ensure an adequate level of protection for personal data transferred from the EU to organizations located in the United States when they take steps to comply with this new "data protection framework." The list of these organizations is managed and published by the US Department of Commerce.

As such, it is now possible to use this tool, as Google is one of the approved companies.

In addition, in September 2021, the CNIL launched a program to identify solutions that can be configured to fall within the scope of the consent exemption.

In September 2021, the CNIL identified various tools that can be identified as serving solely to produce anonymous statistical data, thus allowing for an exemption from consent. You will find the list of tools below:

- The Analytics Suite Delta solution from AT Internet in the version available on March 30, 2021, and referred to in this configuration guide.
;
- The SmartProfile solution from Net Solution Partner in version 21 and covered by this configuration guide;
- The Wysistat Business solution from Wysistat in version 12.1 and covered by this configuration guide;
- Piwik PRO Analytics Suite solution from Piwik PRO in version 15.2.0 and covered by this configuration guide;
- The Abla Analytics solution from Astra Porta in version 1.9 and covered by this configuration guide;
- The BEYABLE Analytics solution from BEYABLE in version 1.0 and covered by this

configuration guide;

- The etracker Analytics solution (Basic, Pro, Enterprise) from etracker in the version available on August 4, 2021, and covered by this configuration guide;
- The Retency Web Audience solution from Retency in version 1.0 and covered by this configuration guide;
- The Nonli solution from Nonli in version 2.0 and covered by this configuration guide;
- The CS Digital solution from Contentsquare in version 10 and covered by this configuration guide;
- The Matomo Analytics solution from Matomo in version 4 and referred to in this configuration guide;
- The Wizaly solution from Wizaly SAS in version 12 and covered by this configuration guide;
- The Compass solution from Marfeel Solutions in version 1.0 and covered by this configuration guide;
- The Statshop solution from Web2Roi in version 1.8 and covered by this configuration guide;
- The Eulerian solution from Eulerian Technologies in version 6 and covered by this configuration guide.
  (source: CNIL)

The CNIL recommends keeping the user's consent or refusal for 6 months.

The recommended duration for cookies (trackers) is 13 months, but 25 months for information collected through these trackers.

https://linc.cnil.fr/fr/cookieviz-une-dataviz-en-temps-reel-du-tracking-de-votre-navigation

b) Observations on the SUNMI website

Observation:
The website www.sunmi.com is accessible from France, but it is not available in French and is not designed to offer products or services specifically intended for the French market. Under these circumstances, it cannot be considered to be aimed at the French public within the meaning of Article 3, §2 of the GDPR. The CNIL's requirements regarding consent to cookies are therefore not fully applicable at this stage.

5) Final observations and strategic recommendations

The analysis carried out on the basis of the annexes provided and the contractual documents shows that "the Company" already has a solid foundation of compliance with the GDPR and the French Data Protection Act. The information provided demonstrates structured governance, comprehensive documentation tools (RoPA, emergency plan, DPIA templates), and technical and organizational security measures aligned with international standards (ISO 27001, PCI DSS, etc.).

At this stage, no major non-compliance issues have been identified. The few points raised mainly concern areas for improvement in documentation or procedures, which are aimed more at strengthening traceability and demonstrating compliance than at correcting actual breaches. In other words, "the company" is broadly compliant with European requirements, and the recommendations set out below should be understood as areas for optimization intended to anticipate any regulatory or contractual changes.

a) Compliance strengths

- Presence of structured GDPR governance: official appointment of a DPO, establishment of a compliance team (Appendix 2 – Appointment of the Data Compliance Team and DPO), designation of a European representative (Appendix 3 – Appointment of European Authorized Representative Letter).
- Existence of records of processing activities (RoPA) for the roles of data controller and data processor (Appendices 10 and 11).
- Internal documentation available: breach response plan (Appendix 14), retention schedule (Appendix 12), DPIA template (Appendix 13).
- Standard contractual clauses (SCC) signed and Transfer Impact Assessments carried out with certain key partners (Standard Contractual Clauses – M2; TIA Importer/Exporter).
- Comprehensive security addenda with high requirements (Information Security Addendum Terminals; CCV, ENTEL, Wolt partner security appendices).
- Contractual commitment with AWS guaranteeing primary storage in the EU (Frankfurt) and SCC mechanisms for transfers outside the EEA (Appendix 4 – AWS GDPR DPA).
- Robust technical and organizational measures documented (Appendices 5 and 6: TOMs, security).

b) Areas for improvement identified without constituting major non-compliance but requiring documentary or organizational updates

- Purpose/legal basis correspondence: no systematic breakdown in the registers (Appendices 10, 11 and 9).
- Conditional DPIA: no DPIA has yet been conducted for high-risk processing, but the template is ready (Appendix 13).

- Rights management: policy and forms exist, but no evidence of a systematic register (Appendix 7).
- List of processors: some "N/A" entries remain in the table (Annex 8).
- Retention periods and erasure: table available (Appendix 12), but no formalized traceability of deletions.
- International transfers: ITAs available (ITAs Importer/Exporter; Appendix 8), but legal analysis of Chinese law remains to be formalized.
- Cookies/ePrivacy: as the website www.sunmi.com is not intended for the French public, there is no non-compliance, but anticipation is recommended.

In conclusion, "the company" already has a high level of maturity in terms of compliance and is overall in compliance with applicable EU data laws in all material aspects. The proposed actions are primarily a means of consolidating documentation and demonstrating compliance even more clearly to partners, investors, and authorities. The current framework is therefore compliant, and the recommendations aim to move from "operational" compliance to "exemplary" compliance.

6) <u>Reservation clause</u>

We are addressing this opinion to the Company, the Joint Sponsors, the Overall Coordinators, and the Underwriters (as defined in in the prospectus of the Company dated April 21 2026 in connection with the Listing) at their request and for their benefit

This opinion is based on the documents and information provided to date, as well as on observation of public interfaces.

It does not prejudge any processing that has not been brought to my attention or any subsequent regulatory, contractual or organizational changes.

Any changes to the processing, the geographical scope of activities or technological partnerships will require a reassessment of compliance.

Yours sincerely,

Aurore BONAVIA