

From

Studio Legale De Berti Jacchia Franchini Forlani

to

OneRobotics (Shenzhen) Co., Ltd.

Milano, Italy

18 December 2025

Dear Sirs,

**Re: OneRobotics (Shenzhen) Co. Ltd – advice on GDPR and NIS 2
compliance legal matters – compliance check of Listing Prospectus as
against Listing Guidelines having regard to GDPR and NIS 2 matters**

as agreed, please find herebelow our legal analysis as requested.

[THE REMAINDER OF THIS PAGE HAS BEEN INTENTIONALLY LEFT
BLANK]

Avv. Roberto A. Jacchia
Avv. Guido E. M. Callegari
Avv. Antonella Terranova
Avv. Barbara Calza
Avv. Cristina Fussi
Avv. Giuseppe Cristiano¹
Avv. Michelangelo Cicogna
Avv. Marco Frazzica
Dott. Massimiliano Gazzo^{2,7}
Avv. Silvia Doria
Avv. Prof. Fabio Ferraro³
Avv. Andrew G. Paton^{1,5}
Dott. Tiziana Zona^{2,7}
Avv. Claudio Corba Colombo
Avv. Prof. Armando Ambrosio
Avv. David Maria Santoro
Avv. Elena Maria Granatello
Avv. Gaspare Roma
Avv. Luca Pescatore
Avv. Andrea Terragni
Avv. Pietro Meda
Avv. Massimo Caiazza⁹
Avv. Chiara Caliendo

Dott. Giulio Francesco Angius
Avv. Isabella Basilico
Avv. Giulia Beneduci
Avv. Matteo Bilei
Avv. Silvia Bolognani
Avv. Laura Bussoli
Avv. Camillo Campi
Avv. Diego Conte
Avv. Francesco De Berti
Avv. Michele De Zio
Avv. Alessandro Foti
Dott. Veronica Franco
Avv. Adriano Garofalo
Aleksy Grechnev⁴
Avv. Giovanni Grossi
Avv. Rachele Maggi
Avv. Benedetta Mazzotti
Avv. Emanuela Monteleone
Avv. Laura Mucciarelli
Avv. Federico Muzzati
Avv. Gaetano Nascimben
Avv. Federico Neri
Avv. Gennaro Paone
Alisa Pestryakova⁵
Dott. Alice Piattelli
Avv. Jacopo Piemonte
Rag. Comm. Nicola Pizzuti
Avv. Alessandro Saracco
Avv. Ilaria Sgrilli
Avv. Maria Francesca Soriano
Dott. Marco Stillo
Avv. Ilaria Uletto
Dott. Angela Valente^{2,7}
Avv. Vittoria Vezzoli
Avv. Francesca Zironi
Avv. Giuseppina Zoccali

Of Counsel

Avv. Giovanni De Berti⁶
Avv. Maria Cristina Franchini

Consulenti

Avv. Marco Brignone
Dott. Ferruccio di Lenardo²
Maria Lovtsova^{4,6}
Avv. Vittorio Poli
Avv. Andrea Sonino

Strategy Consultant

Michael Siebold¹⁰



associazione professionale

Index

SECTION A: COMPLIANCE WITH REGULATION (EU) 2016/679 (GDPR) ..4	
1. Introduction and scope of work.....4	4
2. Description of the Company and basic overview of its operations in the EU 5	5
3. The processing activities subject to the present assessment.....5	5
4. Transparency: compliance with Articles 13 and 14 of the GDPR8	8
5. Lawfulness of Processing: compliance with Articles 6, 7, 9 and 10 of the GDPR9	9
6. Data minimization and storage limitation: compliance with Articles 5 of the GDPR 12	12
7. Data Processing Impact Assessment: compliance with Articles 35 and 36 of the GDPR 12	12
8. Data Transfers to Controllers, Joint Controllers, and Processors, and Transfers of Personal Data Outside the EEA: Compliance with Articles 26, 28, 44 et seq. of the GDPR 13	13
9. Staff Training: compliance with Article 29 of the GDPR..... 17	17
10. Record of processing activities: compliance with Article 30 of the GDPR 17	17
11. Security of processing and data breaches: compliance with Articles 32, 33, 34 of GDPR 18	18
12. Data Protection Officer (DPO): compliance with Articles 37, 38 and 39 of GDPR 19	19
13. EU Representative: compliance with art. 27 of GDPR..... 19	19
14. Minors: compliance with consideranda 38 58 and Article 8 of GDPR .20	20
15. Data subjects' rights: compliance with Articles 12 and 15-22 of GDPR 21	21
16. Sanctions under the GDPR.....22	22
17. Conclusions22	22
SECTION B – COMPLIANCE WITH DIRECTIVE (EU) 2022/2055 (NIS2) ...24	
SECTION C – LISTING PROSPECTUS26	
1. Scope of work.....26	26
2. Answer to Question n. 127	27
3. Answer to Question n. 228	28
4. Answer to Question n. 328	28
5. Conclusions.....29	29

SECTION D – OVERALL CONCLUSIONS.....30

[THE REMAINDER OF THIS PAGE HAS BEEN INTENTIONALLY LEFT
BLANK]

SECTION A: COMPLIANCE WITH REGULATION (EU) 2016/679 (GDPR)

1. Introduction and scope of work

Studio Legale De Berti Jacchia Franchini Forlani (hereinafter referred to as "**the Firm**") has been entrusted by OneRobotics (Shenzhen) Co., Ltd. to assist in (i) reviewing the data processing activities carried out by Wonderlabs, inc., SwitchBot, inc. and Woan Technology Limited (hereinafter, along with OneRobotics (Shenzhen) Co., Ltd., collectively referred to as "**OneRobotics**", "**the Company**", or "**your Company**") in connection with the OneRobotics group's business operations in the European Union (EU), (ii) identifying data privacy risks, and (iii) conducting compliance analysis work in accordance with the General Data Protection Regulation (GDPR) and its implementing rules.

This assessment has been prepared exclusively on the basis of the documentation and information made available to us, all of which were provided in the English language. Specifically, we have received the documents contained in the folder "Documents", which constitute an attachment to this opinion.

In performing the task entrusted to our Firm, we relied on the contents of the memorandum prepared by Jingtian & Gongcheng Law Firm ("**Memorandum**"). We have assumed such information to be accurate, complete, and up to date, and have not undertaken any independent verification or audit of the facts, technical systems, or data processing activities described therein.

Accordingly, the analysis and conclusions contained in this opinion are strictly limited to the scope of the materials reviewed, including the Memorandum, and should not be interpreted as encompassing any document and information, including personal data processing operations or practices, that were not disclosed, described, or otherwise identifiable from the documentation provided. Under no circumstances should this opinion be construed as providing assurances or legal assessments in respect of such other information or documentation which may exist. The analysis and conclusions herein are for OneRobotics (Shenzhen) Co., Ltd.'s benefit only and do not constitute legal advice. This Firm assumes no legal liability in this regard.

2. Description of the Company and basic overview of its operations in the EU

According to the information provided the Company is an AI-embodied home robotics system provider dedicated to building an ecosystem centred on smart home robot products. Your Company primarily targets markets outside China and sells its products through overseas standalone websites and overseas third-party e-commerce platforms.

The Company has not established any legal entity or local employees in Europe. Business operations in the EU region are managed by affiliated companies in the United States of America and Hong Kong, China (namely, Wonderlabs, Inc., SwitchBot, Inc., Wonderlabs Limited, and Woan Technology Limited).

The Company primarily sells smart home products directly to consumers in the EU market through the standalone website (switch-bot.com) and third-party e-commerce platforms (e.g., Amazon Germany, Italy, Spain, and the Netherlands). As of the date of issuance of this opinion, there are about 610,000 users in the EU.

3. The processing activities subject to the present assessment

The data processing activities that are the subject of the present assessment correspond to those identified under Section 1 of the Memorandum. For the sake of completeness and convenience of reference, the relevant section is reproduced in full below, so as to ensure full alignment between the scope of this analysis and the description of the processing operations as originally outlined in the Memorandum.

“The information systems and corresponding data processing involved in the Company's business operations in the EU are as follows:

- 1) *Standalone Website Sales Information Cloud Storage Service System.*
This system is a standalone website for Switchbot product sales (switch-bot.com) built on the third-party Shopify platform, primarily used to provide product introduction, product purchase, and shipping functions. In this system, data of EU users is usually stored on the Frankfurt node in Germany. However, due to cloud server load balancing and other operational needs, user data may also be allocated to and stored on nodes in the United States, Canada and Singapore. The data processed

by this system mainly includes user account registration data on the standalone website, purchase history, shipping information, payment information, browsing history, and cookie records.

- 2)** *Video Cloud Storage System.* *This system is primarily used for the video storage function of Cam products (with video recording capabilities, including SwitchBot Pan/Tilt Cam) sold by your Company. It provides remote monitoring services such as event video storage and real-time viewing to users who have activated video subscription features. The system primarily utilizes a dedicated video cloud storage service provided by the third-party provider Tuya, with data stored on the AWS Frankfurt node. The data processed by this system mainly includes event videos and image data. According to your Company's feedback, such video/image data can only be accessed by users through a unique account and password provided by the third-party provider Tuya, and your Company is unable to access or retrieve this data.*
- 3)** *App & Smart Device Cloud Storage System.* *This system is primarily used to support and respond to the functionalities of the SwitchBot App and intelligent connected devices. The components that serve EU user requests in this system are deployed on the Frankfurt node in Germany. The data processed by this system mainly includes user's App account registration data (email address, nickname, password, preferred language), account login records (date, time, IP address), bound smart product information, App mobile device information (device ID, model, OS system), smart product device information (MAC address, serial number), device event data (e.g., power-on/off records, cleaning paths, battery levels), scene settings (scene name, conditions, execution actions, validity period), home group information, and App geolocation information. Among these, the App geolocation information is mainly used for supporting certain products involving geofencing (e.g., automatic unlock (beta) function of Lock Pro or Lock Ultra). According to your Company's feedback, in certain products/scenes, the location information is only processed locally within the App, and your Company does not collect, track, or store users' location information.*
- 4)** *Third-party Mabang ERP Logistics System.* *This system is primarily used for order shipment on the standalone website. Order data from the standalone website system is directly integrated with this system, which then transmits the data to the corresponding overseas warehouses for shipment. This system is provided by the third party Mabang and is deployed on the Singapore node. The data processed by this system mainly includes order data (product information and quantity) and*

shipping data (shipping address, recipient's name, and recipient's contact information).

- 5) Third-party Zendesk System for Customer Service Management. This system is primarily used to handle after-sales service requests from EU users, providing functions such as online customer support chat and service record tracking. This system is provided by the third party Zendesk Inc., with components serving EU user requests deployed on nodes in the EU. The data processed by this system mainly includes customer service information (e.g., customer service records and case handling status).*
- 6) Third-party E-commerce Platform System. According to the Company's feedback, data (email address, address, and purchase history) generated when users purchase products through third-party e-commerce platforms (e.g., Amazon Germany, Italy, Spain, and the Netherlands) is stored on the servers of these third-party platforms. Logistics data is directly pushed by Amazon Logistics to overseas warehouses for shipping, and such data is processed by third-party e-commerce platforms. The Company only accesses and handles issues in the third-party e-commerce platform system in exceptional cases, such as missing items during shipping or other after-sales issues. Data provided by consumers when purchasing products through agent or distributor channels is collected, used, and processed by agents or distributors. The Company neither obtains nor has the capability to access user data from such channels.*
- 7) Processing of Biometric Features. According to the Company's feedback, while some products are related to biometric features, your Company does not engage in the collection, storage, or processing of biometric features. For instance, in the case of fingerprint unlocking function on smart door locks, the fingerprint information is only stored locally on the device and is not uploaded to cloud servers. Additionally, as of the date of issuance of this Memorandum, your Company is not involved in the analysis, extraction, storage, or processing of facial recognition features or voiceprint recognition features”.*

Having regard to the above information systems and the data processing activities entailed thereby, we provide herebelow our analysis as concerns the following areas of interest: (i) transparency; (ii) lawfulness; (iii) minimisation; (iv) data protection impact assessment; (v) staff training; (vi) record of processing activities; (vii) security of processing and data breaches; (viii) data protection officer; (ix) EU representative; (x) minors; (xi) rights of the data subjects.

4. Transparency: compliance with Articles 13 and 14 of the GDPR

4.1 Actions undertaken by the Company regarding the transparency of processing

The Company has prepared a privacy notice addressed to the data subjects in relation to the processing activities described in the preceding section (**“Privacy Policy”**). In particular, Section 1 (“How We Collect and Use Your Information”) of the Privacy Policy provides a relatively detailed description of the processing operations carried out, outlining the purposes of processing and the corresponding legal basis on which such processing relies (in particular, please refer to paragraph n. 5 herein on lawfulness of the processing).

The subsequent sections of the Privacy Policy include the information required under Article 13 of the GDPR, such as details on the recipients, or categories of recipients, of personal data, information regarding transfers of data outside the European Economic Area (EEA) and the safeguards adopted to ensure adequate protection of the data subject to such transfers, as well as information concerning the identity of the data controller and the contact details of both the controller and the appointed Data Protection Officer (DPO).

The Privacy Policy also outlines the rights of data subjects as provided for under the GDPR and explains the ways in which those rights may be exercised. Furthermore, it specifies the criteria used to determine the data retention periods, thereby contributing to transparency and compliance with the principles of purpose limitation and storage limitation under the Regulation.

A link to the Privacy Notice is clearly visible on the homepage of the Company’s website. As regards the mobile App, a link to the Privacy Notice is also prominently displayed to users at the time of account registration, accompanied by a checkbox allowing them to confirm that they have read the notice. Furthermore, users may consult the Privacy Notice at any time by visiting the “Preferences” section of their profile.

4.2 Company’s compliance status

Overall, the Privacy Policy provides the required information in a manner that is generally clear, concise, easily accessible, and understandable, in accordance with the transparency obligations set out under the GDPR.

In addition, the Privacy Policy appears to have been drafted in substantial compliance with Articles 13 and 14 of the GDPR and can therefore be regarded as meeting the main requirements imposed by the Regulation and achieving

the objectives of transparency and information disclosure expected by European Data Protection Authorities.

However, certain aspects could benefit from greater clarity and detail, as some information might lead to different interpretations. In particular, we suggest, in paragraph 8 (*“Transfer of personal information”*), to include a clear reference to transfers of personal data to specific geographical region(s), also specifying the safeguards and security measures adopted to ensure the lawfulness of such transfers. This addition would strengthen the transparency and comprehensiveness of the Privacy Policy.

5. Lawfulness of Processing: compliance with Articles 6, 7, 9 and 10 of the GDPR

5.1 Actions Undertaken by the Company regarding the lawfulness of processing

Personal data not belonging to particular categories (“common data”)

As indicated in Section 1 of the Privacy Policy, the processing activities are generally performed on one or more of the following grounds: the data subject’s consent, the performance of a contract, compliance with a legal obligation, or the Company’s legitimate interest, depending on the specific nature of each processing activity.

Biometric data

Based on the documentation reviewed — and in particular the contents of the Privacy Policy and the Memorandum —the Company may process biometric data for the purpose of user’s identification. For example, as stated in the Privacy Policy, *“For smart lock, keypad, and smart doorbell, the fingerprint and facial recognition data collected are only stored on the device side, for the purpose of verifying your identity”*.

It should be noted that biometric data processed for the purpose of uniquely identifying an individual fall within the scope of special categories of personal data as defined under Article 9(1) of the GDPR, which generally prohibits their processing unless one of the exceptions set out in Article 9(2) applies.

According to the information made available, the Company appears to require the user’s explicit consent directly through the device interface before activating biometric functionalities.

5.2 Company's compliance status

Personal data not belonging to particular categories ("common data")

While acknowledging the Company's general compliance with the GDPR regarding the lawfulness of the processing, certain editorial and structural improvements could enhance the clarity and transparency of the Privacy Policy, ensuring that data subjects can more easily understand the legal basis applicable to each type of processing.

In particular, Section 1 of the Privacy Policy lists among the legal basis the following statement:

"Process personal information that you disclose yourself or that has been legally disclosed by others within a reasonable scope and in accordance with the law".

This formulation does not correspond precisely to any of the legal basis under Article 6 of the GDPR, and it is not immediately clear which specific processing operations it refers to. While there are no elements suggesting that the related processing is unlawful, it is recommended that the Company clarifies which activities this clause concerns and explicitly link them to one of the recognized legal basis under the GDPR (e.g., consent, contractual necessity, legal obligation, or legitimate interest).

With respect to the processing operations listed under Section 1 of the Privacy Policy, such as:

- *"Process and fulfil your purchases"*
- *"Providing the product or service: ensure our products operate as intended and expected"*
- *"Customer support: diagnose product problems, repair customers' devices, and provide other customer care and support services"*
- *"Product activation and registration"*
- *"Product improvement"*
- *"Security, safety and dispute resolution"*

- *“Business operations”*
- *“Marketing communications”*
- *“Support communications”*
- *“Detect, investigate and prevent fraudulent transactions and other illegal activities and protect the rights and property of you and others”*

the Privacy Policy refers to the legal basis as *“Other situations stipulated by laws and administrative regulations”*.

This reference may be misleading, since many of the above processing activities would not normally rely on a legal obligation but rather on the user’s consent, the performance of a contract, or the Company’s legitimate interests.

Where processing is based on legitimate interests, it would be advisable to more clearly articulate the specific legitimate interest pursued by the Company or third parties, as required by Article 13(1)(d) GDPR.

Biometric data

On the basis of the information provided, whilst certain biometric data are processed by the single device and stored therein, we are given to understand that (i) the end user is requested to consent such activity; and (ii) the Company does not access such biometric data and, henceforth, not to process those. We are also given to understand that certain new products might, in the future, require the processing of users’ biometric data. User’s explicit consent directly through the device interface are advised to be obtained prior to enabling the biometric functions. Such a mechanism, whereby the user actively provides consent on the device itself, would constitute a valid legal basis under Article 9(2)(a) of the GDPR, thereby allowing the lawful processing of biometric data for the specific purpose of identity verification.

This approach, if effectively implemented as described, would support full compliance with the GDPR requirements concerning the processing of special categories of personal data, as it ensures that consent is both informed and freely given, and obtained before any processing occurs.

6. Data minimization and storage limitation: compliance with Articles 5 of the GDPR

Based on the documentation received, we obtained on a sampling basis an overview of all personal data processed, including the specific retention periods and the detailed data minimization measures applied in relation to the purposes pursued.

On that basis, we note that the Company has, in all material respects, implemented noteworthy and virtuous practices in line with data protection principles. For instance, biometric data is not collected nor retained, reflecting a proactive approach to minimizing sensitive data processing.

Furthermore, based on the Memorandum, we learn that *“the Company adopts differentiated storage strategies based on various data types. For instance, the standalone website data, as well as App and device data collected by the Company are stored on a long-term basis in accordance with business needs. Such data will be deleted when users delete their accounts or initiate data deletion requests. Device usage records are retained for one year and are automatically deleted upon expiry”*. This would suggest that the Company has implemented structured data retention policies consistent with GDPR principles, including purpose limitation and storage limitation.

Overall, while a complete picture cannot be fully reconstructed from the documentation alone, there are no indications of processing activities that would appear to contravene GDPR principles, and the measures observed suggest a strong commitment to compliance, data protection, and privacy-conscious practices.

7. Data Processing Impact Assessment: compliance with Articles 35 and 36 of the GDPR

7.1 Actions Undertaken by the Company regarding the data protection impact assessment

Pursuant to Articles 35 and 36 of the General Data Protection Regulation (GDPR), data controllers are required to conduct a Data Protection Impact Assessment (“**DPIA**”) whenever a type of processing — particularly when using new technologies — is likely to result in a high risk to the rights and freedoms of natural persons. The purpose of a DPIA is to identify, assess, and mitigate the potential risks associated with processing operations that could significantly affect data subjects.

From the information made available, the Company has already prepared a DPIA template designed to be used whenever a processing operation potentially falls within the scope of Article 35 GDPR. This proactive measure reflects a readiness to comply with the relevant regulatory requirements and demonstrates the Company's awareness of its accountability obligations under the GDPR.

At present, the Company is assessing whether any of its ongoing or planned processing operations require a formal DPIA, in accordance with the risk-based approach mandated by Article 35. Moreover, should a DPIA indicate that the envisaged processing activities are likely to present a high residual risk even after mitigation, the Company acknowledges its obligation to consult the competent Supervisory Authority under Article 36 GDPR prior to commencing such processing.

7.2 Company's compliance status

Based on the information currently available we believe the Company is taking actions so as to ensure its compliance with this specific GDPR requirement.

8. Data Transfers to Controllers, Joint Controllers, and Processors, and Transfers of Personal Data Outside the EEA: Compliance with Articles 26, 28, 44 et seq. of the GDPR

8.1 Actions Undertaken by the Company regarding the transfer of personal data

Data sharing with data controllers and processors in EU or US may occur:

- (a) *"In scenarios involving third-party e-commerce platforms (Amazon Germany, Italy, Spain, and the Netherlands), Amazon, acting as an independent data controller, collects consumers' personal data and shares certain data with SwitchBot (order details for abnormal orders, shipping addresses, and recipient email addresses) for purposes such as order fulfilment and marketing. Amazon discloses in its Amazon Privacy Policy the circumstances under which it provides information to third-party sellers. SwitchBot, acting as an independent controller, processes this data based on the necessity for contract performance.*

- (b) Shopify (Standalone Website Scenario): SwitchBot entrusts Shopify to process user information via its standalone website (switch-bot.com), including account information, purchase history, shipping addresses, and user tags. SwitchBot is the data controller, and Shopify is the data processor. The two parties have entered into the Shopify Terms of Service and Shopify Data Processing Addendum online, which clearly specify Shopify's obligations, including processing data as instructed, fulfilling confidentiality obligations, and implementing security safeguards.*
- (c) AWS (App Scenario): SwitchBot entrusts AWS to provide data storage services for the SwitchBot App, including the storage of account data, device data, and device usage information. SwitchBot is the data controller, and AWS is the data processor. The two parties have signed the AWS services terms and AWS Data Processing Addendum.*
- (d) Zendesk (Customer Support Scenario): SwitchBot entrusts Zendesk to process customer service data, including after-sales feedback and resolution records. SwitchBot is the data controller, and Zendesk is the data processor. Zendesk offers the Data Processing Agreement and completes agreement signing with SwitchBot through the Signing Process, clearly defining data protection responsibilities”.*

We acknowledge the above based on the Memorandum.

Transfer of personal data to China

With regard to the transfer of personal data to China, there exist two separate Transfer Impact Assessments (TIAs) in order to evaluate the level of protection afforded to the transferred data and the potential risks associated with such transfers.

Specifically, one TIA concerns the data transferred by SwitchBot Inc to Woan Technology (Shenzhen) Co., Ltd. (“**Woan**”), while the other relates to the data transferred by Wonderlabs Inc to the same Woan.

Furthermore, it was possible to review the Standard Contractual Clauses (SCCs) executed between SwitchBot Inc and Shanghai Mabang Technology Co., Ltd (“Mabang”). SwitchBot Inc entrusts Mabang with the processing of warehouse logistics information (shipping details and shopping order information) for order shipment and warehouse management. SwitchBot Inc is the data controller, Mabang is the data processor, and the overseas warehouse service provider is the data sub-processor.

According to the information contained in the Transfer Impact Assessments (TIAs), Standard Contractual Clauses (SCCs) have been executed between SwitchBot Inc and Woan and between Wonderland Inc and Woan in relation to the transfer of personal data described in the TIAs. However, such documents were not available for review, and our assessment is therefore based solely on the representations included within the TIAs. In this respect, we have proceeded on the assumption that the SCCs have indeed been duly executed, that the appropriate set of clauses has been selected in accordance with the respective privacy roles of the parties according to GDPR, that the annexes have been properly completed, and that the standard wording has not been altered or modified.

Transfer of personal data to Singapore

The Memorandum also indicates that personal data may be transferred to Singapore through the service provider Mabang. As described, we have received the SCCs executed between SwitchBot Inc and Mabang.

8.2 Company's compliance status

Data sharing with data controllers and processors in EU or US:

The Company has relied on international service providers of proven reliability and reputation, selected on the basis of their ability to ensure compliance with the data protection principles set forth under the EU General Data Protection Regulation (GDPR), including the safeguards and contractual guarantees required under Article 28 GDPR. These providers offer robust technical and organizational measures, standardized compliance frameworks, and internationally recognized certifications, which collectively contribute to ensuring a high level of protection for the personal data processed on behalf of the Company.

Transfer of personal data to China

Regarding the TIAs, it should be noted that our review has been conducted exclusively from the perspective of European data protection law, and we do not possess specific expertise in Chinese national legislation, including its regulatory framework on data protection, cybersecurity, or cross-border data transfers.

Consequently, we are not in a position to verify whether Chinese legislation effectively allows for the protection of personal data in a manner consistent with

the requirements of European law, and we cannot assess or express any opinion on the accuracy, completeness, or legal adequacy of the analyses and conclusions contained in the Transfer Impact Assessments (TIAs) with respect to the interpretation or application of Chinese law.

With specific reference to the SCCs related to the transfer of personal data to China, we are aware that the following have been signed:

- SCCs between SwitchBot Inc and Mabang
- SCCs between SwitchBot Inc and Woan
- SCCs between Wonderlab Inc and Woan

The Company has appropriately regulated the aforementioned personal data transfers through the use of SCCs and these may be used as valid legal basis for the data transfer.

At the same time, the Transfer Impact Assessments (TIAs) – which refer to Woan but not Mabang – indicate that *“User’s consent is the legal basis for the Cross-border Transfer. Woan Technology (Shenzhen) Co., Ltd will have remote access to the APP device data, smart hardware device data, and user emails of those who have selected the consent of the Cross-border Transfer in the Privacy Policy”*.

On the basis of the information provided such consent is required by Chinese law but not necessarily meets the requirements of Article 7 of the GDPR; yet we confirm that the SCCs may be a sufficient legal basis to the transfer according to the GDPR.

Transfer of personal data to Singapore

While draft Standard Contractual Clauses (SCCs) relating to the transfer of personal data from SwitchBot Inc to Singapore have been made available and are declared as being in the process of being executed, no corresponding Transfer Impact Assessment (TIA) has been provided for review.

Since the European Commission has not adopted an adequacy decision with respect to Singapore’s data protection regime, the completion of a TIA constitutes a necessary step to assess the potential risks associated with the transfer and to verify the effectiveness of the safeguards implemented under the SCCs. The absence of such documentation therefore prevents a full evaluation of the compliance of this transfer mechanism with the requirements of Chapter V of the GDPR.

Furthermore, the available documentation does not clearly indicate whether other entities within the group – such as Wonder Inc – also rely on Mabang for the provision of their services and, in doing so, entrust the latter with the processing of personal data.

Should this be the case, the appropriate safeguards and contractual measures required under the GDPR would also need to be implemented with respect to such data transfers, in order to ensure compliance with the obligations set forth in Chapter V of the Regulation.

9. Staff Training: compliance with Article 29 of the GDPR

9.1 Actions Undertaken by the Company regarding staff training

Based on the documentation and information made available, the Memorandum indicates that employees have been trained on personal data protection as requested by art. 29 of GDPR.

9.2 Company's compliance status

On the basis of the information provided, as confirmed in the Memorandum, the Company delivers training in data protection to its employees. .

At the same time, we can confirm that this initiative, if effectively implemented, reflects the Company's commitment to fostering a culture of compliance and accountability within its organization and is in line with the best practices recommended by data protection authorities across the EU.

10. Record of processing activities: compliance with Article 30 of the GDPR

10.1 *Actions Undertaken by the Company regarding the record of processing activities*

The Company has developed and adopted a structured template for the preparation of its Record of Processing Activities (RoPA).

This template includes all elements required under Article 30 of the GDPR and is designed to provide a comprehensive and consistent description of all personal data processing operations carried out by the Company and falling within the scope of the GDPR.

10.2 Company's compliance status

Although the Company has not yet finalized or formally completed its Record of Processing Activities, it has nevertheless already demonstrated a clear understanding of the nature and characteristics of the processing operations falling within the scope of the present assessment, including those involving data subjects located within the European Union.

The Company has expressed its intention to complete and formally populate the RoPA in the near future, ensuring that it accurately reflects the purposes, scope, and legal basis of all data processing operations, as well as the applicable technical and organizational measures adopted for the protection of personal data.

Once finalized, this document will enable the Company to fully meet the requirements of Article 30 GDPR and further reinforce its accountability framework, ensuring that all processing activities are properly documented, transparent, and aligned with the principles of the Regulation.

11. Security of processing and data breaches: compliance with Articles 32, 33, 34 of GDPR

11.1 Actions Undertaken by the Company regarding the security of processing and data breaches

The Company has established the Security Incident Response Process, which encompasses procedures for incident identification, assessment, reporting, and recovery. It clearly defines the handling measures, regulatory reporting obligations, and notification requirements following the occurrence of security incidents.

11.2 Company's compliance status

It should be emphasized that the assessment currently being conducted is strictly legal and compliance-focused and does not cover technical or organizational security measures implemented by the Company.

Our review is therefore limited to the legal frameworks, policies, contractual arrangements, and procedural aspects relating to the processing and transfer of personal data, without expressing any opinion on the effectiveness or adequacy of technical or security controls that the Company may have in place.

According to the Company's feedback, as of the date of issuance of this opinion, the Company has not experienced any data security incidents such as data breaches during its operations in the EU. Furthermore, the Company indicates that it has not been inspected, investigated, nor sanctioned by local regulatory authorities for data privacy issues, nor has it been involved in any litigation related to data privacy.

12. Data Protection Officer (DPO): compliance with Articles 37, 38 and 39 of GDPR

12.1 Actions Undertaken by the Company regarding the appointment of a data protection officer

The Company has appointed a DPO and has clearly published the DPO's contact details in its Privacy Policy, which reflects a commitment to transparency and to facilitating communication with data subjects regarding their privacy rights.

12.2 Company's compliance status

Based on the information provided, we are given to understand that the Company has appointed a DPO and hence to be compliant with GDPR requirements in this respect.

At the same time, we remind the Company that the DPO should (i) be conversant with the GDPR; (ii) be able to communicate with the competent authorities and the data subjects; (ii) be independent and made available of a budget. Finally, we also want to remind the Company it should also notify the competent Data Protection Authority of the appointment of the Data Protection Officer pursuant to Article 37(7) of the GDPR.

13. EU Representative: compliance with art. 27 of GDPR

13.1 Actions Undertaken by the Company regarding the appointment of an EU Representative

The Company has not yet appointed an EU Representative as required under Article 27 GDPR, yet it indicates that it intends to do so in the near future.

13.2 Company's compliance status

Based solely on the information provided in the Privacy Policy and the Memorandum, the Company's intention to appoint an EU Representative reflects an awareness of its obligations under the GDPR. Although the appointment has not yet been completed, given the Company's stated plan to regularise this matter in the near term and the absence of any indication of enforcement action or complaint, the risk associated with non-compliance with Article 27 is considered low.

14. Minors: compliance with consideranda 38 58 and Article 8 of GDPR

14.1 Actions Undertaken by the Company regarding the protection of minors' personal data

The Privacy Policy clearly states that *"We do not provide services to children, and we do not knowingly collect or maintain information about persons under 18 (Or the age required by local law) years of age. If We learn that personal information of children has been collected on or through the sites, we will take appropriate steps to delete this information. If you are the parent or legal guardian of a child under the age of 18 and believe that your child has provided us with personal information, please contact us and we will terminate the child's account or service and delete the personal information"*.

However, with regard to the SwitchBot App, users are required, at the time of registration, to declare that they are at least 13 years old (or of the applicable age of consent in their country or region).

14.2 Company's compliance status

Whilst the statements contained in the Privacy Policy appear to be fully aligned with the requirements of the GDPR, there appears to be an inconsistency between what is declared in the Privacy Policy — namely, that the services and products offered are not intended for individuals under the age of 18 — and what is requested during the registration process within the App, where users are asked to confirm that they are at least 13 years old.

For this reason, we recommend amending the registration process in the SwitchBot App so that users are required to confirm that they are 18 years old (or such other age which happens to be the age of majority in the country or region concerned). In this respect, we have been advised that the Company

will, by the end of this month, require user to confirm they are 18 years old or older.

As an alternative, the Company may (i) change the Privacy Policy so as to read that the Company does not provide services to minors; and (ii) change the declaration requested by the SwitchBot App so that users are requested to confirm that they are not minors in accordance with the applicable law.

15. Data subjects' rights: compliance with Articles 12 and 15-22 of GDPR

15.1 Actions Undertaken by the Company regarding the rights of data subjects

The rights of data subjects are clearly and comprehensively described in the Company's Privacy Policy, ensuring transparency regarding how individuals may exercise their rights under the GDPR. The information provided outlines the relevant procedures, contact channels, and expected response times. Nonetheless, the Company must take into consideration the suggested improvements outlined in paragraph 4 hereinabove.

The Company has established both a dedicated channel on its website (<https://support.switch-bot.com>) and an email address (privacy@switch-bot.com) for receiving requests from data subjects wishing to exercise their rights. These channels are clearly and properly indicated in the Privacy Policy. According to the Privacy Policy, the Company is also fully aware of the regulations governing the handling of data subject requests, particularly with regard to verifying the data subject's identity, ensuring that responses are provided free of charge, and complying with the 30-day response period from receipt of the request.

Moreover, according to the Memorandum, the Company *"also provides contact information (privacy@switch-bot.com) and supports users in exercising their rights through the SwitchBot App (e.g., "Profile - Manage Accounts - Delete Account")"*.

With respect to marketing communications, as stated in the Privacy Policy, such communications include a link that allows users to easily "unsubscribe" and thereby withdraw their consent to receive promotional materials.

Finally, according to the Memorandum, the Company adopted an internal procedure to manage data subjects requests.

15.2 Company's compliance status

The Company appears to be aware of the rights granted to data subjects under the GDPR and seems to have fulfilled the related obligations. It has also adopted an internal procedure which, although not mandatory, plays a fundamental role in ensuring that data subjects receive comprehensive responses to their requests within 30 days and that their rights are duly protected.

16. Sanctions under the GDPR

The areas of non-compliance (or those of partial compliance), where not rectified, could expose the Company to sanctions in accordance to Article 83 of the GDPR. Such sanctions could be of significant economic and reputational impact and can be calculated either as a fixed sum or as a percentage of the Group's total worldwide annual turnover.

There are two levels of maximum fines:

1. Up to €10 million, or 2% of the total worldwide annual turnover, whichever is higher, for less severe infringements (e.g., certain obligations of data controllers and processors).
2. Up to €20 million, or 4% of the total worldwide annual turnover, whichever is higher, for more severe infringements (e.g., violation of core data protection principles, data subjects' rights, or international transfers of personal data).

It is important to note that these are maximum fines, and in practice, regulatory authorities rarely impose the full amount.

17. Conclusions

The Company has evidently undertaken significant efforts to ensure a level of data protection comparable to that required under European law. Policies, procedures, and contractual safeguards appear to reflect a strong commitment to GDPR principles and data privacy best practices with its efforts being particularly evident in relation to the transfers of personal data to China.

Based on the documentation and information reviewed, it can be stated that the Company's processing activities appear largely compliant with applicable data protection requirements. However, our analysis has also identified certain measures that are still in the process of being implemented or that should be implemented. Accordingly, these actions when implemented are expected to further improve the level of compliance with the GDPR of the Company.

[THE REMAINDER OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK]

SECTION B – COMPLIANCE WITH DIRECTIVE (EU) 2022/2055 (NIS2)

Directive (EU) 2022/2555 (the NIS 2 Directive) aims to ensure a high common level of cybersecurity across the EU, with the objective of supporting the proper functioning of the internal market. Its scope of application is primarily determined by two criteria: the type of entity and its size. Article 2 provides that the Directive applies to public or private entities of a type listed in Annex I or II, which are considered medium-sized enterprises or larger enterprises. Annex I identifies sectors of high criticality, while Annex II lists other sectors considered essential for the functioning of the economy and society.

The sale of connected consumer electronic products and the provision of associated digital services, such as software updates, mobile applications, or cloud-based data storage and processing, could potentially fall within relevant categories, such as the “manufacture of computer, electronic, and optical products” or providers of certain digital services. These activities may constitute the provision of services within the Union, which is central to the possible applicability of the Directive.

However, since the Company does not have any establishment within the European Union, the first step is to assess whether the NIS 2 Directive can apply to an entity established outside the EU. The NIS 2 Directive does not explicitly provide for an extraterritorial mechanism comparable to that of the GDPR. Therefore, it is necessary to verify how each Member State has transposed the Directive into its national legislation.

We have reviewed the Italian Legislative Decree 138/2024, which implements the NIS 2 Directive in Italy, and understand that the Company should not fall within the scope of the Italian implementing provisions. However, this assessment may vary depending on the Member State concerned. In particular, since, based on the Memorandum, the Company appears to sell its products not only in Italy but also in Germany, Spain, and the Netherlands, it should be verified whether and how these countries have transposed the Directive, specifically with regard to its potential applicability to non-EU entities.

In conclusion, on the basis of the information provided, it is unlikely, but cannot be ruled out, that the Company’s activities could fall within the scope of the NIS 2 Directive. Should this be the case, the Company would be required to comply with several key obligations, primarily focused on cybersecurity risk management and incident reporting, including establishing a robust

governance framework for cybersecurity, implementing proactive risk assessments, and adhering to incident reporting requirements. These obligations may differ across EU Member States.

[THE REMAINDER OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK]

SECTION C – LISTING PROSPECTUS

1. Scope of work

The purpose of this section of this opinion is to verify whether the information disclosed by the Company in its listing application with the Hong Kong Stock Exchange (“**HKEX**”) complies with the requirements set out in the “HKEX Guide to new listing applicants” whose business involves the provision of internet information services (“**Guidelines**”). Our work is limited to the following questions:

1. **Question n. 1:** the regulatory framework governing the provision of internet information services, including any licensing requirements and foreign ownership restrictions;
2. **Question n. 2:** the management of personal data obtained in the course of the Company’s business operations, including the policies and measures adopted for data collection, storage, processing, usage, transfer, disclosure, retention, and destruction; and
3. **Question n. 3:** the status of compliance with personal data and privacy protection laws and regulations in all relevant jurisdictions, including any material data breach incidents, if any.

The scope of our review is therefore limited to assessing whether the Company’s listing materials (“**Listing Prospectus**”) appropriately address and disclose the information required under the Guidelines in connection with the above Questions. This opinion does not extend to any other matter in general and, in particular it does not amount to a technical, operational, or cybersecurity audit, nor does it involve an assessment of the adequacy of the Company’s IT systems or internal controls.

It should also be noted that our analysis has been conducted exclusively on the information and documentation provided – a full list of which is contained in the attached folder named “Documents” – which have been scrutinised and analysed from a European data protection law prospective only, and in particular with reference to the principles and terminology of the EU General Data Protection Regulation (GDPR). At the same time, one must always consider that we are not Hong Kong lawyers nor are lawyers qualified in countries other than Italy, and this opinion should not be interpreted as a legal assessment under Hong Kong legislation or otherwise and our answers to Questions 1, 2 and 3 below shall be considered and relied upon accordingly.

2. Answer to Question n. 1

The Guidelines at page 3.7-4 request to applicants *“whose business involves the provision of internet information services”* the disclosure of the applicable regulatory framework, including any licensing requirements and foreign ownership restrictions.

Based on the information made available to us, and in the absence of any specific definition of “internet information services” within the Guidelines to the contrary, it is our understanding that the Company’s business activities may fall within this category. Consequently, the Company may be required to provide additional disclosure regarding the applicable regulatory framework.

In this respect the Listing Prospectus, at page 74, mentions that the Company is subjected to: *“General Data Protection Regulation (“GDPR”) in the European Union, Act on the Protection of Personal Information in Japan (“APPI”), and various state-level privacy laws in the United States, see “Regulatory Overview — B. Japan Laws and Regulations — Laws and Regulations in Relation to Personal Data Collection”, “Regulatory Overview — C. U.S. Laws and Regulations — Laws and Regulations in Relation to Data Privacy” and “Regulatory Overview — D. Germany and European Union Laws and Regulations — Laws and Regulations relating to Data Protection”*. Furthermore, it is also stated that the Company: *“may also become subject to additional regulatory requirements regarding data protection and data privacy, which may necessitate adjustments to our data framework and incur additional costs”*.

GDPR is also mentioned in the “Regulatory Overview” Section of the Listing Prospectus, page 148.3.

That said, the Listing Prospectus clearly states that the GDPR applies to certain personal data processing activities carried out by the Company. With respect to national laws, the Listing Prospectus explicitly identifies German data protection legislation, also mentioned in the Regulatory Overview section.

It should also be noted that, in addition to German law, the Company is expected to comply with other applicable national data protection laws, including any relevant decisions or guidance issued by the competent national Data Protection Authorities, as part of its overall compliance framework.

This should be disclosed in the “Regulatory Overview” Section of the Listing Prospectus.

The Listing Prospectus does not contain an explicit reference to other European regulatory frameworks, including the recently adopted Regulation (EU) 2023/2854 (Data Act) which may be applicable to the Company.

3. Answer to Question n. 2

Based on the documentation made available to us, at page 259 of the Listing Prospectus the Company has provided a coherent overview of its personal data processing practices.

That said, the description of the processing activities currently included in the listing materials does not appear to be particularly detailed and may be considered insufficient to provide a complete understanding of the nature and scope of the Company's data processing operations. For example, the Listing Prospectus does not provide complete details regarding certain key aspects of the Company's data processing activities. In particular, the categories of personal data processed are only partially specified, the purposes of the processing are not fully described, and the retention periods are indicated only in general terms, stating that the Company follows "*the shortest necessary storage period*" and stores data "*for the minimum period required by our business*". Furthermore, the Prospectus does not provide detailed information on the locations where the data are stored, or on the specific security measures implemented to protect such data.

In this respect, the finalization of the record of processing activities ex art. 30 GDPR, together with the inclusion of the relevant information in the Listing Prospectus, would represent a valuable step forward to both strengthen the Company's compliance with the GDPR and facilitate a more comprehensive and structured disclosure of its data processing operations.

In conclusion, whilst the Company has already included a general description of its processing activities within the Listing Prospectus, we cannot be certain that such disclosure is sufficiently detailed to fully meet the expected standards of completeness required by HKEX.

4. Answer to Question n. 3

With respect to the Company's compliance status regarding GDPR and NIS 2 obligations, we wish to refer to the paragraphs of this opinion specifically dedicated to such matters.

By way of summary, though, we can confirm that based on the information presented in the Listing Prospectus and the level of compliance disclosed

therein, it appears that the Company has outlined in a clear and structured manner the various actions undertaken to align its operations with GDPR requirements. Whilst the description is rather concise, it does nonetheless provide an overview of the Company's compliance efforts, highlighting the key measures implemented and the general approach adopted to ensure data protection and regulatory compliance.

At the same time, the adoption of certain additional measures is advisable to achieve full compliance with the GDPR, and further actions may be required to ensure conformity with other European laws. As a matter of fact, the Listing Prospectus does not account for ongoing nor incomplete measures.

The assessment of compliance with regulations other than GDPR and NIS 2 is beyond the scope of this review.

5. Conclusions

Overall, the Company has demonstrated a high level of diligence and commitment in preparing the Listing Prospectus, providing a clear overview of its data protection framework and the measures undertaken to ensure GDPR compliance. The disclosures reflect a structured and thoughtful approach to privacy and data protection, and the Company's efforts are commendable.

That said, it cannot be excluded that HKEX may request further details or additional clarifications regarding certain aspects of the information presented in the Listing Prospectus.

[THE REMAINDER OF THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK]

SECTION D – OVERALL CONCLUSIONS

On the basis of the analysis carried out and described in this opinion, we confirm that the Company appears having kept a high level of diligence and commitment in preparing the Listing Prospectus, providing a clear overview of its data protection framework and the measures implemented to ensure compliance with the GDPR. The disclosures reflect a structured and thoughtful approach to privacy and data protection, and the Company's efforts in this regard are commendable.

In particular, based on the documentation and information reviewed, the Company's personal data processing activities appear largely compliant with the applicable requirements under the GDPR. At the same time, we have found and suggest certain ambits of intervention which combined with certain measures which the Company is still in the process of being completed, are capable of improving the level of compliance with the GDPR.

With respect to the NIS 2 Directive, and on the basis of the information provided, it appears unlikely — though it cannot be entirely ruled out — that the Company's activities would fall within its scope of application. Should this nevertheless be the case, the Company would be required to comply with specific obligations primarily concerning cybersecurity risk management and incident reporting.

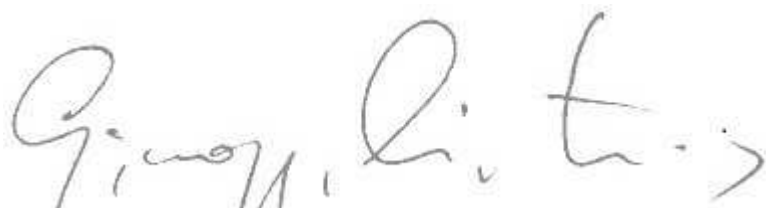
As part of our assessment, we have also reviewed the adequacy of the Listing Prospectus submitted to HKEX, with specific regard to the accuracy and completeness of the information provided on data protection compliance. Overall, the Prospectus presents a clear and well-structured overview of the Company's data protection framework, reflecting a diligent and transparent approach to privacy and regulatory matters. While some areas may require further intervention, the overall level of preparedness may be considered satisfactory. That said, it cannot be excluded that HKEX may request additional clarifications or further details regarding certain aspects of the information disclosed.

* * *

[THE REMAINDER OF THIS PAGE HAS BEEN INTENTIONALLY LEFT
BLANK]

We hope the above proves useful and remain at your disposal in case of need.

Kind regards,

A handwritten signature in dark ink, appearing to read "Giuseppe Cristiano". The signature is written in a cursive, flowing style with some loops and a trailing flourish.

Signed by Giuseppe Cristiano, Partner
On behalf of De Berti Jacchia Franchini Forlani