Data Privacy Policy

1. Introduction

This Data Privacy Policy, as amended from time to time (the **Data Policy**) is dated and effective as of 7 July 2021 (the **Effective Date**).

Screening Eagle Technologies AG, together with all its affiliates Screening Eagle Dreamlab Pte. Ltd., Screening Eagle Dreamlab S.L., Proceq AG, Proceq Rus Ltd., Proceq USA Inc., Proceq UK Ltd., Proceq Asia Pte Ltd., Proceq SAO Equipamentos de Medição Lta., and Proceq Trading (Shanghai) Co.,Ltd. (hereinafter **we, us, our**) are committed to protect and respect your data. In this Data Policy **you** may be a user of one or more of our services, platforms, cloud-based services, mobile applications and software made available by us to you in connection with any of our sensors or on a stand-alone basis (collectively our **Services**).

As a technology company specializing in the development of tools for data processing, we take the protection of your personal data seriously. For this reason, we would like to provide you with detailed information about the types of personal data we collect and process in connection with your use of any of our Services, to whom this personal data is transferred, and the rights you have in connection with the processing of this personal data. As an internationally oriented company based in Switzerland, we adhere to the data protection standards of the Swiss Federal Act on Data Protection (FADP) and the EU General Data Protection Regulation (GDPR).

Please read the following carefully to understand our views and practices regarding your personal and non-personal data and how we will treat it. You are not required to provide the personal information that we have requested, but, if you chose not to do so, in many cases we will not be able to provide you with our Services or respond to any queries you may have. By using our Services and/or registering for an account with us, you are accepting the terms of this Data Policy and consenting to our processing of your information as described herein. For the avoidance of doubt, "processing" may mean on a computer/handheld device or using or touching information in any way, including, but not limited to, collecting, storing, deleting, using, combining and disclosing information.

2. Applicability and Scope

2.1. This Data Policy together with any other terms provided by us applies to your use of all our Services unless a separate policy or legal document applies to a particular Service, in which

case that policy or legal document applies.

2.2. This Data Policy describes and sets out the basis for the collection, use, disclosure, storage retention and protection of the personal data you provide to us while using any of the Services, and applies to all personal data we collect through your use of our Services. We do not endorse, nor do we have influence on the content or policies of third-party services and therefore cannot assume any responsibility for them.

2.3. Before you disclose to us any personal data of another person (including employees and contractors) you must obtain that person's consent to both the disclosure and the processing of that personal data in accordance with this Data Policy.

3. Responsibilities

3.1 We act as provider of the Services and determine the purposes and means of the processing of your personal data. This means that we qualify as controller within the meaning of the GDPR.

3.2 As controller, we are committed to ensure that your privacy and personal data is protected and that your personal data is only used in accordance with this Data Policy. For any inquiries regarding our use of your personal data, you can contact us as follows:

- by post to the following address: Ringstrasse 2, 8603 Schwerzenbach, Switzerland;
- by telephone, on the contact number +41 43 355 38 00;
- by email, using the email address data.privacy@screeningeagle.com;
- using our website contact form.

4. Purposes of Use and Legal Basis for Processing

We only process your personal data if this is necessary to provide our Services. The processing of your personal data is only carried out on the following legal bases and purposes:

(a) Processing on the basis of your consent to the processing of your personal data (art. 6 (1) (a) GDPR);

(b) Perform our contractual obligations towards you, manage, administer, analyze, enable and improve usage of our Services and enhance their stability;

(c) Help us create, develop, operate, deliver, and improve our products, Services, content and advertising, and for loss prevention and anti-fraud purposes;

(d) For internal purposes such as auditing, data analysis, and research to improve our products, services, and customer communications;

(e) Processing for the performance of a contract to which you are party or in order to take

steps at your request prior to entering into a contract (art. 6 (1) (b) GDPR); or

(f) Processing for the purpose of legitimate interests pursued by us or third parties (art. 6 (1) (f) GDPR).

5. Storage, Retention and Deletion of Personal Data

5.1. Personal data that is collected and processed as described herein is stored by us on our own secure servers in Switzerland, in our secure facility server at Amazon Web Services (**AWS**) located in the EU (Frankfurt) which maintains the ISO 27018 certification (standard for protecting Personally Identifiable Information in the cloud) or as otherwise identified herein.

5.2. To the extent that you are a user of certain of our Services in the Republic of China, your personal data collected and processed as described herein, is stored by us on Alibaba Cloud- a server in Republic of China (the **Alibaba Cloud**). The Alibaba Cloud adheres to all domestic data security standards of the countries and regions where Alibaba Cloud services are deployed, is GDPR compliant, and its compliance program includes a comprehensive range of certifications and worldwide attestation reports. For more information please refer to https://www.alibabacloud.com/trust-center/compliance?spm=a3c0i.17650567.6791778070.dnavwhyc1.4e382ae3G8FM5F#J_5959942230

5.3. We will retain the data provided by you for as long as you use our Services and the performance of our contractual obligations as well as compliance obligations or other purposes pursued with the processing and for a reasonable time thereafter so long as it is necessary and relevant for our business operations and beyond this duration in accordance with legal retention and documentation obligations.

5.4. Notwithstanding other provisions of this Data Policy, we may retain documents (including electronic documents) containing personal data:

(a) to the extent that we are required to do so by law or to fulfil our contractual obligations towards you;

(b) if we believe that the documents may be relevant to any ongoing or prospective legal proceedings relevant to us; and

(c) in order to establish, exercise or defend our legal rights (including without limitation, collection of any fees owed, resolve disputes, troubleshoot problems, enforce this Data Policy and/or our terms of use or providing information to others for the purposes of fraud prevention and reducing credit risk.

5.5. After it is no longer necessary for us to retain your personal data, we dispose of it in a secure

manner according to our data retention and deletion policies. The personal data will also be deleted if a statutory storage period expires, unless there is a need for further storage of the data for the conclusion or performance of a contract.

6. Transfer of Personal Data

6.1. In the context of our business activities and in line with the purposes of the data processing set out herein, we may transfer your personal data to third parties, insofar as such a transfer is permitted and we deem it appropriate, in order for them to process data for us or, as the case may be, their own purposes. In particular, the following categories of recipients may be concerned:

(a) Affiliate companies of Screening Eagle Technologies AG;
(b) Service providers und subcontractors such as law firms, banks, insurance companies and cloud infrastructure providers;
(c) Business partners;
(d) Courts, authorities and arbitral tribunals.

6.2. Certain data recipients may be within Switzerland, but they may be located in any country worldwide. In particular, data may be transferred to countries, in which our clients, their affiliates, or business partners are located as well as countries in which service providers are located or where our clients and affiliate companies are involved in business. If we transfer data to a country without adequate legal data protection, we ensure an appropriate level of protection as legally required by way of using appropriate contracts or binding corporate rules or we rely on the statutory exceptions of consent, performance of contracts, the establishment, exercise or enforcement of legal claims, overriding public interests, published personal data or because it is necessary to protect the integrity of the persons concerned.

7. Disclosure of Personal Data

7.1. We may use and disclose your data as we deem necessary: (i) under applicable law, or payment method rules; (ii) to enforce any applicable terms of use or rights; (iii) to protect our rights, data, safety or property, and/or that of our affiliates, you or others; and (iv) to respond to requests from courts, law enforcement agencies, regulatory agencies, stock exchanges and other public and government authorities, which may include authorities outside your country of residence.

7.2. We do not disclose information about identifiable individuals to our advertisers, but we may provide them with anonymous aggregate information about our users and customers. We may

also use such aggregate information to help advertisers reach the kind of audience they want to target. We may make use of the data we have collected from you to enable us to comply with our advertisers' wishes by displaying their advertisement to that target audience.

7.3. We may disclose some or all of the data we collect from you when you download or use our Services to some third parties, including but not limited to mobile applications, websites and third-party integrations on or using our Services, partners or collaborators. Information collected by these third-party apps, websites or integrated services is subject to their own terms and policies.

7.4. We may disclose your data to any member of our group, affiliates which means our subsidiaries, our ultimate holding company and/or its subsidiaries.

7.5. We may disclose your data to third parties:

(a) in the event that we sell or buy any business or assets, in which case we may disclose your data to the prospective seller or buyer of such business or assets;

(b) if our company or substantially all of its assets are acquired by a third party, in which case personal data held by it about its customers will be one of the transferred assets;

(c) if we are under a duty to disclose or share your personal data in order to comply with any legal or regulatory obligation or request;

(d) with our trusted services providers who work on our behalf, do not have an independent use of the information we disclose to them, and have agreed to adhere to the rules set forth hereunder;

(e) when we believe in good faith that disclosure is necessary to protect our rights, property or safety of our customers or protect your safety or the safety of others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction, or respond to a government request, inter alia;

(f) in order to enforce or apply any applicable terms of use and other agreements or to investigate potential breaches.

8. Google Analytics

8.1 Our Services uses Google Analytics, a web analytics service provided by Google, Inc. (**Google**). All data collected by Google is transferred to servers located in the USA. To ensure an adequate level of protection, personal data is only transferred to Google on the basis of the European Commission’s standard contractual clauses for data transfers from controllers to processors outside the EU or EEA. We have further concluded a data processing agreement with Google and are therefore fully compliant with the requirements of the GDPR when using

Google Analytics.

8.2 Google Analytics is used to measure your engagement with certain of our Services such as mobile apps. This may include number of users, location and activities, types of mobile devices and iOS versions. With Google Analytics we don't track personal data and all online behavior is anonymized.

9. Firebase and Crashlytics

9.1. Some of our Services use Firebase and Crashlytics, mobile app analytics service provided by Google. All data collected by Google is transferred to servers located in the USA. To ensure an adequate level of protection, personal data is only transferred to Google on the basis of the European Commission's standard contractual clauses for data transfers from controllers to processors outside the EU or EEA. We have further concluded a data processing agreement with Google and are therefore fully compliant with the requirements of the GDPR when using Firebase.

9.2. Firebase and Crashlytics provides us insight on how you use our applications as well as a crash reporting, analytics and monitoring service. Data we collect may include information about mobile devices (model, iOS version, location, state), unique device identifiers, user activities in the app such as data synchronization, sharing and exports, which screens in the apps are used, QR code scanning, etc. Similar to other Google data collection services we may use, we get only anonymized data points that we use to improve the way our products give service to our customers. The processing of your personal information allows us to provide a more stable application, to offer a better user experience and to strengthen and improve our technical support. Since we have a legitimate interest in understanding how you use the application and provide you a stable application to provide a better user experience, Art. 6 (1) f) GDPR serves as the legal basis for processing your personal data.

10. OneSignal

In certain of our Services we may use OneSignal, Inc. (**OneSignal**) push notifications services to provide us with vendor identifiers data. By using their services, we may share with OneSignal certain data such as spot related information for instance spot number, date and user-name, as well as additional data to assist you, as a user of certain of our Services, to navigate through a particular displayed view of such Service, like unique user ID, notification topic, or project. Data collected through OneSignal when using our respective Services is

generally not personally identifiable information. For more information, please refer to https://onesignal.com/privacy_policy.

11. Hubspot

For our marketing activities and to enable us to send and manage email campaigns across channels and send our newsletters, we recur to the services of an online marketing platform operated by HubSpot, Inc., 25 First Street, 2nd Floor, Cambridge, MA 02141 USA (**Hubspot**). Personal data we may share with Hubspot are your e-mail address, name, company, phone, country and region. These data are transferred to their servers located: HubSpot's product infrastructure is hosted on Amazon Web Services (AWS) in the United States East region. HubSpot leverages the Google Cloud Platform (GCP) in the EU (Frankfurt, Germany region) to support the processing of local customer data that is critical to our customers' businesses. This includes leads, email events, and analytics. By hosting these services in both AWS in the USA and GCP in Germany, HubSpot has increased the performance and reliability of those services by locating them closer to end users in the EU. To ensure an adequate level of protection, personal data is only transferred to Hubspot on the basis of the European Commission's standard contractual clauses for data transfers from controllers to processors outside the EU or EEA. We have further concluded a data processing agreement with Hubspot and are thus compliant with data protection requirements, especially GDPR when using it. For more information please refer to https://legal.hubspot.com/privacy-policy.

12. SugarCRM

We use the CRM system provided by SugarCRM Inc., 10050 North Wolfe Road, SW2-130, Cupertino, CA 95014, USA (**SugarCRM**) in order to more quickly and efficiently process user inquiries and manage our customer relationship (legitimate interests in accordance with Article 6(1)(f) of the GDPR). Personal data we may share with SugarCRM are your e-mail address, name, company, phone, country and region. SugarCRM solely utilizes this data for the technical processing of inquiries and managing our customer relationship with you and does not pass this data on to third parties. Such data is stored in the SugarCRM cloud in Ireland. More information can be found in SugarCRM's privacy policy accessible under https://www.sugarcrm.com/legal/privacy-policy.

13. SMARKET

For certain of our marketing activities and to enable us to send and manage email campaigns, WeChat messages, short message services across channels and send our newsletters in the Republic of China, we recur to the services of SMARKET, an online marketing platform operated by SINObase Marketing Technology Corp. Shanghai Branch (**SINObase**), room 3051 of building A, No.128 Huayuan Road, Hongkou District, Shanghai, Republic of China. Personal data we may share with SINObase are your e-mail address, name, company, phone, job title, country and region. These data are transferred to their servers located at: SINObase's product infrastructure is hosted on Alibaba Cloud in Republic of China.

14. Your Rights as a Data Subject

14.1. If personal data concerning you are processed, you are a data subject within the meaning of the GDPR and you have the following rights:

(a) Right of access: You can ask us to confirm whether personal data concerning you is being processed by us. Is that the case, you can request the information as defined in art. 15 (1) GDPR from us. Further, you have the right to request information as to whether the personal data concerning you is transferred to a third country or to an international organization. In this context, you may request to be informed of the appropriate safeguards pursuant to art. 46 GDPR relating to the transfer.

(b) Right to rectification: You have the right to obtain from us the rectification and/or completion of incorrect or incomplete personal data concerning you. Your right to rectification may be restricted to the extent that it is likely to render the performance of research or statistical purposes impossible or seriously compromises it and the restriction is necessary for the performance of research or statistical purposes.

(c) Right to restriction of processing: In line with the conditions stated in art. 18 (1) GDPR, you have the right to request the restriction of processing of your personal data. Where processing of personal data concerning you has been restricted, such personal data may only be processed – with the exception of storage – with your consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of an important public interest of the European Union or a Member State.

(d) Right to erasure: You have the right to obtain from us the erasure of your personal data and we are obliged to erase personal data without undue delay where one of the grounds pursuant to art. 17 (1) GDPR apply. Please note that your right to erasure shall not apply

to the extent that a processing is necessary as stated in art. 17 (3) GDPR, this includes, amongst others the establishment, exercise or defence of legal claim.

(e) Right to information: If you have exercised your right of rectification, erasure or restriction of processing against us, we are obliged to notify all recipients to whom your personal data have been disclosed, unless this proves impossible or involves disproportionate effort. You have the right to obtain from us the information about those recipients.

(f) Right to data portability: You have the right to receive the personal data concerning you which you have provided to us in a structured, commonly used and machine-readable format. In addition, you have the right to transmit the data to another data controller without hindrance from us to which the personal data have been provided in line with art. 20 GDPR.

(g) Right to object: You have the right to object, on grounds relating to your particular situation, at any time to the processing of personal data concerning you which is based on art. 6 para. 1 lit. e or f GDPR, including profiling based on those provisions. We no longer process the personal data concerning you, unless we demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or for the establishment, exercise or defence of legal claims.

(h) Where personal data is processed for direct marketing purposes, you have the right to object at any time to processing of the personal data concerning you for such marketing, which includes profiling to the extent that it is related with such direct marketing. Where you object to processing for direct marketing purposes, the personal data concerning you will no longer be processed for such purposes.

(i) You have the possibility to exercise your right of object in the context with the use of information society services, and notwithstanding Directive 2002/58/EC, by automated means using technical specifications.

(j) Right to withdraw the consent to process personal data: You have the right to withdraw your consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

(k) Right to lodge a complaint with a supervisory authority: Without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence, place of work or place of the alleged infringement, if you consider that the processing of personal data concerning you infringes the GDPR or the Swiss Federal Act on Data Protection. In

Switzerland, the Federal Data Protection and Information Commissioner is the competent data protection authority.

15. Creation of a Screening Eagle ID

14.1 To get access to and make use of our Services, you are required to register and create a user account (**Screening Eagle ID**). To create a Screening Eagle ID, you will be asked to provide us with the following personal data (**Account Information**) relating to you: first name and last name; e-mail address; company name; phone number; username; region; and personal password.

14.2 The collection and processing of account data is carried out with the purpose of identifying you as the unique holder of the account and the Screening Eagle ID, enable features, prevent fraud, perform customer support, and to ensure that your personal data can only be viewed by you. To further enhance your security and the integrity of your personal data, we expressly reserve the right to collect additional reregistration information.

14.3 Since the collection of the personal data described here is necessary to fulfil our contractual obligations, the processing is based on Art. 6 (1) (b) GDPR.

16. Use of Account Information for Marketing Purposes

We may use the Account Information that is collected as described above to send you non-marketing commercial communications as well as marketing communications relating to our business or the businesses of carefully selected third parties which we think may be of interest to you. If you do not wish to receive any marketing information, you can unsubscribe from this service at any time.

17. Collection of Device and Location Information

17.1. Each time you use one of our Services, in particular any of our mobile software applications, and/or you log in with your Screening Eagle ID, we may automatically collect the following data about you and/or your device, or data that has been uploaded onto or stored in such applications, which may be linked to your Account Information in order to enable the use of such Services:

- technical information, including the type of device you use, a unique device identifier, your Screening Eagle ID, network information, your operating system, the type of browser you use, time zone setting, etc.;
- information stored in certain of our Services or on your device, including without limitation,

measurement data and signal related information, functions you use, type of measurement signals and displayed results, pictures, videos, notes, voice-notes, chat messages, photos, videos, comments and audio attachments, local mobile applications logs, processed data, generated reports, uploaded information, and time and geographic location of when you accessed to our Services;

- information obtained using inertial measurement technologies, visual computing tools, wireless networking signals (e.g. Wi-Fi), beacons, or other technologies and tools required for the use of some of our Services;
- details of your use of and interaction with any of our Services which may include, but is not limited to, traffic data, location data, and any crash data and logs, weblogs and other communication data, whether this is required for our own purposes or otherwise and the resources that you access or usage trends.

17.2. When you use one of our Services, we may also use a positioning technology system to determine your current location when accessing to or using any of our Services to enable the association of your location with certain of our Services' features and consequently use thereof. Some of our location-enabled Services require your personal data for the feature to work and may be linked to your Account Information, in particular your Screening Eagle ID. If you wish to use the particular feature, you will be asked to consent to your data being used for this purpose. You can withdraw your consent at any time by uninstalling our respective Service.

18. Non-Personal Data Ownership and Liability

18.1. When you use our Services, we may collect data in a form that does not, on its own, permit direct association with any specific individual. We may collect, use, transfer, and disclose non-personal data for any purpose. You retain the property rights in and to the data processed by us, uploaded, transmitted, stored or located in or provided to us by you while using or arising out of your use of our Services. You hereby grant us an irrevocable, perpetual and unconditional right to use, reproduce, distribute, or prepare derivative works based on any such non-personal data, on an anonymized way. You hereby agree that we shall keep at all times any and all right, title and interest in and to any such derivative works.

18.2. You shall be at all times fully responsible for all the data and content collected through, uploaded into, stored in or transmitted by means of our Services either by yourself or any third-

party using or with access to our Services, lawfully or unlawfully, based on your agreement with us.

19. Security

19.1. We are concerned about safeguarding the confidentiality of your information. We provide physical, electronic, and procedural safeguards to protect information we process and maintain. For example, we limit access to this information to authorized employees and contractors who need to know that information in order to operate, develop or improve our Services. Please be aware that, although we endeavor to provide reasonable security for information we process and maintain, no security system can prevent all potential security breaches.

19.2. We will take reasonable technical and organisational precautions to prevent and prevent the risk of loss, misuse or unauthorized access, disclosure and alteration of your personal data. The storage of your data on our servers is password- and firewall-protected and all electronic financial transactions entered through our Services will be protected by encryption technology.

19.3. You acknowledge that the transmission of information over the Internet is inherently insecure, and we cannot guarantee the security of data sent over the internet.

19.4. You are fully responsible for keeping and securing your access to our Services, including without limitation, keep the password you use for accessing any of our Services safe and confidential; we will not ask you for your password (except when you log in to certain of our Services).

19.5. Where we have given you (or where you have chosen) a password that enables you to access certain parts of our Services, you are responsible for keeping this password confidential.

19.6. Unfortunately, the transmission of information via the Internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to Services; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access, according to the Security section.

19.7. If you believe your account has been abused, please contact us immediately following the instructions in the Contact section below.

19.8. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Data Policy.

20. Third Parties Data Practices

17.1 Our Services may, from time to time, contain content, links to and from websites of our partner networks, advertisers and affiliates or unrelated third parties (including, but not limited to, websites on which our Services are advertised). We cannot guarantee the data or security of your information once you provide it to a third party and we do not accept any responsibility or liability for these policies or for any data that may be collected through these third-parties websites or services. We encourage you to evaluate the data and security policies of such third party before choosing to share your information.

17.2 In order to pay for certain of our Services we may use third-party partners or platforms according to their own terms and conditions. We disclaim any responsibility or liability for such third-parties' terms and conditions and the way they treat and process your data. Any payment transactions carried out by us or our chosen third-party provider of payment processing services will be encrypted.

17.3 This Data Policy addresses only the use and disclosure of information we collect, process from you or that has been provided by you while using our Services. If you disclose your information to others, or if you are directed to a third-party website, their particular policies and practices shall apply.

21. Minors

Our Services are not designed or intended for use by children under the age of eighteen (18). We do not knowingly collect any personal data on our Services from anyone under the age of eighteen (18) without the prior, verifiable consent of a parent or guardian. Such parent or guardian may have the right, upon request, to view the information provided by the child and require that it be deleted. Moreover, all minors should seek their parent's or guardian's permission prior to using or disclosing any personal data or online resource.

22. Export Controls

Some of our Services may be subject to the export laws of various countries including, without limitation, those of Switzerland, the EU and its member states, and of USA. You acknowledge that, pursuant to the applicable export laws, trade sanctions, and embargoes issued by these countries, we may be required to take measures to prevent entities, organizations, and parties listed on government-issued sanctioned-party lists from accessing certain products, technologies, and services through our Services or other delivery channels controlled by us. Our compliance may include (i) automated checks of any user registration data as set out herein and other information a user provides about his or her identity against applicable

sanctioned-party lists; (ii) regular repetition of such checks whenever a sanctioned-party list is updated or when a user updates his or her information; (iii) blocking of access to our Services in case of a potential match; and (iv) contacting a user to confirm his or her identity in case of a potential match.

23. California Privacy Disclosures

23.1. California consumers have a right to knowledge, access, and deletion of their personal data under the California Consumer Privacy Act. California consumers also have a right to opt out of the sale of their personal data by a business and a right not to be discriminated against for exercising one of their California privacy rights. We do not sell the personal data of California consumers and do not discriminate in response to privacy rights requests.

23.2. This Data Policy includes what personal data is collected, the source of the personal data, and the purposes of use, as well as whether we disclose that personal data and if so, the categories of third parties to whom it is disclosed.

24. Changes to the Data Policy

This Data Policy may be updated from time to time for any reason at our sole discretion. We will notify you of any changes to our Data Policy by posting the new Data Policy in our website and informing you when you next start using or log onto one of the Services. You are advised to consult our Data Policy regularly for any changes, as continued use is deemed approval of all changes. The new terms may be displayed on-screen and you may be required to read and accept them to continue your use of certain of the Services.

25. Translations

As an internationally company present in many different countries, we may make available certain translations of our Data Policy for your convenience only. The English version of this Data Policy shall be the legally binding and controlling version in all respects, and shall prevail in the event of any conflict, inconsistency or discrepancy between the English and any translated version of the Data Policy.