



## SCREENING EAGLE

### WEBSITE DATA PRIVACY POLICY

This Website Data Privacy Policy, as amended from time to time (the **Website Data Policy**) is dated and effective as of 6<sup>th</sup> December 2022 (the **Effective Date**).

#### A. Introduction

Screening Eagle Technologies AG, together with all its affiliates Screening Eagle Singapore Pte. Ltd., Screening Eagle Dreamlab S.L., Screening Eagle USA, Inc., Screening Eagle UK Ltd., Proceq AG, Proceq Rus 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 Website Data Policy **you** may be a visitor to the website <https://www.screeningeagle.com> including any of its subsites (the **Website**) or a user of one or more of our services, platforms, social media, forums or otherwise made available by us to you in connection with any of our instruments or on a stand-alone basis (our **Services**).

As a technology software 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 the Website or 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.

#### B. General Information

##### 1. Applicability and Scope

- 1.1 This Website Data Policy together with any other terms provided by us applies to your use of the Website or our Services unless a separate policy or legal document applies to a particular Service, in which case that policy or legal document applies.
- 1.2 This Website 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 the Website or 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.

- 1.3 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 Website Data Policy.

## **2. Responsibilities**

2.1 Screening Eagle Technologies AG acts as the operator of the Website and provider of the Services and determines the purposes and means of the processing of your personal data. This means that Screening Eagle Technologies AG qualifies as controller within the meaning of the GDPR.

2.2 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 Website 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](mailto:data.privacy@screeningeagle.com);
- using our Website contact form.

## **3. Purposes of Use and Legal Basis for Processing**

We only process your personal data if this is necessary to provide a functional Website and 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).

## **4. Storage, Retention and Deletion of Personal Data**

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

4.2 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.

- 4.3 Notwithstanding other provisions of this Website 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 Website Data Policy and/or our terms of use or providing information to others for the purposes of fraud prevention and reducing credit risk.
- 4.4 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.

## **5. Transfer of Personal Data**

- 5.1 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.
- 5.2 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 affiliates, 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.

## **6. Disclosure of Personal Data**

- 6.1 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; (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.

- 6.2 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.
- 6.3 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.
- 6.4 We may disclose your data to any member of our group, affiliates which means our subsidiaries, our ultimate holding company and/or its subsidiaries.
- 6.5 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.

## **7. Your Rights as a Data Subject**

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

- 7.1 **Right of access:** You can ask us to confirm whether personal data concerning you is being processed by us. If that is 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.
- 7.2 **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.

- 7.3 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.
- 7.4 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.
- 7.5 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.
- 7.6 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.
- 7.7 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.
- 7.8 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.
- 7.9 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.
- 7.10 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.
- 7.11 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.

## **C. Individual Processing Activities Related to the Use of the Website**

### **1. Provisions of the Website and Creation of Logfiles**

1.1 Every time you visit our Website, our system automatically collects data and information from the computer system of the calling computer that may qualify as personal data under the GDPR. The following data may be collected:

- Type of device that is used for access, including a unique device identifier;
- Browser type and version;
- Operating system;
- Internet Service Provider;
- IP address;
- Date and time of access;
- Websites from which your system reaches our Website;
- Websites accessed by your system via our Website;

The data may be also temporarily stored in the log files of our system but is not stored together with other personal data concerning you.

1.2 The temporary storage of your IP address by the system is necessary to enable the Website to be delivered to your computer. For this the IP address must remain stored for the duration of the session. The remaining data that as mentioned above serves us to optimize the website and to ensure the security of our information technology systems. The data is not evaluated for marketing purposes in this context. Since we have a legitimate interest in providing a functional website to you, Art. 6 (1) f) GDPR serves as the legal basis for processing your personal data.

1.3 Your personal data will be deleted as soon as it is no longer necessary to achieve the purpose for which it was collected. In the case of the collection of data for the provision of the website, the data will be deleted when the respective session has ended. If personal data is stored in log files, it will be deleted after seven days.

1.4 The collection of personal data for the provision of the Website and the storage of personal data in log files is necessary for the operation of the Website. Consequently, there is no possibility of objection.

### **2. Subscription to Newsletter**

2.1 On our Website you have the possibility to subscribe to a free newsletter. Our newsletter primarily contains information about our products and promotions, such as competitions or discount campaigns, as well as evaluation requests.

2.2 When registering for the newsletter, the following personal data from the input mask will be transmitted to us:

- Email address;
  - First name and last name;
  - Company name;
  - Main interests (industry/vertical).
- 2.3 The collection of your e-mail address is required to deliver the newsletter. The remaining personal data is collected in order to personalize the newsletter and prevent misuse of the services or the email address that is used. The personal data will be used exclusively for sending the newsletter and will be stored for as long as the newsletter subscription is active.
- 2.4 For the processing of your personal data, your consent will be obtained during the registration process in accordance with Art. 6 (1) (a) GDPR and reference will be made to this data protection declaration. The consent is based on a double opt-in procedure. This means that after registration you will receive an email asking you to confirm your registration. This confirmation is necessary to ensure that nobody registers with a third-party e-mail address. The registrations for the newsletter are logged to prove the registration process according to legal requirements. This includes the storage of the time of registration and confirmation as well as the IP address used by your system.
- 2.5 The subscription to our newsletter can be cancelled at any time by using the link in our newsletter. When you cancel your subscription, your consent to the processing of your personal data as described in this clause is automatically revoked.

### **3. Communication by Email or Contact Form**

- 3.1 The contact form on our Website can be used for electronic contact. If you use the contact form, the following personal data will be transmitted to us:
- E-mail address;
  - First name and last name;
  - Company name
  - Phone number;
  - IP address
  - Country/State.
- 3.2 The collection of your e-mail address allows us to contact you to process your contact request. The remaining personal data is collected to prevent misuse of the contact form. As an alternative to using the contact form, it is also possible to contact us via the e-mail address [contact@screeningeagle.com](mailto:contact@screeningeagle.com). In this case, in addition to your e-mail address, all personal data transmitted with the e-mail will be processed and stored. The data transmitted to us is used exclusively for processing your contact. The data will not be passed on to third parties or automatically registered for our newsletter.
- 3.3 If you contact us via the contact form or by email, we may keep a record of that correspondence. The personal data transmitted to us from the input mask and by email is deleted as soon as the data is no longer required for the purpose of collection. This is the case after ten (10) years at the latest, unless we are legally and contractually bound by longer storage obligations.

#### 4. Events

If you register for an event, seminar, or webinar provided by us, we may share basic participant information (typically your name, company, title, and email address) with other participants of the same event, seminar, or webinar for the purpose of communication and the exchange of ideas with your consent. 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.

#### 5. Employment Application

If you apply for a job (e.g via our Website or social media), we may require you to submit additional personal information as well as a resume or curriculum vitae and other information. We encourage you to limit the personal data to the information necessary to enable us to evaluate your suitability for the position you are applying for. Personal data relating to employment applications will be deleted as soon as the data is no longer required for the purpose of collection or no legal basis exists.

#### 6. 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. 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 US 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 <https://legal.hubspot.com/privacy-policy>.

#### 7. 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>.

## 8. Google Analytics

- 8.1 Our Website 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 uses cookies that collect the following information about your use of the Website:
- The IP address of the system you are using;
  - The website from which you have reached our Website (referrer);
  - The individual pages you call up;
  - The time spent on the website and individual pages;
  - The frequency of the call of a site and individual pages;
  - The country, region or city from where access is made.
- 8.3 The information above will be transferred to and stored by Google on servers in the United States. Before the transfer this information will be anonymized by removing the last octet of your IP address. Google will process this information on our behalf for the purpose of evaluating your use of the Website, compiling reports on Websites activity and providing other services relating to Websites activity and internet usage. Google will not link your IP address with any other data held by Google.
- 8.4 You may object to the use of cookies by selecting the appropriate settings on your browser. However, please note that if you do this you may not be able to use the full functionality of this Websites. You may further opt-out of the collection of your usage data (including your IP-address) and the processing of the data by Google by downloading and installing the add-on for your current web browser from the following link: <https://tools.google.com/dlpage/gaoptout>.
- 8.5 Google Analytics is also used to measure your engagement with our Website and 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. Hotjar

- 9.1 Our Website uses the Hotjar web analytics service provided by Hotjar Ltd., a company incorporated in Malta (**Hotjar**). We have concluded a data processing agreement with Hotjar and are therefore fully compliant with the requirements of the GDPR when using Hotjar.
- 9.2 Hotjar uses cookies that collect the following information about your use of the Website:

- The IP address of the system you are using;
- The website from which you have reached our Website (referrer);
- The individual pages you call up;
- The time spent on the Website and individual pages;
- The frequency of the call of a site and individual pages;
- The country, region or city from where access is made.

9.3 We use Hotjar to understand the Website usability and user experience through anonymized sample tracking of Website visits. Hotjar stores the collected personal data in a pseudonymized user profile. The information will not be used by Hotjar or by us to identify individual users, nor will it be combined with other data about individual users.

9.4 You may object to Hotjar storing a user profile and information about your visit to our website by clicking on the appropriate button on this website: <https://www.hotjar.com/legal/compliance/opt-out>. For more information about Hotjar handling of personal data, please see Hotjar's privacy policy: <https://www.hotjar.com/legal/policies/privacy>.

## 10. Google Tag Manager

10.1 Our Website uses the Google Tag Manager, a service that allows website tags to be managed through an interface. The Google Tag Manager only implements tags. This means that no cookies are used, and no personal data is collected. The Google Tag Manager triggers other tags, which in turn collect data if necessary. However, the Google Tag Manager does not access this data.

10.2 If a deactivation has been made at domain or cookie level, it remains valid for all tracking tags if they are implemented with the Google Tag Manager.

## 11. Facebook Custom Audiences

11.1 Our Website uses the remarketing function "Custom Audiences" of Facebook Inc. (**Facebook**). All data collected by Facebook is transferred to servers located in the USA. To ensure an adequate level of protection, personal data is only transferred to Facebook on the basis of the European Commission's standard contractual clauses for data transfers to processors outside the EU or EEA. We have further concluded a data processing agreement with Facebook and are therefore fully compliant with the requirements of the GDPR when using Custom Audiences.

11.2 To use the Custom Audiences function, we have integrated the so-called Facebook pixel into our Website. The Facebook pixel is a piece of code that communicates with Facebook and enables us to optimize our advertising campaigns. With the help of the Facebook pixel, Facebook is able to show you interest-based advertisements (Facebook ads) when visiting the social network Facebook or other websites that also use this tool. The Facebook pixel further enables us to ensure that our Facebook ads correspond to the potential interest of the users. By showing us whether users have been redirected to our Website after clicking on a Facebook ad (conversion), the Facebook pixel further allows us to track the effectiveness of our Facebook ads for statistical purposes.

- 11.3 The Facebook pixel is integrated directly by Facebook when you call up our Websites and can store a cookie on your device, provided that you have agreed to the Cookiebot setting. If you subsequently log in to Facebook or visit Facebook when logged in, the visit to our online offer will be noted in your Facebook profile. The data collected about you is anonymous to us, so we cannot draw any conclusions about the identity of the user. However, the data is stored and processed by Facebook so that a connection to the respective user profile is possible and can be used by Facebook as well as for our own market research and advertising purposes. If we should transmit data to Facebook for comparison purposes, this data is encrypted locally in the browser and only then sent to Facebook via a secure connection. This is done solely for the purpose of comparison with the data encrypted by Facebook.
- 11.4 The “Custom Audiences” function can be deactivated for this Website and other websites at <https://www.facebook.com/settings/?tab=ads#>. To do this, you must be logged in to Facebook. The “Custom Audiences” function can also be deactivated for this Website by withdrawing your consent to the setting of marketing cookies under [https://www.facebook.com/ads/preferences/?entry\\_product=ad\\_settings\\_screen](https://www.facebook.com/ads/preferences/?entry_product=ad_settings_screen)

## 12. LinkedIn Plug-in

- 12.1 The LinkedIn button of LinkedIn Corporation, 1000 W Maude, Sunnyvale, California 94085, USA, (**LinkedIn**) may be integrated on certain web pages of our Website (**LinkedIn Plug-in**). When you call up a page of our Website that contains such a LinkedIn Plug-In, your browser establishes a direct connection to the servers of LinkedIn. The content of the LinkedIn Plug-in is transmitted directly to your browser and integrated into the page. Through this integration, LinkedIn receives the information that your browser has called up the corresponding page of our Website, even if you do not have a profile on LinkedIn or are not currently logged in. This information (including your IP address) is transmitted by your browser directly to a server of LinkedIn, which may be located in the USA, and stored there.
- 12.2 If you are logged in to LinkedIn, your visit to our Website can be directly assigned to your profile on LinkedIn. If you interact with LinkedIn Plug-in's, for example by clicking the LinkedIn button, this information is also transmitted directly to a server of the platform operator and stored there. If you wish to prevent this, please log out of your LinkedIn or other social media accounts before visiting our Website. We have no influence on the data that LinkedIn collects on the basis of their LinkedIn Plug-ins. The purpose and scope of the data collection and the further processing and use of the data by LinkedIn as well as your rights and settings options in this regard to protect your privacy, can be found in the data protection notices of LinkedIn, see here: [https://www.linkedin.com/legal/privacy-policy?trk=homepage-basic\\_footer-privacy-policy](https://www.linkedin.com/legal/privacy-policy?trk=homepage-basic_footer-privacy-policy) and here: <https://www.linkedin.com/help/linkedin/answer/50986/social-plugin-data?lang=en>.
- 12.3 In order to increase the protection of your data when visiting our Website, the LinkedIn-Plug-ins are not integrated into the page without restriction, but only using an HTML link (so-called "Shariff solution" from c't). This integration ensures that when you call up a page of our Website that contains such plugins, no connection is established with the servers of the provider of LinkedIn. If you click on one of the buttons, a new window of your browser opens and calls up the page of the respective service provider on which you can (if necessary after entering your login data) e.g. click on the Like or Share button. The purpose and scope of the data collection and the further processing and use of the data by the providers on their

pages as well as your rights in this regard and setting options for protecting your privacy can be found in the data protection notices of the respective providers.

- 12.4 In addition, you can completely prevent the loading of the LinkedIn Plug-ins with add-ons for your browser, such as the script blocker "NoScript", which can be downloaded at <https://noscript.net>.

### 13. Cookies

If you use our Websites, we may use various website navigation information including tracking technologies such as cookies and web beacons to collect and store information from you, according to the Cookie Declaration on our Website. To learn more about it, please visit <https://www.screeningeagle.com/cookie-declaration>.

### 14. Lead Forensics

- 14.1 We use IP Tracking technology to identify businesses visiting our Websites and the pages they visit. Lead Forensics cannot identify the individual visiting the websites, only the company, and provide us with information readily available in the public domain, including the visiting company's contact information.
- 14.2 Lead Forensics provides a mixture of business data and personal data. When our Website gets a visit, the Lead Forensics software tracks the active business IP address and matches it to further business details that lead forensics holds on their database, providing publicly available details such as business name and address, telephone number and email addresses of key decision makers. However, identifiable individual email addresses and employee names fall under personal data. As the software identifies the business visitor (as opposed to the individual visitor) through tracking a company IP, we are able use the data Lead Forensics provides for B2B marketing purposes processed under the grounds of legitimate interest. More information can be found on <http://www.leadforensics.com>.

## D. Individual Processing Activities Related to the Use of some Services

### 1. Creation of a Screening Eagle ID

- 1.1 To get access to and make use some 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;
  - Email address;
  - Company name;
  - Phone number;
  - Username
  - Region;
  - Personal password.

- 1.2 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, enables 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.
- 1.3 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.

## **2. 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.

## **3. Collection of Device and Location Information**

- 3.1 Each time you use certain of our Services and/or you log in with your Screening Eagle ID, we may automatically collect the following personal data about you and your device 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 and signal related information, functions you use, type of measurement signals and displayed results, pictures, videos, notes, voice-notes, chats, photos, videos, comments, audio attachments, 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.
- 3.2 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.

#### **4. Non-Personal Data Ownership and Liability**

- 4.1 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.
- 4.2 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.

#### **E. Miscellaneous**

##### **1. Security**

- 1.1 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.
- 1.2 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.
- 1.3 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.
- 1.4 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).
- 1.5 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.
- 1.6 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.

- 1.7 If you believe your account has been abused, please contact us immediately following the instructions in the Contact section below.
- 1.8 We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Website Data Policy.

## **2. Internet and Social Networking**

- 2.1 Personal information that you publish, share or submit for publication in our Website, social media channels may be available, via the Internet, around the world. We cannot prevent the use or misuse of such information by others and hereby disclaim any responsibility thereon.
- 2.2 Certain Services include social networking, chat room or forum features. You shall ensure when using these features that you do not submit any personal data that you do not want to be seen, collected or used by other users.

## **3. Third Parties Data Practices**

- 3.1. Our Website and 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.
- 3.2. 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.
- 3.3. This Website 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.

## **4. Do Not Track Signals**

Unless otherwise stated herein, we do not track our Website users over time or across third party websites to provide targeted advertising and therefore do not respond to Do Not Track (DNT) signals.

## **5. 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.

## **6. California Privacy Disclosures**

- 6.1 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.
- 6.2 This Website 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.

## **7. 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.

## **8. Changes to the Website Data Policy**

This Website 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 Website Data Policy by posting the new Website 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 Website 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.