Privacy Policy

1. Introduction

1.1. Your privacy is important to us. This privacy policy provides you with information regarding the processing of your personal information when you make contact with us or use one of our services.

1.2. This privacy policy is provided per the General Data Protection Regulation 2016/679 ("**GDPR**") and any EU national laws implementing or supplementing the same (the "**Data Privacy Laws**").

2. About us and our privacy commitment

2.1. The iCOVER Group ("**iCOVER**" or "**We**"), specialized in international verification services under the brands "iCOVER" and "Square Facts", is headquartered in France and operates through several legal entities around the world to provide its clients background screening, due diligence, and compliance services ("**Services**") through a Service Agreement or Terms of Services agreed upon between iCOVER and you ("**Service Agreement**").

2.2. We are firmly committed to respecting your right to privacy and take seriously our responsibilities concerning the processing of personal information. We do not collect or process personal information unnecessarily nor solicit or receive information from children.

2.3. The privacy policy (the "**Policy**") sets out important information about your rights concerning the processing of your personal information in the course of using our services. The Policy also outlines the basis on which any personal information, we collect from you or that you provide to us, will be processed in connection with your use of our services.

2.4. If you have any questions about this Privacy Policy or want to exercise your rights set out in this Privacy Policy, please contact us by sending an email to privacy@icover-services.com

3. What information do we collect?

3.1. The Policy is primarily related to personal information collected and processed in order to operate our business.

3.2. We may collect personal information from you in the course of our business, including through your use of our website, when you contact or request information from us, when you engage our team to provide Services.

3.3. We collect information such as name and contact details in order to communicate and facilitate the provision of our services with our clients, potential clients, or suppliers. Initial information about you can be provided by the company you are working for. You may provide us with information by using our services or by corresponding with us by phone, e-mail, or otherwise. Other occasions during which you provide us information are when searching for a product, placing an order, reporting a problem, or engaging with any other form of communication with us. We may collect information to respond to inquiries regarding our products and services or to provide you with information, reports, or updates.

3.4. When you visit our website or use our platforms, we may collect, as a data controller, information about your visit such as your IP address, login information, browser type, time zone setting and the pages you visited and, when you use our Services we may collect

information on how you use those services. Our websites and online platforms may use cookies from time to time. Cookies may be used to save your personal preferences so you do not have to re-enter them each time you access our services. For more information about our use of cookies and how you can disable them, please see our Cookie Policy.

3.5. In the course of providing our Services to our clients, they engage us on a wide range of matters to help them mitigate risk such as conducting due diligence on a potential partner, employee, or client through reports.

3.5.1. The personal information we process in the performance of Services for and on behalf of our clients, as a data processor, includes but is not limited to any information relating to an identified or identifiable individual ("**Data Subject**"), for example, the individual's name, contact information, education information, work history, directorships, financial information, as well as, where necessary, data concerning criminal convictions and offenses. We treat all such information within the strict confines of the GDPR.

3.5.2. The lawful bases for such data processing are defined by our client in their privacy policy or another document and will vary depending on the nature of the information and the project. Before ordering, iCOVER's client has assessed the necessity, permissibility, and relevance of the service. iCOVER's client warrants to iCOVER that: (1) the personal data is processed in a lawful, fair, and transparent manner in relation to the data subject; (2) the personal data is collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; (3) the personal data is adequate, relevant, and limited to what is necessary for the purposes for which it is processed; and (4) if applicable after seeking appropriate legal advice, information notice or authorization form or any other mandatory document, has been duly provided to/required from the data subject.

3.5.3. iCOVER warrants the legality of the access to the information expected to be verified and defines the scope. iCOVER does not guarantee compliant use of the data in this report by the client. iCOVER has used its professional care and diligence to verify information against authorized public and/or private sources. iCOVER cannot be held responsible for the content provided by the sources. iCOVER cannot certify that no change has occurred since the preparation of the report.

4. What do we do with your information?

4.1. We will only process personal information when the law allows us to.

4.2. We may use your information for the following purposes: Fulfilment of Services, Client services, Business administration, and legal compliance or Recruitment:

4.2.1. Where we process your personal information to register you as a customer/user, accept your orders, deliver Services to you, collect our fees; we do so on the basis that it is necessary to perform our obligations under a contract with you or a company you work for. It may also be necessary to comply with certain legal obligations.

4.2.2. Where we process your personal information to send you newsletters, respond to your questions, improve the contents of our website and marketing efforts, conduct research and analysis, and display content based on your interests; we do so on the basis that it is necessary for our legitimate business interests. These interests include the interests of ensuring our clients receive premium service, growing our business to best satisfy changing market needs, and ensuring continual improvements to our Services.

4.2.3. Where we process your personal information for business administration and legal compliance, we comply with our legal obligations (including Know Your Client and Anti-Money Laundering or similar obligations), to enforce our legal rights, in connection with a business transaction; we do so on the basis that we have a legal obligation to do so.

4.2.4. Where we process your personal information for recruitment purposes to assess your suitability for any position for which you may apply at iCOVER whether such application has been received by us online, via email, or by hard copy or an in-person application; we do so in connection with us taking steps at your request to enter a contract we may have with you or it is in our legitimate interest to use personal information in such a way to ensure that we can make the best recruitment decisions for iCOVER. We will not process any special category data except where we can do so under applicable legislation. You may request at any point of the recruitment process iCOVER's background screening policy.

4.3. We will only use your personal information for the purposes for which we collected it unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your personal information without your knowledge or consent, in compliance with this Policy, where this is required or permitted by law.

5. Disclosure of your information

5.1. We only share your personal information with your consent or following this Policy. We will not otherwise share, sell or distribute any of the information you provide to us except as described in this notice.

5.2. We may disclose information to any department or authorized person within our company or any affiliated company within iCOVER and selected third parties only in the circumstances where it is necessary and the supplier has agreed to the same standards and terms of privacy as set out in the Policy.

5.3. iCOVER is a global corporation and any information that we collect or that you provide to us may be shared and processed by any iCOVER entity and affiliated. You can find out more about the iCOVER entities and locations in Appendix 1.

5.4. We may also share personal information with a variety of the following categories of third parties as necessary:

5.4.1. Professional advisers such as lawyers and accountants.

5.4.2. Government or regulatory authorities.

5.4.3. Professional indemnity or other relevant insurers.

5.4.4. Regulators/tax authorities/corporate registries.

5.4.5. Third parties to whom we outsource certain services such as, without limitation, translation services, confidential waste disposal.

5.4.6. Third parties engaged in the course of the services we provide to clients such as information furnishers.

5.4.7. Third party service providers to assist us with client insight analytics, such as Google Analytics.

5.5. A list is provided in Appendix 1, there may be other examples where we need to share with other parties in order to provide the Services as effectively as we can.

5.6. We will disclose your personal information to third-party recipients in the event that we sell or buy any business or assets, in which case we will disclose your personal information to the prospective seller or buyer of our business or assets or if we are under a duty to disclose or share your personal information in order to comply with any law, legal obligation or court order, or in order to enforce rights under the GDPR or to apply our Terms of Use and other agreements.

6. International transfers

6.1. In order to provide the Services we may need to transfer your personal information to locations outside the jurisdiction in which you provide it.

6.2. If you are based within the European Economic Area (EEA), please note that where necessary to deliver the Services we will transfer personal information to countries outside the EEA (including the United States, Mexico, Tunisia, and India).

6.3. All iCOVER entities have signed a data sharing agreement which is based on the EU standard contractual clauses to ensure we will comply with our legal and regulatory obligations in relation to personal information, including having a lawful basis for transferring personal information and putting appropriate safeguards in place to ensure an adequate level of protection for the personal information.

7. How long we keep your personal information?

7.1. We will only retain your personal information for as long as necessary to fulfill the purposes we collected it for, including to satisfy any legal, accounting, or reporting requirements. The period for which we store your personal information may depend on the type of information we hold.

7.2. To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of your personal information, the purposes for which we process your personal information, and whether we can achieve those purposes through other means, and the applicable legal requirements. For example, we may hold personal data as needed for our accounting or tax compliance purposes or where needed for our compliance with anti-money laundering regulations per the respective statutory periods.

7.3. For Data Subjects, we store their personal information for as long as the data controller (our client) has instructed us to in the Service Agreement.

8. Security measures

8.1. We use accepted standards of physical and technical measures and require our hosting partners to use the same standard of care to protect personal information. Despite our best effort to protect personal information, the transmission of information via the internet is not completely secure. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorized access.

8.2. You will find an excerpt of our security measures in Appendix 2.

9. Your rights

9.1. You have the following rights in relation to the personal information we hold about you:

9.1.1. Your right of access: If you ask us, we'll confirm whether we're processing your personal information and, if necessary, provide you with a copy of that personal information (along with specific other details). If you require additional copies, we may charge a reasonable fee.

9.1.2. Your right to rectification: If the personal information we hold about you is inaccurate or incomplete, you are entitled to request to have it rectified. If you are entitled to rectification and if we've shared your personal information with others, we'll let them know about the rectification where possible. If you ask us, where possible and lawful to do so, we'll also tell you who we've shared your personal information with so that you can contact them directly.

9.1.3. Your right to erasure: You can ask us to delete or remove your personal information in some circumstances such as where we no longer need it or if you withdraw your consent (where applicable). If you are entitled to erasure and if we've shared your personal information with others, we'll let them know about the erasure where possible. If you ask us, where it is possible and lawful for us to do so, we'll also tell you who we've shared your personal information with so that you can contact them directly.

9.1.4. Your right to restrict processing: You can ask us to 'block' or suppress the processing of your personal information in certain circumstances, such as where you contest the accuracy of that personal information or you object to us. If you are entitled to restriction and if we've shared your personal information with others, we'll let them know about the restriction where we can do so. If you ask us, where it is possible and

lawful for us to do so, we'll also tell you who we've shared your personal information with so that you can contact them directly.

9.1.5. Your right to data portability: You have the right, in certain circumstances, to obtain personal information you've provided us with (in a structured, commonly used, and machine-readable format) and to reuse it elsewhere or to ask us to transfer this to a third party of your choice.

9.1.6. Your right to object: You can ask us to stop processing your personal information, and we will do so if we are: (i) relying on our own or someone else's legitimate interests to process your personal information, except if we can demonstrate compelling legal grounds for the processing; or (ii) processing your personal information for direct marketing purposes.

9.1.7. Your right to withdraw consent: If we rely on your consent (or explicit consent) as our legal basis for processing your personal information, you have the right to withdraw that consent at any time.

9.1.8. Your right to complain with the supervisory authority: If you have a concern about any aspect of our privacy practices, including the way we've handled your personal information, you can report it to the relevant Supervisory Authority.

9.2. Please note that some of these rights may be limited where we have an overriding interest or legal obligation to continue to process the data.

10. Third-party material

10.1. The website and/or Services may contain links to other sites whose information practices may be different than ours. Visitors should consult the other sites' privacy notices as iCOVER has no control over information that is submitted to, or collected by these third parties.

11. Changes to this policy

11.1. Any changes made to this Policy from time to time will be published on the Platform. Any material or other change to the data processing operations described in this Policy that is relevant to or impacts on you or your personal data will be notified to you. In this way, you will have an opportunity to consider the nature and impact of the change and exercise your rights under the GDPR in relation to that change (e.g., to withdraw consent or to object to the processing) as you see fit.

12. Contact

12.1. If you have any comments or questions about our privacy policy or our processing of your information, please contact iCOVER - Data Protection Office – 1rue de la Bourse, 75002 Paris or privacy@icover-services.com.

12.2. For further information on the protection of personal data, you can consult the website of the Commission Informatique et Liberté, www.cnil.fr.

Effective date: 1 May 2023

Appendix 1 – List of sub-processors that may have access to your personal data

• (BULGARIA) ICOVER SERVICES EOOD • (MEXICO) I-COVER SCREENING MX SA DE CV • (INDIA) ICOVER INDIA INFORMATION AND SERVICES PRIVATE LIMITED • (SWITZERLAND) I COVER SWITZERLAND SARL • (TUNISIA) ICOVER SARL • (UNITED STATES) ICOVER INC. • (UNITED KINGDOM) I-COVER (SCREENING) LIMITED • (FRANCE) SQUARE FACTS SAS • (BULGARIA) SQUARE FACTS • (MOROCCO) SQUARE FACTS SARL
• Microsoft (Working tool) • Google workspace (Working tool) • Zoom (Communication platform) • Atlassian (Jira, Confluence) • Eurecia (HR services) • Figma (Working tool) • Monday.com (Working tool) • Adobe (Working tool) • Amazon webservice (hosting system) • OVH (hosting system) • Hetzner (hosting system) • Online.net (hosting system) • Slack (Communication platform) • Zoho (Customer management)

Privacy Policy

Appendix 2 – Security measures

- ISO 27001 certified Information Security Program. iCOVER has developed and implemented a comprehensive security program that includes reasonable administrative, technical, and physical safeguards, which are reasonably designed to protect: the security and confidentiality of Personal Data; against unauthorized access to or use of Personal Data.
- Procedures and Controls. iCOVER has developed, documented, and will maintain procedures and controls: for the secure handling, transfer, and disposal of Personal Data, whether in electronic or physical form; to protect against destruction, loss, or damage of Personal Data due to human error, potential environmental hazards, or technological failures; to restrict access to Personal Data at physical locations, such as buildings, computer facilities, and records storage facilities; to authenticate and limit access to its systems to authorized individuals; for the secure configuration and maintenance of information systems (e.g., servers, network infrastructure devices, and networks), including procedures for change management; the pseudonymization and encryption of Controller Data; for detecting, preventing and responding to attacks, intrusions, or other systems failures, including actions to be taken in the event of suspected or detected unauthorized access to its systems.
- Safeguards. iCOVER has designed and implemented reasonable safeguards to control reasonably foreseeable internal and external risks to its systems by restricting access to those who have a business need to access various systems, via control of administrative and user account privileges.
- Monitoring. iCOVER monitors security within its organization by: Using enterprise-grade automated tools to monitor workstations, laptops, and servers for malware, with central compilation of such logging; Leveraging firewalls and intrusion prevention systems to monitor externally facing assets; Collecting and analyzing audit logs of events and

generated alerts, to help detect an attack; performing penetration testing on an annual basis.

- Access. iCOVER manages and controls system access by: using Active Directory to control administrative privileges for Windows servers and some applications; restricting user account privileges to what is necessary in order to do their job.
- Disaster Recovery/Business Continuity and Incident Response Plans. iCOVER has designed plans for responding to a: disaster, including processes and procedures for resuming business operations; network and/or system attack, including incident handling.