September, 2025

Online Privacy Policy, Terms of Use and End User License Agreement (EULA)

This Online Privacy Policy ("Policy") is a continued part of SocioCultural Research Consultants, LLC ("SCRC")'s Terms of Use to which You and SCRC have agreed will apply to Your use of the Software ("The App") and constitutes a continued part of Your agreement with SCRC. In this Policy, "we," "us," and "our" refers to SCRC.

This Policy includes rules and protections for your personal and application data.

Recitals:

WHEREAS, the Parties understand that The App is solely owned by SCRC;

WHEREAS, You desire to use The App in connection with research;

WHEREAS, SCRC desires compensation in return for providing The App to You for research services via The App; and

WHEREAS, the Parties understand and agree that The App is and shall continue to be sole and proprietary intellectual property of SCRC.

NOW, BASED ON THE FOREGOING, the Parties agree to the following terms and conditions:

1. Definitions.

"Software;" the "De-ID App;" website at https://de-idapp.com and/or SCRC's software and/or to SCRC's software as a service (SaaS) ("The App"). "You;" "Your;" and "User" herein refers to the individual accessing or using the "Software" or "The App" as described above, and the company, organization, or entity on whose behalf You purport to use the Software, and each of them. You and SCRC are collectively referred to as "Party" or "Parties" collectively. "We," "Us," and "Our" refers to SCRC.

"PII" and/or "Personal Identifiable Information" refers to information such as Your email address, phone number, and name that is collected for the purposes of creating and maintaining an account with SCRC.

"Project Data" and/or "Your data" refers to data You upload via The App for the purposes of Your project.

2. Agreement and Counterparts.

You fully acknowledge that You have read, understand and agree to the following counterparts which are incorporated herein by reference: (i) ONLINE PRIVACY POLICY; and (ii) TERMS OF USE, END USER LICENSE AGREEMENT, DISCLAIMER, AND RELEASE OF LIABILITY.

3. SCRC Intellectual Property Statement.

SCRC respects the intellectual property of others and requires its users to do the same. SCRC may, in its sole and absolute discretion, disable and/or terminate the accounts of users who may be infringing the intellectual property rights of others.

4. Retroactivity.

You agree that this Agreement is and will be effective retroactively to the date You first used the Software.

5. Notices Regarding Changes to This Agreement.

You fully understand and agree that, with notice to You by email, mail, or posted notice. This Agreement can be subject to periodic change thereby. Posted notice is and will be made online at < https://de-id.zendesk.com/hc/en-us/articles/39537148987917-Terms-of-Service >. The earliest retroactive date for legacy Users will apply as early as December 1, 2006.

6. Inform Us of Infringement.

If You believe that Your work has been copied in a way that constitutes copyright infringement, or if You believe that Your intellectual property rights have been otherwise violated, please provide the SCRC Copyright Agent identified below with the following information:

- an electronic or physical signature of the person authorized to act on behalf of the owner of the copyright or other intellectual property interest;
- a description of the copyrighted work or other intellectual property that You claim has been infringed;
- a description of where the material that You claim is infringing is located on the site or The App;
- Your full name, alternative names used, address, telephone number, and email address;
- a statement by You that You have a good faith belief that the disputed use is not authorized by the copyright or intellectual property owner, its agent, or the law; and
- a statement by You that the above information in Your Notice is accurate and, under penalty of perjury, that You are the copyright or intellectual property owner or authorized to act on the copyright or intellectual property owner's behalf.

7. How To Obtain a License.

If You would like to use SCRC trademarks, service marks, trade dress, slogans, screenshots, marketing materials, copyrighted works, designs, or other brand features, please contact SCRC.

8. Notice re: Copyright Agent.

SCRC's designated copyright agent to whom notice of claims of copyright or other intellectual property infringement can be directed, may be reached as follows:

By Mail:

Attn: Eli Lieber, Designated Copyright Agent on behalf of SocioCultural Research Consultants, LLC 2110 Artesia Blvd #191 Redondo Beach, CA 90278, United States

By Phone:

(866) 680-2928

By Fax:

(866) 580-3837

By Email:

support@de-idapp.com

9. Construction of Terms; Resolving Ambiguities; Superseding Provisions.

In the event any terms or conditions are construed to conflict or alleged to be vague or ambiguous, whether patently or latently, the term or condition at issue will be construed to have been intended as and read as favoring the most protection for SCRC and its affiliates. In addition, a more protective provision will be construed to supersede any less protective provision that may have overlap, inconsistency, or conflict with a more protective provision. The more protective provision active, not stricken to maintain protection of SCRC. In particular, such greater protective construction of terms, conditions and provisions is fully agreed by the Parties and broadly understood to apply to this Agreement, and it stipulated as being in line with public policy to maintain continued operation of a valued provider of research services such as SCRC here, which is also important including to promoting research and academic tools.

10. EU Data Protection Authorities (DPAs) and Swiss Federal Data Protection and Information Commissioner (FDPIC) and UK Information Commissioner's Office (ICO)

In compliance with the U.S. Federal Trade Commission (FTC) and International Trade Administration (ITA) authority, and consistent with the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, SCRC designates the following Independent Recourse Mechanisms (IRMs) for unresolved complaints relating to personal data transfers:

- **European Union / EEA:** EU Data Protection Authorities (DPAs)
- **Switzerland:** Swiss Federal Data Protection and Information Commissioner (FDPIC)
- **United Kingdom:** UK Information Commissioner's Office (ICO)

Before escalation to the IRM, SCRC requires data subjects to first submit complaints directly to SCRC. SCRC will investigate and make good faith efforts to resolve issues within **30 days**. Where a complaint is unusually complex and cannot reasonably be resolved within this period, SCRC may extend the response time once for an additional 30 days.

11. Dispute Resolution—United States and General Provisions.

If the dispute arises in the United States or in a jurisdiction not specifically listed, the following procedure for dispute resolution will apply in the following order:

11.1 Written communication. First, in the event the parties have a dispute, the first step toward resolution will be informally and directly made by the parties through written communication sufficient to describe in detail the issue and what is required to be resolved; followed by a 30 minute phone or zoom conference to discuss the matter in good faith directly between the parties toward settlement of the matter.

11.2 Mediation. Second, if written communication did not resolve the issue, the parties will in good faith conduct private mediation. The Parties will each propose three candidate mediators each and agree on one mediator to proceed with mediation. The Parties will share costs of mediation. If mediation fails to resolve the matter, then resolution will be made by mandatory

and binding arbitration.

11.3 Binding Arbitration. You or SCRC may invoke mandatory and binding arbitration when other dispute resolution procedures have been exhausted. Binding arbitration can be initiated through JAMS or and ADR Services.

Terms of Use and End User License Agreement

1. Introduction

SocioCultural Research Consultants, LLC ("SCRC") is committed to safeguarding the privacy of our website and The App visitors and service users. This Policy applies where we are acting as a data processor with respect to personal data of our website visitors and service users.

When using our sites and applications, You may transmit and obtain information, access online products and services, communicate with us or others, or link to other websites and services. You may choose to provide information so that SCRC can deliver enhanced products or services to You and to personalize Your experience on our website and while using our applications.

This Policy describes how we use and seek to protect Personally Identifiable Information ("PII") which You chose to transmit or share with SCRC. This Policy is retroactively effective to the date You first used The App; and as to legacy customers of SCRC this Policy is otherwise made effective January 1, 2025, modified periodically, and may be subject to change by posting notice at https://de-id.zendesk.com/hc/en-us/articles/39537148987917-Terms-of-Service or by mail or more typically by email when significant changes are made.

The following principles govern websites and applications owned and operated by SCRC. These principles may or may not apply to any other websites of other entities to which we may provide links. SCRC is not responsible and cannot control the privacy practices or content of any other website. SCRC collects PII when You register with SCRC to use The App or any other SCRC applications or services for the following purposes:

- To access and use the products and services You or Your company have ordered for Your use from SCRC;
- To maintain accounting and billing contact information and other financial records;
- To customize the advertising and content available on our website;
- To contact you regarding our services.

When You register with SCRC, we may ask for Your name, e-mail address, physical address, telephone numbers and, in some cases, credit card information when You order services online.

Some SCRC customers arrange for teams of researchers, colleagues, or others being able to use SCRC services. Some of our customers include other institutions, businesses, or organizations as collaborators. Our customers will sometimes list business offices, individuals in those offices, or others involved in payment or business transactions on behalf of the customer. SCRC may store this information on behalf of our customers as necessary to fulfill our obligations to our customers. SCRC requires that all such customers use, hold and process such PII in accordance with applicable privacy laws. SCRC also automatically receives and records information regarding Your IP address, cookie information, and the page(s) You requested. SCRC routinely collects information that cannot be identified to a particular individual such as

timestamps and logs events (like features used, number of participants, etc.). These data are used for accounting or billing purposes, as well as for performance and optimization of SCRC services.

Some of our customers will store information on their respective database in The App that may identify the names, addresses, telephone numbers, or other identifying information linked to individuals, groups, or organizations that they have included in their information database. SCRC tries to ensure that such records are viewed only by the customer and others authorized by the customer to access such records. However, SCRC is not responsible for any unauthorized access which may result from actions beyond the sole and exclusive control of SCRC. Each SCRC customer represents that he, she, or they, has the full authority to transmit to SCRC all of the information actually transmitted.

We use cookies on our website and The App. Insofar as those cookies are not always strictly necessary for the provision of our website, The App and services, we will ask You to consent to our use of cookies when You first visit our website or The App. Note that blocking cookies can affect whether and how The App or website will function for You.

Our website and The App incorporate privacy controls which affect how we will process Your personal data.

By using the privacy controls, You can specify whether You would like to receive direct marketing communications and limit the publication of Your information.

Project data are data uploaded and belonging to a project in The App.

2. Retention

SCRC reserves the right to change its privacy policies. SCRC will post those changes to this policy statement at least 30 days before they take effect. Therefore, You should view this online privacy policy every 30 days to check for changes. In limited cases, we may be required to disclose certain information to comply with a legal process, such as a court order, subpoena or search warrant.

SCRC may use and retain Your PII when You use this website or other SCRC applications, or services. SCRC may also receive PII from its business partners.

SCRC retains the PII that it collects only for the period of time such information is required to achieve the purposes set forth above. Generally, the retention period, will not be greater than two years after You cease to be an active customer depending on the purpose and any regulatory or audit requirements (e.g., financial records may be retained for a longer period to satisfy audit requirements).

SCRC uses and retains only Your PII which is directly relevant to the purpose for which it is collected. This information is retained as You provide it, but will be updated when You notify us of changes in order to maintain its accuracy.

SCRC assumes no independent responsibility to verify the accuracy or currency of any PII.

3. Information Sharing and Disclosure

SCRC will not sell or rent Your PII except as authorized under this policy. SCRC will send

PII about You to other companies or people only when:

- SCRC has Your consent to share the information;
- SCRC needs to share Your information to provide the application or service You have requested;
- SCRC needs to send the information to companies who work on behalf of SCRC in order to provide an SCRC application or service or to otherwise assist SCRC with its business activities;
- SCRC determines, in its sole and absolute discretion, that it is necessary to transmit Your PII to respond to subpoenas, court orders or engage in the legal process; or
- SCRC determines that Your actions on our websites violate this Online Privacy Policy, the Terms of Service; or the Terms of Use, End User License Agreement, Disclaimer, and Release of Liability.

4. Corrections or Modifications to PII

You can direct SCRC to edit, correct, or erase Your PII, at any time, except as otherwise provided for in this policy. To request such account maintenance, send Your e-mail request to support@de-idapp.com. You may also indicate that You do not wish to receive messages from SCRC regarding our services or update and can send Your information relating to such messages at support@de-idapp.com. Following Your request for either type of data editing, Your information will be changed within a reasonable amount of time in SCRC's databases after we receive the information necessary to process Your request.

5. Confidentiality

SCRC strongly recommends that You carefully guard any passwords issued by SCRC for use of the websites or applications. It is the policy of SCRC to require that each customer identify one individual to whom an administrative password will be issued (the "Account Administrator"). The Account Administrator is solely and exclusively responsible for guarding their password. Any additional passwords authorized for multiple users of The App will be issued to the Account Administrator, who will have sole and exclusive responsibility to provide any additional passwords to other authorized users. SCRC is not responsible for any unauthorized acquisition and use of passwords or unauthorized access to The App resulting from such acquisition and use after the Account Administrator is provided the administrative password issued by SCRC.

The Account Administrator may choose to relinquish a password at any time. However, such relinquishment will only be effective if done so according to SCRC's policies and procedures. Within thirty (30) days of service termination, SCRC will terminate all passwords issued to the Customer.

6. How We Use Your Personal Data

In this portion of the Policy, we explain:

- the types of personal data that we may process;
- if personal data was not obtained from You, the source and categories of that data;

- purposes we may process personal data; and
- legal bases of processing.

Usage Data. For example, we may process data about Your use of our website, The App and services **("usage data")**. The usage data may include Your IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views and website navigation paths, as well as information about the timing, frequency and pattern of Your service use. Usage data is generated as the user accesses and uses the application. These data are stored as part of the application's internal logging system. Usage data may be processed for analyzing the use of the website, The App and services, or for troubleshooting issues found while utilizing The App. The legal basis for this processing is consent OR our legitimate interests, namely monitoring and improving our website and services (The App), OR as deemed legally necessary by law.

6.1. Account Data. We may process Your account data. The account data may include Your name and/or account names and/or supplied email address, provided by You, Your account manager and/or Your employer. The account data may be processed for the purposes of operating our website or The App, providing our services, ensuring the security of our website and services (The App), maintaining back-ups of our databases and communicating with You. The legal basis for this processing is with specific consent (either verbal or written) OR other legitimate interests, namely when seeking support/troubleshooting OR performance of a contract between You and SCRC and/or taking steps, at Your request, to enter into such a contract, OR on an as-needed legal basis.

6.2. Profile Data. We may process Your information **("profile data")**. The profile data may include Your name, address, telephone number, or email address. The profile data may be processed for the purposes of enabling and monitoring Your use of our website/or services (The App). The legal basis for this processing is with specific consent (either verbal or written) OR other legitimate interests, namely when seeking support/troubleshooting OR performance of a contract between You and SCRC and/or taking steps, at Your request, to enter into such a contract, OR on an as-needed legal basis.

6.3. Service Data. We may process Your personal data that are provided in the course of the use of our services **("service data")**. The service data may include Your name, address, telephone number, or email address. The profile data may be processed for the purposes of enabling and monitoring Your use of our website/or services (The App). The legal basis for this processing is with specific consent (either verbal or written) OR other legitimate interests, namely when seeking support/troubleshooting OR performance of a contract between You and SCRC and/or taking steps, at Your request, to enter into such a contract, OR on an as-needed legal basis.

6.4. Publication Data. We may process information that You post for publication on our website, The App or through our services or support staff **("publication data")**. The publication data may be processed for the purposes of enabling such publication and administering our

website, The App and services. The legal basis for this processing is with specific consent (either verbal or written) OR other legitimate interests, namely when seeking support/troubleshooting OR performance of a contract between You and SCRC and/or taking steps, at Your request, to enter into such a contract, OR on an as-needed legal basis.

6.5. Enquiry Data. We may process information contained in any enquiry You submit to us regarding services and/or support inquiries **("enquiry data")**. The enquiry data may be processed for the purposes of offering, marketing and selling relevant goods and/or services to You. The legal basis for this processing is specific verbal or written consent.

Customer Relationship Data. We may process information relating to our customer relationships, including customer contact information **("customer relationship data")**. The customer relationship data may include Your name, Your employer, Your contact details, and information contained in communications between us and You or Your employer. The source of the customer relationship data You or Your employer. The customer relationship data may be processed for the purposes of managing our relationships with customers, communicating with customers, keeping records of those communications and promoting our products and services to customers. The legal basis for this processing is specific written/oral consent OR our legitimate interests, namely the proper management of our customer relationships OR for managing/providing specific support-related inquiries.

6.6. Transaction Data. We may process information relating to transactions, including purchases of goods and services, that You enter into with us and/or through our website and/or The App **("transaction data")**. The transaction data may include Your contact details, Your card details and the transaction details. The transaction data may be processed for the purpose of supplying the purchased goods and services and keeping proper records of those transactions. The legal basis for this processing is the performance of a contract between You and us and/or taking steps, at Your request, to enter into such a contract and our legitimate interests, namely the proper administration of our website, The App and business OR managing/providing specific support-related inquiries.

6.7. Notification Data. We may process information that You provide to us for the purpose of subscribing to our email notifications and/or newsletters **("notification data")**. The notification data may be processed for the purposes of sending You the relevant notifications and/or newsletters. The legal basis for this processing is Your consent OR the performance of a contract between You and us and/or taking steps, at Your request, to enter into such a contract.

6.8. Correspondence Data. We may process information contained in or relating to any communication that You send to us **("correspondence data")**. The correspondence data may include the communication content and metadata associated with the communication. Our website and The App will generate the metadata associated with communications made using the website contact forms or through The App. The correspondence data may be processed for the purposes of communicating with You and record- keeping. The legal basis for this processing is

our legitimate interests, namely the proper administration of our website, business and The App, and communications with users.

6.9. Legal Process. We may process any of Your personal data identified in this policy where necessary for the establishment, exercise or defense of legal claims, whether in court proceedings or in an administrative or out-of-court procedure. The legal basis for this processing is our legitimate interests, namely the protection and assertion of our legal rights, Your legal rights and the legal rights of others.

6.10. Risk Mitigation. We may process any of Your personal data identified in this policy where necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, or obtaining professional advice. The legal basis for this processing is our legitimate interests, namely the proper protection of our business and customers against risks.

Compliance With Legal Duties. In addition to the specific purposes for which we may process Your personal data set out in this Paragraph, we may also process any of Your personal data where such processing is necessary for compliance with a legal obligation to which we are subject, or in order to protect Your vital interests or the vital interests of another natural person.

6.11. Restriction On Supply of Others' Data. Please do not supply any other person's personal data to us, unless we prompt You to do so.

7. Providing Your Personal Data to Others

We may disclose Your personal data to any member of our group of companies (this means our subsidiaries, our ultimate holding company and all its subsidiaries) insofar as reasonably necessary for the purposes, and on the legal bases, set out in this policy.

We may disclose Your personal data to our insurers and/or professional advisers insofar as reasonably necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, obtaining professional advice, or the establishment, exercise or defense of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

Financial transactions relating to our website and services (The App) are OR may be handled by stripe.com, our payment services providers. We will share transaction data with our payment services providers only to the extent necessary for the purposes of processing Your payments, refunding such payments and dealing with complaints and queries relating to such payments and refunds. You can find information about the payment services providers' privacy policies and practices at: https://stripe.com/.

In addition to the specific disclosures of personal data set out in this Paragraph, we may disclose Your personal data where such disclosure is necessary for compliance with a legal obligation to which we are subject, or in order to protect Your vital interests or the vital interests of another natural person. We may also disclose Your personal data where such disclosure is necessary for the establishment, exercise or defense of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

8. International Transfers of Your Personal Data

In this Paragraph, we provide information about the circumstances in which Your personal data may be transferred to countries outside the European Economic Area (EEA).

You acknowledge that personal data that You submit for publication through our website or The App or services may be available, via the internet, around the world. We cannot prevent the use (or misuse) of such personal data by others.

9. Retaining And Deleting Personal Data

This Paragraph sets out our data retention policies and procedure, which are designed to help ensure that we comply with our legal obligations in relation to the retention and deletion of personal data.

Personal data that we process for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

We will retain Your personal data as follows:

- Personal data shall be retained between 6 and 24 months after termination of services, depending on contractual, legal, regulatory, or audit requirements. Certain data (such as financial records) may be retained longer where required by law.
- User-Related Data will be retained for a minimum period of 6 months following the User's termination of services, and for a maximum period of 24 months following the User's termination of services.

In some cases, it is not possible for us to specify in advance the periods for which Your personal data will be retained. In such cases, we will determine the period of retention based on the following criteria: the period of retention of Personal Data will be determined based on the same 6 to 24-month principle described above. SCRC is not responsible for maintaining Personal Data for any specific purpose beyond the minimum length of time of the required retention period. You may delete your De-ID account and associated personal data via the De-ID app in the "Personal Data" section of account management settings.

Notwithstanding the other provisions of this Paragraph, we may retain Your Personal Data where such retention is reasonably necessary for compliance or good faith belief in compliance with a legal obligation to which we are subject, or in order to protect Your vital interests or the vital interests of another natural person based on SCRC's determination to do so in good faith.

10. Amendments

We may update this policy from time to time by publishing a new version on our website and/or The App. You should check this page occasionally to ensure You are happy with any changes to this policy. We will notify You of significant changes to this policy by posted notice; by email; or if no email then by mail to your last known address.

11. Your Rights

This Paragraph is designed to disclose rights You have under data protection law. Some of the rights are complex, and not all of the details have been included in our summaries. Accordingly, You should read the relevant laws and guidance from the regulatory authorities for a full

explanation of these rights.

Identification of Your rights as an EU individual under data protection law are:

- the right to access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to object to processing;
- the right to data portability;
- the right to complain to a supervisory authority; and
- the right to withdraw consent.

You have the right to confirmation as to whether or not we process Your personal data and, where we do, access to the personal data, together with certain additional information. That additional information includes details of the purposes of the processing, the categories of personal data concerned and the recipients of the personal data. Providing the rights and freedoms of others are not affected, we will supply to You a copy of Your personal data. The first copy will be provided free of charge, but additional copies may be subject to a reasonable fee. You can access Your personal data by visiting Your Account Workspace when logged into The App.

You have the right to have any inaccurate personal data about You rectified and, taking into account the purposes of the processing, to have any incomplete personal data about You completed.

In some circumstances You have the right to the erasure of Your personal data without undue delay. Those circumstances include: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; You withdraw consent to consent-based processing; You object to the processing under certain rules of applicable data protection law; the processing is for direct marketing purposes; and the personal data have been unlawfully processed. However, there are exclusions of the right to erasure. The general exclusions include where processing is necessary:

- to exercise the right of freedom of expression and information;
- to seek to comply with a legal obligation; or
- for the establishment, exercise, or defense of claims in a legal or quasi-legal proceeding.

Regarding the Right to Erasure:

You have the right to request the erasure of Your personal data without undue delay where one of the grounds in Article 17(1) of the GDPR (and the equivalent provisions of UK GDPR and the Swiss FADP) applies. This includes where the data are no longer necessary for the purposes for which they were collected, where You withdraw consent and no other lawful basis exists, where You successfully object to processing, where the data have been unlawfully processed, or where the data must be erased for compliance with a legal obligation.

Erasure is subject to the exemptions under GDPR Article 17(3), UK GDPR, and FADP, including

where processing is necessary for exercising freedom of expression, for compliance with a legal obligation, for reasons of public interest, or for the establishment, exercise, or defense of legal claims.

Where SCRC has made Your personal data public, or has shared Your personal data with third parties, SCRC will take reasonable steps to inform other controllers processing Your data of Your erasure request, unless this proves impossible or involves disproportionate effort (as permitted under GDPR Article 19).

SCRC will respond to valid erasure requests within thirty (30) days. Where a request is unusually complex, SCRC may extend this period once for an additional thirty (30) days, provided that SCRC notifies You within the initial 30-day period.

Notwithstanding the foregoing, SCRC may retain certain personal data for up to twenty-four (24) months after termination of services, or longer if required by law or regulatory obligations (e.g., financial records, audit requirements). Retention beyond this period will occur only where strictly necessary and lawfully justified.

In some circumstances, You have the right to restrict the processing of Your personal data; for example: You contest the accuracy of the personal data; processing is unlawful but You oppose erasure; we no longer need the personal data for the purposes of our processing, but You require personal data for the establishment, exercise or defense of legal claims; and You have objected to processing, pending the verification of that objection. Where processing has been restricted on this basis, we may continue to store Your personal data. However, we will only otherwise process it: with Your consent; for the establishment, exercise or defense of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important public interest.

You have the right to object to our processing of Your personal data on grounds relating to Your particular situation, but only to the extent that the legal basis for the processing is that the processing is necessary for: the performance of a task carried out in the public interest or in the exercise of any official authority vested in us; or the purposes of the legitimate interests pursued by us or by a third party. If You make such an objection, we will cease to process the personal information unless we can demonstrate compelling legitimate grounds for the processing which override Your interests, rights and freedoms, or the processing is for the establishment, exercise or defense of legal claims.

You have the right to object to our processing of Your personal data for direct marketing purposes (including profiling for direct marketing purposes). If You make such an objection, we will cease to process Your personal data for this purpose.

You have the right to object to our processing of Your personal data for scientific or historical research purposes or statistical purposes on grounds relating to Your particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

To the extent that the legal basis for our processing of Your personal data is:

- consent; or
- that the processing is necessary 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; and
- such processing is carried out by automated means, You have the right to receive Your personal data from us in a structured, commonly used and machine-readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others.

If You consider that our processing of Your personal information infringes data protection laws, You have a legal right to lodge a complaint with a supervisory authority responsible for data protection. You may do so in the EU member state of Your habitual residence, Your place of work or the place of the alleged infringement.

To the extent that the legal basis for our processing of Your personal information is consent, You have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

You may exercise any of Your rights in relation to Your personal data by written notice to us OR via phone.

12. How to Contact SCRC

This website and services (The App) is owned and operated by SocioCultural Research Consultants, LLC. SCRC's principal place of business is: SocioCultural Research Consultants, LLC 2110 Artesia Blvd #191 Redondo Beach, CA 90278, United States. You can contact us:

- by post, to the postal address given above;
- using our website contact form;
- by telephone, on the contact number published on our website and/or The App from time to time; or
- by email, using the email address published on our website and/or The App from time to time

13. Data Protection Officer

Our data protection officer contact details are provided as follows: Jose Gamez, SocioCultural Research Consultants, LLC 2110 Artesia Blvd #191 Redondo Beach, CA 90278, United States.

14. Cookies Policy

14.1. About cookies.

A cookie is a file containing an identifier (a string of letters and numbers) that is sent by a web server to a web browser and is stored by the browser. The identifier is then sent back to the server each time the browser requests a page from the server. Cookies may be "persistent" or "session" cookies. A persistent cookie will be stored by a web browser and will remain valid until its set expiry date, unless deleted by the user before the expiry date. A session cookie, on the other hand, will expire at the end of the user session, when the web browser is closed. Cookies do not typically contain any information that personally identifies a user, but personal information

that we store about You may be linked to the information stored in and obtained from cookies.

14.2. Cookies That We Use.

We use cookies for the following purposes:

- Authentication - we use cookies to identify You when You visit our website or The App and as You navigate our website or The App, cookies used for this purpose are for identifying purposes only
- Identification - we use cookies to help us to determine if You are logged into our website or The App (cookies used for this purpose are for identifying purposes only);
- Personalization - we use cookies to store information about Your preferences and to personalize the website and/or The App for You (cookies used for this purpose are authentication and access- related); and
- Security - we use cookies as an element of the security measures used to protect user accounts, including preventing fraudulent use of login credentials, and to protect our website and services (The App) generally (cookies used for this purpose are: identification and authentication).

14.3. Cookies Used by Our Service Providers.

Our service providers use cookies and those cookies may be stored on Your computer when You visit our website and/or The App. We use Google Analytics to analyze the use of our website and The App. Google Analytics gathers information about website use by means of cookies. The information gathered relating to our website and The App is used to create reports about the use of our website and The App. Google's privacy policy is available at: https://www.google.com/policies/privacy/. The relevant cookies include identification cookies.

14.4. Managing Cookies.

Cookies are managed via Your internet browser controls. Please review the user manual for Your browser for the most up to date information on managing Your browser's cookies setting and whether cookies are blocked or not, particularly for The App being accessed via or any of its subdomains.

Blocking all cookies will have a negative impact upon the usability of many websites as well as The App. If You block cookies, You will not be able to use all the features on our website or The App.

15. Data Transmission Security

All application data transmission between client and server occurs over HTTPS encrypted connections. HTTPS connection cypher suite selection is updated in accordance with IETF cypher suite recommendations and is updated regularly as those recommendations are changed over time. Currently TLS 1.3 and 1.2 are supported with all weak cypher suites combinations disabled.

16. Data Storage Security

The App is hosted on commercial servers with all application data backed-up in-full on a nightly basis, encrypted using AES-256 processes, and transferred automatically replicated to Georedundant storage volumes using Azure's automated backup features. Microsoft's Azure

Cloud Platform is fully SAS 70 Type II / SSAE 16 SOC and HIPAA compliant.

17. Data Retention

SCRC strongly believes Your data are Your data. SCRC will not share Your data with any third parties and allow You to export all Your data at any time. You acknowledge and agree that SCRC is authorized to automatically delete all user data after a two (2) year period of no active user login. You may, at any time, wish for Your data and/or Your user and account information to be deleted. If so, please send an authorized request to support@de-idapp.com and we will facilitate the processing.

Following the expiration of all of Your user licenses for The App with authorized administrative access to a project's data on a particular client account, users can regain access to the project after re-activating their respective subscription for as long as SCRC continues to archive the project data. The following details SCRC's data retention policy for data uploaded to The App:

- SCRC will retain data for not more than two years after the expiration of all user logins;
- Authorized users can regain access to project data during this two-year period by providing a specific written request to SCRC to support@de-idapp.com;
- Upon specific written request from the user SCRC will permanently delete all user data at no charge BEFORE the two-year period;
- Within six months of either: a) the end of the two-year retention period, or b) after receiving the express written request from the user or account owner, SCRC, using all available technical measures, will delete all data from backup media; and SCRC may retain project data longer than two years upon written request from an authorized individual.

17.1 Artificial Intelligence Statement

SCRC fully appreciates the responsibility of protecting human subjects and engaging in ethical research practices. Accordingly, SCRC believes Your data are Your data and thus SCRC does not use your project or personal data to inform the development of any large language models or any artificial intelligence services.

18. Privacy Protection

SCRC provides industry standard protection for personally identifying information.

- Under limited circumstances, SCRC can be obligated to disclose and will then disclose as required by law in good faith, personally identifiable information about users or information about Your project to third parties in the following situations: (1) with Your consent; or (2) when we have a good faith belief it is required by law, such as pursuant to a subpoena or other governmental, judicial, or administrative order.
- If SCRC is required by law to disclose personally identifying or project data, SCRC will attempt to provide You with notice (unless we are prohibited from doing so) that a request for Your information has been made in order to give You an opportunity to object to the disclosure.

We will attempt to provide this notice by email, if You have given us an email address, and/or by postal mail if You have provided a postal address. Even if You challenge the disclosure request, we may still be legally required to turn over the personally identifying information and/or project data.

19. Data Breach Notification and Incident Response Plan

SCRC hosts all data within the continental U.S. unless agreed upon and determined as needed on a project- by-project basis. SCRC has a systematic plan for response and notification of any breach in data security.

Upon the detection of any breach in data security, SCRC technical staff, led by the SCRC Chief Technical Officer, will immediately assess the size, scope, and severity of the breach. Following this assessment,

SCRC will notify all project administrators of projects that may have been involved and communicate the response plan. Depending on the nature and cause of the breach, SCRC will take appropriate action to prevent any future breach and then, to the extent reasonably practicable, restore the integrity of all project data that had been affected. Further details about this notification and response plan will be provided upon request.

SCRC cannot and does not guarantee complete data security and integrity for project related data. However, the tools described above are designed to provide industry-standard security and SCRC recommends that users strictly adhere to the security protocols described in this document and are diligent in their protection of the data for which they are responsible.

20. Information About Required Categories of Disclosures

In accordance with the following requirements, SCRC provides the following:

- Information about personal information necessarily disclosed to third parties is in Paragraph 7, “Providing Your Personal Data to Others.”
- Information about the right of individuals to access their personal data is in Paragraph 11, “Your Rights.”
- Information about the choices and means SCRC offers individuals for limiting the use and disclosure of their personal data is in Paragraph 11, “Your Rights.”
- Information about FTC Power: SCRC is subject to the Federal Trade Commission’s power to investigate or enforce according to due process of law. SCRC will in good faith comply with any legal requirements and will make reasonable efforts to notify You of a demand for Your PII according to the Parties’ agreements and counterparts.
- Information about disclosure concerning EU individuals regarding arbitration: There exists the possibility, under certain conditions, for the individual to invoke binding arbitration when others dispute resolution procedures have been exhausted. Under certain conditions, You being a subject under applicable laws and pursuant to the DPF may invoke binding arbitration. SCRC is obligated to arbitrate claims and follow the terms as set forth in Annex I of the DPF Principles, provided that an individual has invoked binding arbitration by delivering notice to SCRC

and following the procedures and subject to conditions set forth in Annex I of Principles.

- Information about disclosure concerning EU individuals if required by law enforcement: Personal information may be disclosed to respond to lawful requests by public authorities. SCRC is required to disclose personal information in response to lawful requests by public authorities, including those necessary to meet national security or law enforcement requirements. SCRC will in good faith comply with any legal requirements and will make reasonable efforts to notify You of a demand for Your PII according to the Parties' agreements and counterparts.
- Information about liability concerning EU individuals in case of onward transfer to third parties: SCRC can be contacted regarding a claim of liability in writing as follows: By mail to: SocioCultural Research Consultants, LLC 2110 Artesia Blvd # 191, Redondo Beach, CA USA 90278-3073; By Phone: (866) 680-2928; By Fax: (866) 580-3837; or By Email: <support@de-idapp.com>. SCRC does not automatically admit liability, but does acknowledge the potential for liability in cases of onward transfers to third parties of personal data of EU individuals received pursuant to EU-U.S. Data Privacy Framework Principles. SCRC remains strongly committed to protecting PII as exhaustively described in the Parties' agreements and counterparts, including by the SCRC 7-Lock System as summarized in the Online Privacy Policy, Paragraph 18.

21. GDPR and Data Privacy Network

SCRC complies with the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce.

SCRC has certified to the U.S. Department of Commerce that it adheres to:

- the EU-U.S. DPF Principles with regard to personal data received from the European Union in reliance on the EU-U.S. DPF,
- the UK Extension to the EU-U.S. DPF with regard to personal data received from the United Kingdom, and
- the Swiss-U.S. DPF Principles with regard to personal data received from Switzerland.

If there is any conflict between the terms in this Privacy Policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern.

To learn more about the Data Privacy Framework (DPF) Program, and to view our certification, please visit: https://www.dataprivacyframework.gov/s/

SCRC will investigate and make good faith efforts to resolve all reported issues within 30 days. If a complaint is unusually complex and cannot reasonably be resolved within this period,

SCRC may extend the response time once for an additional 30 days, provided that SCRC notifies the individual within the initial 30-day period.

In compliance with the GDPR and the applicable DPF Principles, SCRC commits to resolve complaints about our collection or use of your personal information. Individuals with inquiries or complaints regarding our privacy policy should first contact SCRC at:

SocioCultural Research Consultants, LLC 2110 Artesia Blvd # 191, Redondo Beach, CA 90278-3073 USA.

22. Intellectual Property Rights

The following provisions shall apply with respect to copyrightable works, proprietary, development, technical, assessment methodologies, artwork, presentation materials, manuals, computer programming techniques and all record bearing media containing or disclosing such information and techniques, ideas, discoveries, inventions, applications for patents, and patents (collectively, "Intellectual Property").

SCRC exclusively owns and holds an interest in the Intellectual Property that is described herein. Intellectual Property will include but not be limited to those products and services, including but not limited to the Software developed by SCRC and/or its affiliates before, during and after services provided and described in this Agreement. Any improvements to Intellectual Property items listed herein, further inventions or improvements, and any new items of Intellectual Property discovered or developed by SCRC or its employees or agents, during the term of this Agreement shall be the sole and exclusive property of SCRC.

You will not acquire any rights or interest in any way in such Intellectual Property by virtue of the development, experimentation, modification, or adaptation of any portion of the Software.

SCRC grants You a non-exclusive license to use SCRC's intellectual property embodied in the Software needed to exploit the rights granted under this Agreement. Nothing in this Agreement shall constitute a waiver of any rights or license in any and all patents, trademarks, service marks, ownership interests, or copyrights that SCRC has in the Software.

You agree that You will not distribute the Intellectual Property or software of SCRC contained in the Software to any person or entity other than as contemplated in this Agreement. You agree to undertake best efforts to prevent transmission of usernames or passwords provided by SCRC to any person or entity except as provided in this Agreement.

23. Title and Protection.

All rights, title, and interest in and to the Software are and shall remain at all times the property of SCRC and/or SCRC's suppliers. You agree to take all reasonable steps to protect the Intellectual Property rights of SCRC, including, but not limited to distributing unauthorized passwords, storing any portion of the Software, streaming content or media, or otherwise taking

any actions to dilute the Intellectual Property rights of SCRC.

24. Warranties.

You understand and agree that the software and website are provided "AS IS" and SCRC, its affiliates, suppliers and resellers expressly disclaim all warranties of any kind, express or implied, including without limitation any warranty of merchantability, fitness for a particular purpose or non-infringement. SCRC, its affiliates, suppliers and resellers make no warranty or representation regarding the results that may be obtained from the use of the software, regarding the accuracy or reliability of any information obtained through the software, regarding any goods or services purchased or obtained through Your use of The App or the website, regarding any transactions entered into through the software or that the software will meet any user's requirements, or be uninterrupted, timely, secure or error free. Use of the software is at Your sole risk. any material and/or data downloaded or otherwise obtained through the use of The App or website is at Your own discretion and risk. You will be solely responsible for any damage to You resulting from the use of the software. The entire risk arising out of use or performance of the software remains with You.

25. Indemnification.

You agree to indemnify, defend and hold harmless SCRC, its affiliates, officers, directors, employees, members, and managers (collectively, 'Indemnified Parties') from any and all third party claims, liability, damages and/or costs (including, but not limited to, attorney's fees) (collectively, 'Claims') arising from Your use of the Software, Your violation of this Agreement, Your violation of laws or regulations, or Your
infringement of any intellectual property or other right of any person or entity, but excluding Claims to the extent they arise from any negligence, breach of this Agreement, infringement of any intellectual property or other right of any person or entity, or other wrongful conduct of any Indemnified Parties.

26.1. Introduction.

We are committed to safeguarding the privacy of our website and The App visitors and service users. This policy applies where we are acting as a data processor with respect to the personal data of our website visitors and service users; in other words, where we determine the purposes and means of the processing of that personal data.

Note about cookies: We use cookies on our website and The App. Insofar as those cookies are not strictly necessary for the provision of our website, The App and services, we will ask You to consent to our use of cookies when You first visit our website or The App.

Note about our website and The App: Our website and The App incorporates privacy controls which affect how we will process Your personal data. By using the privacy controls, You can specify whether You would like to receive direct marketing communications and limit the publication of Your information.

Disclosures: SCRC is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC). There exists the possibility, under certain conditions, for the individual

to invoke binding arbitration when other dispute resolution procedures have been exhausted. SCRC is also required to disclose personal information in response to lawful requests by public authorities, including those necessary to meet national security or law enforcement requirements. SCRC acknowledges the potential liability in cases of onward transfers to third parties of personal data of EU individuals received pursuant to the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) and to the rights of EU and UK individuals and Swiss individuals.

26.2. How we use Your personal data.

See Paragraph 6, including subparts 6.1 to 6.14.

26.3. Providing Your Personal Data To Others.

See Paragraph 7.

26.4. International Transfers Of Your Personal Data.

In this Paragraph, we provide information about the circumstances in which Your personal data may be transferred to countries outside the European Economic Area (EEA).

You acknowledge that personal data that You submit for publication through our website or The App or services may be available, via the internet, around the world. You understand and acknowledge that SCRC cannot prevent the use or misuse of such personal data by others.

26.5. Retaining And Deleting Personal Data.

This Paragraph describes our data retention policies and procedure, which are designed to help ensure that we comply with our legal obligations in relation to the retention and deletion of personal data.

Personal data that we process for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

We will retain Your personal data as follows:

- Personal Data will be retained for a minimum period of 6 months following the occurrence of termination of services of the User's account, and for a maximum period of 24 months following the occurrence of termination of services of the User's account.
- Project-Related Data will be retained for a minimum period of 6 months following the occurrence of termination of services of the User's account, and for a maximum period of 24 months following the occurrence of termination of services of the User's account.

In some cases, it is not possible for us to specify in advance the periods for which Your personal data will be retained. In such cases, we will determine the period of retention based on the following criteria: the period of retention of Personal Data will be a minimum period of 6 months following the occurrence of termination of services of the User's account, and for a maximum period of 24 months following the occurrence of termination of services of the User's account.

Notwithstanding the other provisions of this Paragraph, we may retain Your personal data where such retention is necessary for compliance with a legal obligation to which we are subject, or in order to protect Your vital interests or the vital interests of another natural person.

26.6. Amendments.

We may update this policy from time to time by publishing a new version on our website and/or The App. You should check this page occasionally to ensure You agree with any changes to this policy at < https://de-id.zendesk.com/hc/en-us/articles/39537148987917-Terms-of-Service >. We also reserve the right to notify You of significant changes to this policy by email.

26.7. Your Rights.

Below is a summary of the rights that You have under data protection law. We also give you additional explanation further below.

Some of the rights are complex, and not all of the details have been included in our summary; therefore, you should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights. You may also seek independent legal advice regarding the exercise of these rights, though such advice is not required to exercise your rights under applicable data protection law. Rights of EU individuals under data protection law include:

- the right to access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to object to processing;
- the right to data portability;
- the right to complain to a supervisory authority; and
- the right to withdraw consent.

More explanation follows:

You have the right to confirmation as to whether or not we process Your personal data and, where we do, access to the personal data, together with certain additional information. That additional information includes details of the purposes of the processing, the categories of personal data concerned and the recipients of the personal data. Providing the rights and freedoms of others are not affected, we will supply to You a copy of Your personal data. The first copy will be provided free of charge, but additional copies may be subject to a reasonable fee. You can access Your personal data by visiting Your Account Workspace when logged into The App.

You have the right to have any inaccurate personal data about You rectified and, taking into account the purposes of the processing, to have any incomplete personal data about You completed.

In some circumstances, You have the right to the erasure of Your personal data without undue delay; for example: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; You withdraw consent to consent-based processing; You object to the processing under certain rules of applicable data protection law; the processing is for direct marketing purposes; and the personal data have been unlawfully processed. However, there are exclusions of the right to erasure. The general exclusions include where processing is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation; or for the establishment, exercise or defense of legal claims.
In some circumstances, You have the right to restrict the processing of Your personal data; for example: You contest the accuracy of the personal data; processing is unlawful but You oppose erasure; we no longer need the personal data for the purposes of our processing, but You require personal data for the establishment, exercise or defense of legal claims; and You have objected to processing, pending the verification of that objection. Where processing has been restricted on this

basis, we may continue to store Your personal data.

However, we will only otherwise process it: with Your consent; for the establishment, exercise or defense of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important public interest.

You have the right to object to our processing of Your personal data on grounds relating to Your particular situation, but only to the extent that the legal basis for the processing is that the processing is necessary for: the performance of a task carried out in the public interest or in the exercise of any official authority vested in us; or the purposes of the legitimate interests pursued by us or by a third party. If You make such an objection, we will cease to process the personal information unless we can demonstrate compelling legitimate grounds for the processing which override Your interests, rights and freedoms, or the processing is for the establishment, exercise or defense of legal claims.

You have the right to object to our processing of Your personal data for direct marketing purposes (including profiling for direct marketing purposes). If You make such an objection, we will cease to process Your personal data for this purpose.

You have the right to object to our processing of Your personal data for scientific or historical research purposes or statistical purposes on grounds relating to Your particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

To the extent that the legal basis for our processing of Your personal data is:

- consent; or
- that the processing is necessary 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,
- and such processing is carried out by automated means, You have the right to receive Your personal data from us in a structured, commonly used, and machine-readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others besides You.

You consider that our processing of Your personal information infringes data protection laws, You have a legal right to lodge a complaint with a supervisory authority responsible for data protection. You may do so in the EU member state of Your habitual residence, Your place of work or the place of the alleged infringement.

To the extent that the legal basis for our processing of Your personal information is consent, You have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

You may exercise any of Your rights in relation to Your personal data by written notice to us OR via phone.

26.8. Cookie Policy.

See Para. 14 and subparts 14.1. to 14.4.

26.9. Contacting Us.

This website <de-idapp.com> or any of its subdomains and services including The App are owned and operated by SCRC. Our principal place of business is located at 2110 Artesia Blvd # 191, Redondo Beach, CA 90278 USA. You can contact us as follows:

- by post, to the postal address given above;
- using our website contact form;
- by telephone, on the contact number published on our website and/or The App from time to time; or
- by email, using the email address published on our website and/or The App from time to time.

26.10. Cookie Policy.

Contact Information: SCRC's data protection officer can be reached as follows: Jose Gamez support@de-idapp.com SocioCultural Research Consultants, LLC 2110 Artesia Blvd # 191, Redondo Beach, CA 90278 USA.

26.11. Data Communication Security.

See Paragraph 15, "Data Communication Security."

26.12. Data Storage Security.

See Paragraph 16, "Data Storage Security."

26.13. Data Retention.

See Paragraph 17, "Data Retention."

26.14. Privacy Protection.

See Paragraph 18, "Privacy Protection."