Updated: 9/25/23

ONLINE PRIVACY POLICY

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

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 December 1, 2006, modified periodically, and may be subject to change by posting notice at https://dedoose.com/resources/terms (https://dedoose.com/resources/terms) 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 Dedoose 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; and/or
- to contact You regarding our services.

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

Some of our customers use SCRC to include teams of researchers, colleagues, or others 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.) This data is 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 Dedoose database 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 it, 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 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.

Project data are data uploaded and belonging to a project in Dedoose.

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@dedoose.com (mailto:support@Dedoose.com). You may also indicate that You do not wish to receive messages from SCRC regarding our services or update Your information relating to such messages at support@dedoose.com (mailto:support@Dedoose.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, and only 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 Dedoose 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 Dedoose 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.

6.1. 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. The source of the usage data is Google Analytics and Stackify. This usage data may be processed [for the purposes of 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.

6.2. 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.

6.3. Profile Data.

We may process Your information ("**profile data"**). The profile data may include Your name, address, telephone number, email address, date of birth, and employment details. 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. 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, email address, date of birth, and employment details. 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.

6.5. 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.

6.6. 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.

6.7. 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.

6.8. 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.

6.9. 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.

6.10. 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.

6.11. 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.

6.12. 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.

6.13. 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.

6.14. 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 our payment services providers, authorize.net. 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://www.authorize.net (https://www.authorize.net/)

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 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.
- Project-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.

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.

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: 644 36th Street, Manhattan Beach, CA, 90266, 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: Jason Taylor (jtaylor@dedoose.com), 644 36th Street, Manhattan Beach, CA, 90266, 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/ (https://www.google.com/policies/privacy/) . The relevant cookies are: 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 <https://dedoose.com> 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 Communication Security.

All data communication through Dedoose occurs through a 2-lock system. First, Dedoose sets up an AES (Advanced Encryption Standard)-256 CBC (Cipher Block Chaining) Encrypted SSL (Secure Sockets Layer) tunnel using a premium SSL-EV certificate. All communication following this channel is encrypted. The user is not prompted for login information until this communication channel is established. In order to prevent transfer of login details, Dedoose employs a one-way, non-reversible encryption algorithm known as SHA-2 (Secure Hash Algorithm)—designed by the United States National Security Agency. Dedoose does not store user passwords. Rather, the system stores the known result of this algorithm against the username and password and then compares that result to the result the Dedoose software client sends to the server for authentication.

16. Data Storage Security.

Dedoose is hosted on commercial servers with all project data backed-up in-full on a nightly basis, encrypted using AES-256 processes, and transferred automatically to three Geo-redundant storage volumes. One of these volumes is on-site, while the other 2 are off-site and replicated across geographic regions. All project file data are encrypted and stored in a Microsoft Azure Geo-redundant fault tolerant storage volume, and for added safety, this storage volume is encrypted and mirrored in real-time to a Amazon S3 storage volume in the same geographic region. Both Microsoft's Azure Cloud Platform and Amazon's S3 Storage platform are fully SAS 70 Type II / SSAE 16 SOC and HIPAA compliant. To ensure these processes are working as designed, an automated program runs daily which includes: a) downloading the most recent backup files from each storage volume, b) verification the backup file is the correct version, c) a full test restoration of the database to assure data integrity, and c) email reporting of all backup and restoration process results to key members of the SCRC's Dedoose Admin team.

17. Data Retention.

SCRC strongly believes Your data is Your data. SCRC promises not to share Your data with any third parties and allows You to export all of Your data at any time. You acknowledge and agree that SCRC is authorized to automatically delete all project data after two (2) years of no active subscription associated with a project. If for any reason You would like all Your project data and/or Your user and account data deleted. Please send an authorized request to support@dedoose.com (mailto:support@dedoose.com) and we will happily oblige.

Following the expiration of all Dedoose user licenses 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 subscription for as long as SCRC continues to archive the project data. The following details SCRC's data retention policy for Dedoose data:

- 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@dedoose.com;
- Upon specific written request from the project administrator, SCRC will permanently delete all project data **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 project administrator, SCRC will delete all data from backup media; and
- SCRC may, in its sole and absolute discretion, retain project data longer than two years upon written request from a project administrator.

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, lead 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 Dedoose 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. Summary of the Dedoose 7-Lock System.

- Encrypted SSL tunnel is established for communication between Dedoose client and server (SSL TLS 1.3);
- Login username/password is then encrypted in a one-way Hash (SHA-256 + per user unique salt) and transmitted across the SSL tunnel;
- Security and access privileges are set by each Dedoose account owner/project administrator on a per-project basis, via the Security Center. The Security Center allows project administrators to control exactly which information a user is allowed to view, create, edit, or delete;
- The Dedoose Data Center follows SAS 70 Type II, ISO27001, NIST800-53, HIPAA, PCI-DSS compliancy;
- Daily backups are encrypted with SSL AES-256 and transferred to the Amazon S3 Storage system and the Microsoft Azure blob storage for redundancy;
- Server login is accessible only by a private VPN connection with its own SSL tunnel and separate authentication; and
- Server login is protected by windows secure login authentication which uses an AES encryption algorithm.

21. 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 other 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 644 36th Street Manhattan Beach, CA 90266; By Phone: (866) 680-2928; By Fax: (866) 580-3837; or By Email: support@dedoose.com (mailto:support@dedoose.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 Privacy Shield. SCRC remains strongly committed to protecting PII as exhaustively described in the Parties' agreements and counterparts, including by the Dedoose 7-Lock System as summarized in the Online Privacy Policy, Paragraph 18.

22. GDPR and Data Privacy Network.

SCRC complies with 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) 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. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. SCRC has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. 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/

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, SCRC commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF.

In compliance with the GDPR and 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 644 36th Street Manhattan Beach, California 90266 USA.

22.1. 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 Privacy Shield.

22.2. How we use Your personal data.

See Paragraph 6, including subparts 6.1 to 6.14.

22.3. Providing Your personal data to others.

See Paragraph 7.

22.4. 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.

22.5. 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.

22.6. 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://dedoose.com/resources/terms (https://dedoose.com/resources/terms). We will notify You of significant changes to this policy by email.

22.7. 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 are entitled to consult with Your own attorney, at Your own expense, concerning such rights.

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.

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.

22.8. Cookie Policy.

See Para. 14 and subparts 14.1. to 14.4.

22.9. Contacting Us.

This website <dedoose.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 644 36th Street, Manhattan Beach, CA, 90266 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.

22.10. Data Protection Officer.

Contact Information: SCRC's data protection officer can be reach can be reached as follows: Jason Taylor (jtaylor@dedoose.com) SocioCultural Research Consultants, LLC 644 36th Street, Manhattan Beach, CA, 90266 USA.

22.11. Data Communication Security.

See Paragraph 15, "Data Communication Security."

22.12. Data Storage Security.

See Paragraph 16, "Data Storage Security."

22.13. Data Retention.

See Paragraph 17, "Data Retention."

22.14. Privacy Protection.

See Paragraph 18, "Privacy Protection."