TERMS OF SERVICE

Rules and Protections for Your Personal and Dedoose Data

Last Updated: 5/24/2023 Rules and Protections for Your Personal and Dedoose Data

Please Read This Document and Its Counterparts Carefully

By using this website and application, You agree to the following terms and conditions. If You do not agree, You should not use this application or any services contained on, in, or downloaded from this website or The App. These terms and conditions may be changed or updated from time to time. This document entitled "TERMS OF SERVICE: RULES AND PROTECTIONS FOR YOUR PERSONAL AND DEDOOSE DATA" ("Agreement") constitutes a valid and lawful written agreement entered into by and between (i) You, the individual using Dedoose; and (ii) SocioCultural Research Consultants, LLC ("SCRC" or "Company") as of the date You started using the Software. This Agreement is effective December 1, 2006, modified periodically, and may be subject to change without notice or by posting notice at: https://dedoose.com/resources/terms "You" and "Your" refers to the individual accessing or using SCRC's software known as Dedoose ("Software"), and the company or entity on whose behalf you purport to use the Software, and each of them. "SCRC" or "Company" refers to SocioCultural Research Consultants, LLC. "Software" refers to SCRC's software known as Dedoose. The parties acknowledge the Software is exclusively owned by SCRC. You and SCRC and collectively referred to as the "Parties" or each as "Party" in reference to each party's status in connection with this Agreement.

Recitals

1. You desire to use SCRC's Dedoose Software in connection with research; and
2. SCRC desires compensation in return for providing Dedoose to You for research services via its Software; and
3. the Parties understand and agree that such the Software is and shall continue to be sole and proprietary intellectual property of Dedoose.

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

1. Agreement and Counterparts

You fully acknowledge that you have read, understand and agree to the following counterparts which are incorporated herein by reference:

1. Online Privacy Policy; and
2. End User License Agreement, Terms of Use, End User License Agreement, Disclaimer, and Release of Liability.

2. **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.

3. Retroactivity

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

4. **Notice Re: IP Infringement Disclosure to SCRC**

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:

1. an electronic or physical signature of the person authorized to act on behalf of the owner of the copyright or other intellectual property interest;
2. a description of the copyrighted work or other intellectual property that You claim has been infringed;
3. a description of where the material that You claim is infringing is located on the site;
4. Your full name, alternative names used, address, telephone number, and email address;
5. 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
6. 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.

5. **How To Obtain A License**

If You seek permission to use SCRC trademarks, service marks, trade dress, slogans, screenshots, copyrighted designs, or other brand features, please contact SCRC.

6. **Notice re: Copyright Agent**

The SCRC Copyright Agent, to whom notice of claims of copyright or other intellectual property infringement can be directed, may be reached as follows:By Mail: Eli Lieber c/o SocioCultural Research Consultants, LLC 644 36th Street Manhattan Beach, CA 90266 By Phone: (866) 680-2928 By Fax: (866) 580-3837 By Email: support@dedoose.com

SocioCultural Research Consultants, LLC's 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.

1. Introduction

SocioCultural Research Consultants, LLC ("SCRC") is committed to safeguarding the privacy of our website and The App visitors and service users.

The following Policy applies where we are acting as a data controller 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.

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 try to protect any Personally Identifiable Information ("PII") You chose to transmit or share with SCRC. This Policy was initially made effective December 1, 2006, modified periodically, and may be subject to change with or without notice, or by posting notice at https://dedoose.com/resources/terms 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 for use of 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;
- 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 time-stamps and logs events (like features used, number of participants, etc.) This data is used for accounting/billing purposes as well as for performance and optimization of the 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.

2. Retention and Relevance

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 the End User License Agreement, Terms of Use, End User License Agreement, Disclaimer, and Release of Liability or Terms of Service.

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. 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. 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.

Back to Top

6. General; Definitions

1. 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.
2. 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.
3. In this policy, "we", "us" and "our" refer to SCRC. For more information about us, see Section 13.
4. SCRC is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).
5. There exists the possibility, under certain conditions, for the individual to invoke binding arbitration when other dispute resolution procedures have been exhausted.
6. 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.
7. SCRC acknowledges the potential liability in cases of onward transfers to third parties of personal data of EU individuals received pursuant to Privacy Shield.
8. Project data are data uploaded and belonging to a project in Dedoose.

7. How We Use Your Personal Data

This Paragraph sets forth:

the general categories of personal data that we may process;

- the general categories of personal data that we may process;
- in the case of personal data that we did not obtain directly from You, the source and specific categories of that data;

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

1. 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.
2. 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.
3. 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.
4. 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.
5. 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. 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.

7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. In addition to the specific purposes for which we may process Your personal data set out in this Section 3, 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.
14. Please do not supply any other person's personal data to us, unless we prompt You to do so.

8. Providing Your personal data to others

1. 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.
2. 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.
3. Financial transactions relating to our website and services (The App) are OR may be handled by our payment services providers, [authorize]. 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
4. In addition to the specific disclosures of personal data set out in this Section 4, 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.
5. SCRC acknowledges the potential liability in cases of onward transfers to third parties of personal data of EU individuals received pursuant to Privacy Shield.

9. International transfers of Your personal data

1. In this Section 4, we provide information about the circumstances in which Your personal data may be transferred to countries outside the European Economic Area (EEA).
2. 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.

10. Retaining and deleting personal data

1. This Section 5 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.
2. 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.
3. We will retain Your personal data as follows:
    1. *Personal Data* will be retained for a minimum period of *6 months* following the *users termination of services,* and for a maximum period of *24 months* following the *users termination of services.*

2. *Project-Related Data* will be retained for a minimum period of *6 months* following the *users termination of services,* and for a maximum period of *24 months* following *the users termination of services.*

4. 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:
    1. the period of retention of *Personal Data* will be determined based on *the same 6 month principle described in 6.C.*
5. Notwithstanding the other provisions of this Section 6, 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.

11. Amendments

1. We may update this policy from time to time by publishing a new version on our website and/or The App.
2. You should check this page occasionally to ensure You are happy with any changes to this policy.
3. We will notify You of significant changes to this policy by email.

12. Your rights

1. 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.
2. Your principal rights under data protection law are:
    1. the right to access;
    2. the right to rectification;
    3. the right to erasure;
    4. the right to restrict processing;
    5. the right to object to processing;
    6. the right to data portability;
    7. the right to complain to a supervisory authority; and
    8. the right to withdraw consent.
3. 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.

4. 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.
5. 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:
    1. for exercising the right of freedom of expression and information;
    2. for compliance with a legal obligation; or
    3. for the establishment, exercise or defense of legal claims.
6. In some circumstances You have the right to restrict the processing of Your personal data. Those circumstances are: 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.
7. 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.
8. 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.
9. 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.
10. To the extent that the legal basis for our processing of Your personal data is:
    1. consent; or
    2. 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

3. 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.

11. 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.
12. 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.
13. You may exercise any of Your rights in relation to Your personal data by written notice to us OR via phone.

13. 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:

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

14. 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*.

15. Cookies Policy

a) 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 either "persistent" cookies 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.

b) Cookies that we use: We use cookies for the following purposes:

1. 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
2. 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);
3. 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);
4. 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*);

c) Cookies used by our service providers

1. Our service providers use cookies and those cookies may be stored on Your computer when You visit our website and/or The App.
2. 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 are: *identification cookies*.

d) 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. 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.

16. Data Communication Security

All data communication through SCRC occurs through a 2-lock system. First, SCRC 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, SCRC employs a one-way, non-reversible encryption algorithm known as SHA-2 (Secure Hash Algorithm)—designed by the United States National Security Agency. SCRC 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 SCRC client sends to the server for authentication.

17. Data Storage Security

SCRC 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 Admin team.

18. Data Retention

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 describes SCRC's data retention policy for Dedoose:

1. SCRC will retain data for two years after the expiration of all user logins;
2. Authorized users can regain access to project data during this two-year period by providing a specific written request to SCRC. Such request should be sent to: support@dedoose.com
3. Authorized users can delete project data via the Dedoose App user interface.
4. Upon specific written request from the project administrator, SCRC will permanently delete all project data **BEFORE** the two-year period;
5. 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 tapes; and
6. SCRC may, in its sole and absolute discretion, retain project data longer than two-years upon written request from a project administrator.

19. Privacy Protection

SCRC provides industry standard protection for personally identifying information. SCRC would only disclose personally identifiable information about users or information about Your project to third parties in limited circumstances: (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 court 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.

Data Retention and Sharing:

SCRC strongly believes Your data is Your data. SCRC promises not to share Your data with any 3rd parties and allows You to export all of Your data at any time. Our system naturally deletes all project data after 2 years of no active subscription associated with the 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 and we will happily oblige.

Privacy Protection:

SCRC provides industry standard protection for personally identifying information. SCRC would only disclose personally identifiable information about users or information about Your project to third parties in limited circumstances: (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 ou challenge the disclosure request, we may still be legally required to turn over the personally identifying information and/or project data.

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

1. Encrypted SSL tunnel is established for communication between Dedoose client and server (SSL TLS 1.3);
2. Login username/password is then encrypted in a one-way Hash (SHA-256 + per user unique salt) and transmitted across the SSL tunnel;
3. 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;
4. The Dedoose Data Center follows SAS 70 Type II, ISO27001, NIST800-53, HIPAA, PCI-DSS compliancy;
5. Daily backups are encrypted with SSL AES-256 and transferred to the Amazon S3 Storage system and the Microsoft Azure blob storage for redundancy;
6. Server login is accessible only by a private VPN connection with its own SSL tunnel and separate authentication; and
7. Server login is protected by windows secure login authentication which uses an AES encryption algorithm.

21. GDPR and Privacy Shield Compliance Policy

Updated: 9/19/2022

For all users subject to the GDPR, the following applies:

GDPR: SocioCultural Research Consultants, LLC complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. SocioCultural Research Consultants, LLC hereby certifies, including to the U.S. Department of Commerce, that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/

In compliance with the GDPR principals and Privacy Shield 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

SCRC has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved GDPR or Privacy Shield complaints concerning data transferred from the EU and Switzerland.

SocioCultural Research Consultants, LLC's

Terms of Use, End User License Agreement, Disclaimer, and Release of Liability

This is a further 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. ***Please Read This Document Carefully***

By using this website and application, You agree to these terms and conditions. If You do not agree, You should not use this application or any services contained on, in, or downloaded from this website or The App. These terms and conditions may be changed or updated from time to time.

This Terms of Use, End User License Agreement, Disclaimer, and Release of Liability ("the Agreement") is a legal agreement between You and SCRC for use of this website or The App and any applications or programs contained on, in, or downloaded from this website or The App. Such applications include, but are not limited to Dedoose, applications, services, solutions, compilations, reports, summaries, other documents, computer software, and associated media and printed materials generated from use of this website or The App (hereinafter collectively referred to as "the App").

1. Restricted Use of this Product and Disclaimer

The Software is designed exclusively for customers of SCRC who have properly subscribed to this service and been specifically authorized in writing by SCRC to access and use the website and the App. THE MATERIALS, INFORMATION, AND DOCUMENTS CONTAINED IN THE SOFTWARE ARE SOLELY APPLICABLE TO THE AUTHORIZED USERS HOLDING AN APPROVED PASSWORD.

2. Software Product License; Limitations

The Software is protected by copyright laws, as well as other intellectual property laws. The Software is licensed, not sold. You may view and use the Software on the terms and conditions specified herein. You may not store, copy, replicate, or otherwise save any portion of the Software. You may not reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software. The Software is licensed as a single product. Its component parts may not be separated for use on more than one computer. You may not rent, sub-license, or lease the Software. You may not transfer the Software or any rights You may have as a user under this Agreement to another person or entity.

3. Intellectual Property Rights

The following provisions shall apply with respect to copyrightable works, proprietary information, 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 holds an interest in and solely owns 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, written 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 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 the Software to any person or entity other than as contemplated in this Agreement. You agree to undertake Your best efforts to prevent transmission of usernames or passwords provided by SCRC to any person or entity except as provided in this Agreement.

4. 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.

5. Copyright

All titles and copyrights in and to the Software, the accompanying printed materials, and any copies of the Software, are owned by SCRC or its suppliers. The Software is protected by U.S. and international copyright laws. Therefore, You must treat the Software like any other copyrighted material.

6. No Warranties and Indemnification

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.

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.

7. Limitations of Liabilities

Technical or other support services, whether arising in tort (including negligence) contract or any other legal theory, even if SCRC, its affiliates, suppliers or resellers have been advised of the possibility of such damages. In any case, SCRC, its affiliates, and suppliers’ maximum cumulative liability and Your exclusive remedy for any claims arising out of or related to this agreement will be limited to the amount actually paid by You for the Software (if any) in the previous 12 months. because some states and jurisdictions do not allow the exclusion or limitation of liability, the above limitation may not apply to You.

8. Payment

You agree that SCRC may charge to Your credit card or other payment mechanism selected by You and approved by SCRC for all amounts due and owed, including service fees, set up fees, subscription fees, overage fees, processing fees, consulting fees or any other fee or charge associated with Your use of the Software or other SCRC services. SCRC may change prices at any time without prior notice. You agree that in the event SCRC is unable to collect the fees owed to SCRC, SCRC may take any other steps it deems necessary to collect such fees and that You will be responsible for all costs and expenses incurred by SCRC in connection with such collection activity,

including collection fees, court costs and attorneys' fees. You further agree that SCRC may collect interest at the lesser of 1.5% per month or the highest amount permitted by law on any amounts not paid when due.

9. Termination By Customer

You may terminate this Agreement by providing written notice to SCRC via email to support@dedoose.com Such termination will be effective on the last day of the billing cycle, subject to (30) days prior written notice.

10. Export Restriction

You acknowledge that the Software, or portion thereof may be subject to the export control laws of the United States. You will not export, re-export, divert, transfer or disclose any portion of the Software or any related technical information or materials, directly or indirectly, in violation of any applicable export law or regulation.

11. Injunctive Relief

You acknowledge that any use of the Software contrary to this Agreement, or any transfer, sublicensing, copying or disclosure of technical information or materials related to the Software, may cause irreparable injury to SCRC, its affiliates, suppliers and any other party authorized by SCRC to resell, distribute, or promote the Software, and under such circumstances SCRC will be entitled to equitable relief, without posting bond or other security, including, but not limited to, preliminary and permanent injunctive relief.

12. Choice of Law and Forum

This Agreement shall be governed by and construed under the laws of the State of California, United States of America without regard to conflicts of laws. The Parties agree that any and all disputes will be resolved exclusively under the jurisdiction and venue of federal or state courts located in and serving the appropriate state county or federal district covering Los Angeles, California. Any and all disputes will be resolved solely in the English language.

13. Waiver and Severability

Failure by either party to exercise any of its rights under, or to enforce any provision of, this Agreement will not be deemed a waiver or forfeiture of such rights or ability to enforce such provision. If any provision of this Agreement is held by a court of competent jurisdiction to be illegal, invalid or unenforceable, that provision will be amended to achieve as nearly as possible the same economic effect of the original provision and the remainder of this Agreement will remain in full force and effect.

14. Entire Agreement

This Agreement embodies the entire understanding and agreement between the parties respecting the subject matter of this Agreement and supersedes any and all prior understandings and agreements between the parties respecting such subject matter. SCRC may change the terms of

this Agreement at any time by posting modified terms on its website and/or via the Software. This Agreement has been prepared in the English Language and such version shall be controlling in all respects and any non-English version of this Agreement is solely for accommodation purposes and will not control as to the construction or intent of the parties to this Agreement. All notices or other correspondence to SCRC under this Agreement must be sent to the address provided hereinabove, support@dedoose.com, or other address as provided by SCRC for such purpose. Any and all rights and remedies of SCRC upon Your breach or other default under this Agreement will be deemed cumulative and not exclusive of any other right or remedy conferred by this Agreement or by law or equity on SCRC, and the exercise of any one remedy will not preclude the exercise of any other. The captions and headings appearing in this Agreement are for reference only and will not be considered in construing this Agreement.

15. Responsibility for Content of Your Communications

You agree that You are solely responsible for the content of all visual, written or audible communications sent by You and You will not use this website or The App to send unsolicited commercial email outside Your company or organization in violation of applicable law. You further agree not to use this website or The App to communicate any message or material that is harassing, libelous, threatening, obscene, indecent, or would violate the intellectual property rights of any party or is otherwise unlawful, that would give rise to civil liability, or that constitutes or encourages conduct that could constitute a criminal offense, under any applicable law or regulation or that violates Your agreed upon responsibilities to other entities including Institutional Review Boards, COPPA, or HIPAA. You also agree that SCRC may delete any such communications in its sole and absolute discretion without notice.

16. Termination By SCRC

Without prejudice to any other rights, SCRC may terminate this Agreement if You fail to comply with any of the terms or conditions of this Agreement. You have been, or will be, provided with a username and password. You are not allowed, under any circumstances to share Your username and password with any other person or entity. Doing so terminates any rights You have under this Agreement. 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 SCRC 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 SCRC resulting from such acquisition and use after the Account Administrator is provided the administrative password by SCRC .

17. Assignment

SCRC shall have the right to assign this Agreement in its entirety and the right to change or reassign various duties regarding the operation and performance of any duties imposed by this Agreement.

18. Force Majeure

Inability or delay in providing access to the Software resulting from cause beyond the control of SCRC, including but not limited to interruption of communication lines, labor disputes, acts of

terrorism, government action or order, laws, or natural disaster, or war shall not constitute a breach of contract and the parties hereto agree to resolve any resulting issues by mutual agreement, including, without limitation an extension of service, additional service or credit on a pro rata basis.

19. Compliance with Law

Each of the parties to this Agreement shall exert every reasonable effort in the performance of their respective obligations hereunder to comply with all applicable municipal, county, state and federal laws, ordinances and regulations.

20. Copyright Notice; Reservation of Rights

The Dedoose Software is protected by copyright law. Notice is given as follows: **Copyright © 2006-2022SocioCultural Research Consultants, LLC**. All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form or by any means, electric or mechanical, including photocopying, recording, and broadcasting, or by any information storage and retrieval system, without permission in writing from SCRC. Dedoose, www.Dedoose.com, Dedoose logos, Dedoose Logos, Dedoose Seal(s), are registered trademarks of SCRC, subject to rights as asserted in the United States, in California or other states, and/or other jurisdictions outside the United States as applicable. All other trademarks referenced are the trademark, service mark, or registered trademark of the respective holders. The Software and technology used to implement the Software contain trade secrets that SCRCconsiders to be confidential and proprietary information, and Your right to use this material is subject to the restrictions in this Agreement under which You obtained it.

21. Disclaimer

DISCLAIMER: COMPANIES, NAMES, PRODUCTS AND DATA USED IN THE EXAMPLES ILLUSTRATING SCRC PRODUCTS AND DEDOOSE, AND IN THE TRAINING MATERIALS AND DEMONSTRATIONS OF SCRC ARE FICTITIOUS. ANY RESEMBLANCE TO EXISTING COMPANIES, PERSONS, OR PRODUCTS IS COINCIDENTAL AND UNINTENTIONAL.

SocioCultural Research Consultant, LLC Online Privacy Policy

Introduction

SocioCultural Research Consultants, LLC (“SCRC”) respects your privacy and the privacy of others. 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 online privacy policy describes how we use and try to protect any Personally Identifiable Information (“PII”) you chose to transmit or share with SCRC. This policy is effective December 1, 2006 and may be subject to change without notice. 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 for use of 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;
- 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 time-stamps and logs events (like features used, number of participants, etc.) This data is used for accounting/billing purposes as well as for performance and optimization of the 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.

Retention and Relevance

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

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 the SCRC End User License Agreement or Terms of Service

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. 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. 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.

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.

Back to Top

SocioCultural Research Consultants, LLC End User License Agreement

Terms of Use, End User License Agreement, Disclaimer, and Release of Liability

Please Read This Document Carefully

By using this website and application, you agree to these terms and conditions. If you do not agree, you should not use this application or any services contained on, in, or downloaded from this website or The App. These terms and conditions may be changed or updated from time to time.

This Terms of Use, End User License Agreement, Disclaimer, and Release of Liability ("the Agreement") is a legal agreement between you and Dedoose for use of this website or The App and

any applications or programs contained on, in, or downloaded from this website or The App. Such applications include, but are not limited to Dedoose, applications, services, solutions, compilations, reports, summaries, other documents, computer software, and associated media and printed materials generated from use of this website or The App (hereinafter collectively referred to as “the App”).

1. Restricted Use of this Product and Disclaimer

The Software is designed exclusively for customers of Dedoose who have properly subscribed to this service and been specifically authorized in writing by Dedoose to access and use the website and the App. THE MATERIALS, INFORMATION, AND DOCUMENTS CONTAINED IN THE SOFTWARE ARE SOLELY APPLICABLE TO THE AUTHORIZED USERS HOLDING AN APPROVED PASSWORD.

2. Software Product License

The Software is protected by copyright laws, as well as other intellectual property laws. The Software is licensed, not sold. You may view and use the Software on the terms and conditions specified herein. You may not store, copy, replicate, or otherwise save any portion of the Software. You may not reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software. The Software is licensed as a single product. Its component parts may not be separated for use on more than one computer. You may not rent, sub-license, or lease the Software. You may not transfer the Software or any rights you may have as a user under this Agreement to another person or entity.

3. 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”).

Dedoose personally holds an interest in and solely owns 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 Dedoose 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 Dedoose (or its employees or agents,) during the term of this Agreement shall be the sole and exclusive property of Dedoose. 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. Dedoose grants you a non-exclusive, written license to use Dedoose’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 patents, trademarks, service marks, ownership interests, or copyrights that Dedoose has in the Software.

You agree that you will not distribute the Intellectual Property or software of Dedoose contained in the Software to any person or entity other than as contemplated in this Agreement. You agree to

undertake your best efforts to prevent transmission of usernames or passwords provided by Dedoose to any person or entity except as provided in this Agreement.

4. Title and Protection

All rights, title, and interest in and to the Software are and shall remain at all times the property of Dedoose and/or Dedoose's suppliers. You agree to take all reasonable steps to protect the Intellectual Property rights of Dedoose, 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 Dedoose.

5. Copyright

All titles and copyrights in and to the Software, the accompanying printed materials, and any copies of the Software, are owned by SCRC or its suppliers. The Software is protected by U.S. and international copyright laws. Therefore, you must treat the Software like any other copyrighted material.

6. No Warranties and Indemnification

You understand and agree that the software and website are provided "AS IS" and Dedoose, 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. Dedoose, 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.

You agree to indemnify, defend and hold harmless Dedoose, 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.

7. Limitations of Liabilities

Technical or other support services, whether arising in tort (including negligence) contract or any other legal theory, even if Dedoose, its affiliates, suppliers or resellers have been advised of the possibility of such damages. in any case, Dedoose, its affiliates', and suppliers' maximum cumulative liability and your exclusive remedy for any claims arising out of or related to this agreement will be limited to the amount actually paid by you for the software (if any) in the previous 12 months.

because some states and jurisdictions do not allow the exclusion or limitation of liability, the above limitation may not apply to you.

Data Retention and Sharing:

Dedoose strongly believes your data is your data. Dedoose promises not to share your data with any 3rd parties, and allows you to export all of your data at any time. Our system naturally deletes all project data after 2 years of no active subscription associated with the 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 and we will happily oblige.

Privacy Protection:

Dedoose provides industry standard protection for personally identifying information. Dedoose would only disclose personally identifiable information about users or information about your project to third parties in limited circumstances: (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 Dedoose is required by law to disclose personally identifying or project data, Dedoose 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.

Data Breach Notification and Incident Response Plan:

Dedoose hosts all data within the continental U.S. unless agreed upon and determined as needed on a project-by-project basis. Dedoose has a systematic plan for response and notification of any breach in data security. Upon the detection of any breach in data security, Dedoose technical staff, led by the Dedoose Chief Technical Officer, will immediately assess the size, scope, and severity of the breach. Following this assessment, Dedoose 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, Dedoose 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.

Dedoose 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 Dedoose 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.

8. GDPR and Privacy Shield Compliance:

updated 2/27/2022

Dedoose complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. Dedoose has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern.

To learn more about the Privacy Shield program, and to view our certification, please visithttps://www.privacyshield.gov/list

In compliance with the GDPR principals and Privacy Shield Principles, Dedoose 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 Dedoose at:

Dedoose 644 36th Street Manhattan Beach, California 90266

Dedoose has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved GDPR or Privacy Shield complaints concerning data transferred from the EU and Switzerland.

1. **Introduction**

1. 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 controller 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.

1. **Introduction**
    1. We are committed to safeguarding the privacy of our website and The App visitors and service users.
    2. This policy applies where we are acting as a data controller 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.
    3. 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.
    4. 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.
    5. In this policy, "we", "us" and "our" refer to Dedoose. For more information about us, see Section 13.
    6. Dedoose is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).
    7. There exists the possibility, under certain conditions, for the individual to invoke binding arbitration when other dispute resolution procedures have been exhausted.
    8. Dedoose 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.
    9. Dedoose acknowledges the potential liability in cases of onward transfers to third parties of personal data of EU individuals received pursuant to Privacy Shield.
2. **How we use your personal data**

1. In this Section 3 we have set out:
    1. the general categories of personal data that we may process;
    2. in the case of personal data that we did not obtain directly from you, the source and specific categories of that data;
    3. the purposes for which we may process personal data; and
    4. the legal bases of the processing.
2. 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.
3. 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 Dedoose and/or taking steps, at your request, to enter into such a contract, OR on an as-needed legal basis.
4. 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 Dedoose and/or taking steps, at your request, to enter into such a contract, OR on an as-needed legal basis.
5. 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 Dedoose and/or taking steps, at your request, to enter into such a contract, OR on an as-needed legal basis.
6. 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 Dedoose and/or taking steps, at your request, to enter into such a contract, OR on an as-needed legal basis.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.
14. In addition to the specific purposes for which we may process your personal data set out in this Section 3, 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.
15. Please do not supply any other person's personal data to us, unless we prompt you to do so.

3. **Providing your personal data to others**

    1. 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.
    2. 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.
    3. Financial transactions relating to our website and services (The App) are OR may be handled by our payment services providers, [authorize]. 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
    4. In addition to the specific disclosures of personal data set out in this Section 4, 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.
    5. Dedoose acknowledges the potential liability in cases of onward transfers to third parties of personal data of EU individuals received pursuant to Privacy Shield.

4. **International transfers of your personal data**

    1. In this Section 5, we provide information about the circumstances in which your personal data may be transferred to countries outside the European Economic Area (EEA).
    2. 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.

5. **Retaining and deleting personal data**

    1. This Section 6 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.
    2. 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.
    3. We will retain your personal data as follows:
        1. *Personal Data* will be retained for a minimum period of *6 months* following the

           users termination of services, and for a maximum period of *24 months* following the *users termination of services.*
        2. *Project-Related Data* will be retained for a minimum period of *6 months* following the *users termination of services,* and for a maximum period of *24 months* following *the users termination of services.*
    4. 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:
        1. the period of retention of *Personal Data* will be determined based on

           the same 6 month principle described in 6.C.
    5. Notwithstanding the other provisions of this Section 6, 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.

6. **Amendments**

    1. We may update this policy from time to time by publishing a new version on our website and/or The App.
    2. You should check this page occasionally to ensure you are happy with any changes to this policy.
    3. We will notify you of significant changes to this policy by email.

7. **Your rights**

    1. In this Section 8, we have summarized the rights that 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.
    2. Your principal rights under data protection law are:
        1. the right to access;
        2. the right to rectification;
        3. the right to erasure;
        4. the right to restrict processing;

5. the right to object to processing;
6. the right to data portability;
7. the right to complain to a supervisory authority; and
8. the right to withdraw consent.

3. 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.
4. 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.
5. 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: 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.
6. In some circumstances you have the right to restrict the processing of your personal data. Those circumstances are: 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.
7. 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.

8. 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.
9. 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.
10. To the extent that the legal basis for our processing of your personal data is:
    1. consent; or
    2. 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,
    3. 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.
11. 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.
12. 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.
13. You may exercise any of your rights in relation to your personal data by written notice to us OR via phone.

8. **About cookies**
    1. 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.
    2. Cookies may be either "persistent" cookies 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.
    3. 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.
9. **Cookies that we use**
    1. We use cookies for the following purposes:
        1. 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

2. 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);
3. 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);
4. 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*);

10. **Cookies used by our service providers**
    1. Our service providers use cookies and those cookies may be stored on your computer when you visit our website and/or The App.
    2. 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 are: *identification cookies*.
11. **Managing cookies**
    1. 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.
    2. Blocking all cookies will have a negative impact upon the usability of many websites as well as The App.
    3. If you block cookies, you will not be able to use all the features on our website or The App.
12. **Our details**
    1. This website and services (The App) is owned and operated by *Dedoose*.
    2. Our principal place of business is at: *644 36th Street, Manhattan Beach, CA, 90266, United States.*
    3. You can contact us:
        1. by post, to the postal address given above;
        2. using our website contact form;
        3. by telephone, on the contact number published on our website and/or The App from time to time; or
        4. by email, using the email address published on our website and/or The App from time to time.
13. **Data protection officer**

1. Our data protection officer contact details are: Jason Taylor (jtaylor@dedoose.com), *644 36th Street, Manhattan Beach, CA, 90266, United States*.

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 client sends to the server for authentication.

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 Dedoose Admin team.

Data Retention:

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:

1. SCRC will retain data for two years after the expiration of all user logins
2. Authorized users can regain access to project data during this two-year period by providing a specific written request to SCRC. Such request should be sent to:

   support@dedoose.com
3. Upon specific written request from the project administrator, SCRC will permanently delete all project data **BEFORE** the two-year period
4. 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 tapes
5. SCRC may, in its sole and absolute discretion, retain project data longer than two-years upon written request from a project administrator.

Privacy Protection:

SCRC provides industry standard protection for personally identifying information. SCRC would only disclose personally identifiable information about users or information about your project to third parties in limited circumstances: (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.

Summary of the Dedoose 7-lock system:

1. Encrypted SSL tunnel is established for communication between Dedoose client and server (SSL TLS 1.3)
2. Login username/password is then encrypted in a one-way Hash (SHA-256 + per user unique salt) and transmitted across the SSL tunnel
3. 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
4. The Dedoose Data Center follows SAS 70 Type II, ISO27001, NIST800-53, HIPAA, PCI-DSS compliancy.
5. Daily backups are encrypted with SSL AES-256 and transferred to the Amazon S3 Storage system and the Microsoft Azure blob storage for redundancy
6. Server login is accessible only by a private VPN connection with its own SSL tunnel and separate authentication
7. Server login is protected by windows secure login authentication which uses an AES encryption algorithm.

9. Charges

You agree that Dedoose may charge to your credit card or other payment mechanism selected by you and approved by Dedoose for all amounts due and owed, including service fees, set up fees, subscription fees, overage fees, consulting fees or any other fee or charge associated with your use of the Software or other Dedoose services. Dedoose may change prices at any time without prior notice. You agree that in the event Dedoose is unable to collect the fees owed to Dedoose , Dedoose may take any other steps it deems necessary to collect such fees and that you will be responsible for all costs and expenses incurred by Dedoose in connection with such collection activity, including collection fees, court costs and attorneys' fees. You further agree that Dedoose may collect interest at the lesser of 1.5% per month or the highest amount permitted by law on any amounts not paid when due.

10. Termination By Customer

You may terminate this Agreement by providing written notice to Dedoose via email to support@dedoose.com Such termination will be effective on the last day of the billing cycle, subject to (30) days prior written notice.

11. Export Restriction

You acknowledge that the Software, or portion thereof may be subject to the export control laws of the United States. You will not export, re-export, divert, transfer or disclose any portion of the Software or any related technical information or materials, directly or indirectly, in violation of any applicable export law or regulation.

12. Injunctive Relief

You acknowledge that any use of the Software contrary to this Agreement, or any transfer, sublicensing, copying or disclosure of technical information or materials related to the Software, may cause irreparable injury to Dedoose , its affiliates, suppliers and any other party authorized by Dedoose to resell, distribute, or promote the Software, and under such circumstances Dedoose will be entitled to equitable relief, without posting bond or other security, including, but not limited to, preliminary and permanent injunctive relief.

13. Choice of Law and Forum

This Agreement shall be governed by and construed under the laws of the State of California, U.S.A., as to the exclusive jurisdiction and venue of the courts located in and serving Los Angeles, California.

14. Waiver and Severability

Failure by either party to exercise any of its rights under, or to enforce any provision of, this Agreement will not be deemed a waiver or forfeiture of such rights or ability to enforce such provision. If any provision of this Agreement is held by a court of competent jurisdiction to be illegal, invalid or unenforceable, that provision will be amended to achieve as nearly as possible the same economic effect of the original provision and the remainder of this Agreement will remain in full force and effect.

15. Entire Agreement

This Agreement embodies the entire understanding and agreement between the parties respecting the subject matter of this Agreement and supersedes any and all prior understandings and agreements between the parties respecting such subject matter. Dedoose may change the terms of this Agreement at any time by posting modified terms on its website and The App. This Agreement has been prepared in the English Language and such version shall be controlling in all respects and any non-English version of this Agreement is solely for accommodation purposes. All notices or other correspondence to Dedoose under this Agreement must be sent to the address provided here support@dedoose.com above, or other address as provided by Dedoose for such purpose. Any and all rights and remedies of Dedoose upon your breach or other default under this Agreement will

be deemed cumulative and not exclusive of any other right or remedy conferred by this Agreement or by law or equity on Dedoose , and the exercise of any one remedy will not preclude the exercise of any other. The captions and headings appearing in this Agreement are for reference only and will not be considered in construing this Agreement.

16. Responsibility for Content of Your Communications

You agree that you are solely responsible for the content of all visual, written or audible communications sent by you and you will not use this website or The App to send unsolicited commercial email outside your company or organization in violation of applicable law. You further agree not to use this website or The App to communicate any message or material that is harassing, libelous, threatening, obscene, indecent, or would violate the intellectual property rights of any party or is otherwise unlawful, that would give rise to civil liability, or that constitutes or encourages conduct that could constitute a criminal offense, under any applicable law or regulation or that violates your agreed upon responsibilities to other entities including Institutional Review Boards or HIPAA. You also agree that Dedoose may delete any such communications in its sole and absolute discretion without notice.

17. Termination By Dedoose

Without prejudice to any other rights, Dedoose may terminate this Agreement if you fail to comply with any of the terms or conditions of this Agreement. You have been, or will be, provided with a username and password. You are not allowed, under any circumstances to share your username and password with any other person or entity. Doing so terminates any rights you have under this Agreement. It is the policy of Dedoose 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. Dedoose 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 by Dedoose.

18. Assignment

Dedoose shall have the right to assign this Agreement in its entirety and the right to change or reassign various duties regarding the operation and performance of any duties imposed by this Agreement.

19. Force Majeure

Inability or delay in providing access to the Software resulting from cause beyond the control of Dedoose , including but not limited to interruption of communication lines, labor disputes, acts of terrorism, government action or order, laws, or natural disaster, or war shall not constitute a breach of contract and the parties hereto agree to resolve any resulting issues by mutual agreement, including, without limitation an extension of service, additional service or credit on a pro rata basis.

20. Compliance with Law

Each of the parties to this Agreement shall exert every reasonable effort in the performance of their respective obligations hereunder to comply with all applicable municipal, county, state and federal laws, ordinances and regulations.

21. Reservation of Rights