Privacy Policy of ReverbReports.com

Last Updated: January 16, 2024

1. Introduction

Welcome to ReverbReports.com, a knowledge and productivity platform for Testing Psychologists. This Privacy Policy outlines our practices concerning the collection, use, and protection of your personal data.

2. Data Collection

We collect and process the following types of information, including data that relates to identified or identifiable individuals ("**Personal Data**") (note, specific Personal Data elements listed in each category are only examples and may change):

Identity Data: Personal Data about you and your identity, such as your name, gender, marital status, date of birth, username, and other Personal Data you may provide on applications, registration forms, or as part of an account profile (e.g. biographical information).

Transaction Data: Personal Data we collect in connection with a transaction or purchase, such as the item you purchased, the price, the delivery location, zip code, and other similar information.

Contact Data: Personal Data used to contact an individual, e.g. email address(es), physical address(es), phone number(s), or social media or communications platform usernames/handles, as well as a name or other salutation.

Financial Data: Personal Data relating to financial accounts or services, e.g. a credit card, bank, or other financial account numbers, and other relevant information you provide in connection with a financial transaction.

Device/Network Data: Personal Data relating to your device, browser, or application e.g. IP addresses, MAC addresses, application ID/AdID/IDFA, identifiers from cookies, session navigation history and similar browsing metadata, and other data generated through applications and browsers, including cookies and similar technologies.

Location Data: Personal Data relating to your precise location, such as information collected from your device's GPS or other precise localization service.

Special Category Data: Personal Data revealing racial, national, or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, health information, or information relating to sex life or sexual orientation.

Custom Content: Custom Content: Information that a user provides in a free text or other unstructured format, or pursuant to custom fields created by a Client; this may include Personal Data or Special Category Data to the extent provided by the user.

3. Purpose of Data Collection

The purpose of data collection is primarily to enable account registration and creation. We may also use data collection for the following:

Operate our Services and Fulfill Obligations: We process any Personal Data as is necessary to provide the Services, and as otherwise necessary to fulfill our obligations to you, e.g. to provide you with the information, features, and services you request.

Personalization/Customization: We process Personal Data (excluding Special Category Data) as necessary in connection with our legitimate business interest in personalizing our Services. For example, aspects of the Services may be customized to you so that it displays your or a Client's name, to reflect appearance or display preferences, display recent or commonly used features or data, or other similar functionality.

Internal Processes and Service Improvement: We process Personal Data (excluding Special Category Data) as necessary in connection with our improvement of the design of our Services, understanding how our Services are used or function, for customer service purposes, in connection with the creation and analysis of logs and metadata relating to service use, and for ensuring the security and stability of the Services. Additionally, we may use Personal Data to understand what parts of our Service are most relevant to users, how users interact with various aspects of our Services, how our Services perform or fail to perform, etc., or we may analyze use of the Services to determine if there are specific activities that might indicate an information security risk to the Services or our Users. We also use anonymized data to improve our large language models for more accurate report writing in the future.

4. Data Storage and Security

At ReverbReports.com, we prioritize the security of your personal data. Our measures for safeguarding your information include:

- **Secure Data Transmission:** We use SSL encryption to protect your data during transmission, ensuring its confidentiality and integrity.
- **Reliable Hosting:** Our data is hosted on Microsoft Azure, a platform renowned for its robust security features. This includes compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), ensuring the highest standards of privacy and security for healthcare-related information.
- **Business Associate Agreement (BAA) with Microsoft:** We have a formal agreement with Microsoft, which outlines our mutual responsibilities under HIPAA, further enhancing the protection of your sensitive health data.
- **Enhanced Login Security:** To access our platform, we require two-factor authentication. This additional security layer helps in verifying user identities and reducing the risk of unauthorized access.

- **Database Encryption:** All data stored in our databases is encrypted, providing an additional layer of security against unauthorized access or data breaches.
- **Automatic Logout Protocol:** For added security, our system is designed to automatically log you out after 15 minutes of inactivity. This feature helps prevent unauthorized access to your data if your device is left unattended.
- **Audit Trail:** We maintain comprehensive audit logs that track all data uploads and downloads, enabling us to monitor and review data access and transfer activities for enhanced security.
- **Restricted Data Storage Locations:** Our data storage is confined to specific, secure locations: Microsoft Azure, Azure DevOps, our internal email system, and a controlled internal shared drive. This limitation helps in managing the security and integrity of your data effectively.

5. Data Sharing and Disclosure

We use multiple layers of data redaction to anonymize data with third parties, minimizing personal identifiable information (PII) exposure. When anonymization isn't feasible, we ensure HIPAA-compliant BAAs are in place with third parties that aid in providing or improving our services.

6. User Rights

Users have direct access to their data within the platform and can modify it as needed.

7. Policy Updates

We may update this policy from time to time. Users are encouraged to review this policy regularly for any changes.

8. Contact Information

For any inquiries related to privacy, please contact us at legal@ReverbReports.com.

9. Jurisdiction and Compliance

This policy is governed by US Federal Laws and adheres to GDPR and CCPA regulations.

Under the California Consumer Privacy Act ("CCPA") and other California laws, California residents may have the following rights, subject to your submission of an appropriately verified request (see below for verification requirements):

PRIVACY RIGHTS

Right to Know: You may have the right to request any of following, for the 12 month period preceding your request: (1) the categories of Personal Data we have collected about you, or that we have sold, or disclosed for a commercial purpose; (2) the categories of sources from which your Personal Data was collected; (3) the business or commercial purpose for which we collected or sold your Personal Data; (4) the categories of third parties to whom we have sold your Personal Data, or

disclosed it for a business purpose; and (5) the specific pieces of Personal Data we have collected about you.

Right to Delete: You may have the right to delete certain Personal Data that we hold about you, subject to exceptions under applicable law.

Right to Non-Discrimination: You may have the right to not to receive discriminatory treatment as a result of your exercise of any rights conferred by the CCPA.

Direct Marketing: You may request a list of Personal Data we have disclosed about you to third parties for direct marketing purposes (if any) during the preceding calendar year.

Opt-Out of Sale: If we engage in sales of Personal Data (as defined by applicable law), you may direct us to stop selling or disclosing Personal Data to third parties for commercial purposes. At this time, we do not sell Personal Data.

SUBMISSION OF RIGHTS REQUESTS

You may submit requests by contacting us (see below for summary of required verification information).

VERIFICATION OF RIGHTS REQUESTS

All rights requests must be verified to ensure that the individual making the request is authorized to make that request, to reduce fraud, and to ensure the security of your Personal Data. We may require that you provide the email address we have on file for you (and verify that you can access that email account) as well as an address, phone number, or other information we have on file, in order to verify your identity. If an agent is submitting the request on your behalf, we reserve the right to validate the agent's authority to act on your behalf.

10. Cookies and Tracking Technologies

Our application may use cookies or similar technologies to enhance and personalize the user experience.

We, and certain third parties, may process Device/Network Data when you interact with cookies and similar technologies. We may receive this data from third parties to the extent allowed by the applicable partner. Please note that the privacy policies of third parties may apply to these technologies and information collected.

In connection with our legitimate interests in providing and improving the user experience and efficiency of our Services, and understanding information about the devices and demographics of visitors to our Services, we use this information (i) for "essential" or "functional" purposes, such as to enable various features of the Services such as your browser remembering your username or password, maintaining a session, or staying logged in after a session has ended; (ii) for analytics and site performance purposes, such as tracking how the Services are used or perform, how users engage with and navigate through the Services, what sites users visit before visiting our Services,

how often they visit our Services, and other similar information; and (iii) for the purpose of displaying advertisements via retargeting to those users who visited our Site or who may be interested in our Service.

Some of these technologies can be used by third parties to identify you across platforms, devices, sites, and services. Clients may also have access to information, such as reports and analytics, generated through these services.

11. Age Restriction

Users must be 16 years of age or older to use our services.

Our Services are intended for use by Users and Clients and are neither directed at nor intended for direct use by individuals under the age of 16. Further, we do not knowingly collect Personal Data directly from such individuals. If we learn that we have inadvertently done so, we will promptly delete it. Do not access or use the Services if you are not of the age of majority in your jurisdiction unless you have the consent of your parent or guardian.

12. International Data Transfer

We do not transfer your data internationally, ensuring compliance with local data protection laws.

13. Data Retention

Personal Data is retained as long as it remains relevant to its intended purpose, or as required by law. If processing data on behalf of Clients, we adhere to their specified retention periods or delete data upon their request. Retention periods are periodically reviewed, with potential pseudonymization or anonymization of data held for extended durations.

14. User Consent

Following notice to you or your acknowledgment of this Privacy Policy (including any updates), your continued use of any of our Services indicates your consent to the practices described in this Policy

This Policy is incorporated into the Master License Agreement governing your use of any of our Services. Any capitalized terms not defined in this Privacy Policy will have the definitions provided in our Master License Agreement.

Following notice to you or your acknowledgment of this Privacy Policy (including any updates), your continued use of any of our Services indicates your consent to the practices described in this Policy.