# Security & Privacy Overview

## Introduction

At Recollective, we prioritize the security and privacy of your valuable research data. We use a multi-layered approach with rigorous cybersecurity measures, SOC 2 compliance, and adherence to global privacy regulations like GDPR. This document offers a comprehensive look at how we protect your sensitive information, from our secure cloud infrastructure and proactive security measures to our strict data protection protocols and user authentication procedures. Our goal is to provide a transparent and trustworthy platform for all your research needs.

The following overview relates to all Recollective offerings, including Recollective Qual and Recollective Connect. Additional information about Recollective's security and privacy practices, including our current SOC 2 report, is available in the Recollective Trust Center. Please visit trust.recollective.com to request access.

## Cyber Security and SOC 2 Compliance

Recollective is committed to maintaining the highest standards of security and privacy through a robust cybersecurity program and adherence to SOC 2 compliance. This integrated approach ensures the protection, availability, and confidentiality of our services and customer data.

### SOC 2 Compliance

Recollective is proud to be SOC 2 Type 2 compliant. SOC 2 (System and Organization Controls 2) is a set of standards designed to help service organizations manage customer data. Achieving SOC 2 compliance provides independent validation of our controls and processes, offering assurance that we are following best practices in data protection and information security. Customers may request a copy of our SOC 2 Type 2 compliance report which is available in our Trust Center (trust.recollective.com).

### Cyber Security Program

Recollective's cybersecurity and information security program includes administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of confidential information and our Information Systems.

## Key Components

- **Risk Assessment:** Identification and assessment of internal and external cybersecurity risks that may threaten the security or integrity of confidential information.
- **Defensive Infrastructure:** Implementing policies and procedures to protect information systems and data from unauthorized access, use, or other malicious acts.
- **Incident Detection and Response:** Procedures to detect cybersecurity events, mitigate negative effects, and promptly restore normal operations and services.
- **Data Retention and Destruction:** Definition and periodic reevaluation of data retention schedules and mechanisms for secure data destruction.
- **Configuration Management Processes:** Secure management and maintenance of all configurations for relevant Information Systems according to industry best practices and vendor guidance.
- **Vulnerability Management:** Regular scans of information systems to detect security vulnerabilities. Identified vulnerabilities are assessed and remediated in a timely manner according to established standards.
- **Disaster Recovery and Business Continuity:** Comprehensive plans that are regularly tested to ensure the resilience of our services. These plans include procedures for responding and recovering from various disruptive events.

## Continuous Improvement and Monitoring

- **SOC 2 Compliance Monitoring:** Regular internal audits and external assessments to ensure ongoing compliance with SOC 2 standards.
- **Proactive Security Monitoring:** 24x7x365 monitoring using advanced tools and services to detect potential malicious activities and ensure the security of our infrastructure.
- **Regular Training and Awareness:** Continuous education for all personnel on security best practices and specific security protocols related to our services. This training is tailored to specific roles and responsibilities and includes industry best practices as well as training related to the sensitivity of the data processed on behalf of our clients.

# Software Requirements

Recollective is a web-based application that functions within all web browsers and smartphones. Its adaptive design accommodates all screen resolutions without the need to install desktop software, web browser extensions or native mobile applications.

# Deployment Options and Data Residency

Recollective offers flexible deployment options and a commitment to data residency to meet the diverse needs and regulatory requirements of our global clientele. We leverage the extensive infrastructure of Amazon Web Services (AWS), providing you with choices for where your data is stored and managed. This section details our regional deployment options, data residency commitments, and the flexibility offered through multi-tenant clusters and dedicated deployments.

## Data Residency

Recollective leverages the global footprint of Amazon Web Services (AWS) by offering site deployments in one of five geographic regions:

- **Asia Pacific** (Seoul, Korea)
- **Asia Pacific** (Sydney, Australia)
- **Canada** (Montreal, Canada)
- **European Union** (Dublin, Ireland)
- **United States** (Northern Virginia, USA)

This broad geographic distribution ensures Recollective has mirrored its operations in multiple distinct AWS regions. All backups are configured across AWS availability zones in the same region for maximum resiliency.

## Multi-Tenant Clusters

Recollective's standard deployment leverages multi-tenant clusters strategically positioned across our supported geographic regions. These clusters are built with a security-first approach, utilizing a shared pool of resources while maintaining strict isolation between customer environments.

- **Load Balancers:** Distribute incoming traffic across multiple servers to ensure high availability and responsiveness.

- **Web Application Servers:** Host and run the Recollective application, processing user requests and serving dynamic content.
- **File Storage Services:** Securely store all uploaded files, media, and research data.
- **Databases:** House all structured data related to your Recollective site, including user information, study configurations, and research responses.

This architecture offers a cost-effective and scalable solution for most customers. You can select your preferred regional cluster based on data residency requirements or proximity to your target audience. For enhanced security and isolation, we also offer Dedicated Deployments.

### Dedicated Deployments

For organizations with specific performance, customization, or compliance needs, Recollective offers dedicated deployments. This premium option provides a completely isolated instance of the Recollective platform's processing and database resources within your chosen geographic region.

- **Dedicated Resources:** Enjoy dedicated load balancers, application servers and databases, ensuring optimal performance and resource availability.
- **Enhanced Security:** Benefit from increased isolation from other Recollective customers and data.
- **Customization Options:** Configure your own outgoing (SMTP) email server for greater control over email delivery and branding.

Dedicated Deployments represent an upgrade from our standard multi-tenant cluster option and are tailored to customers who require the highest level of control and isolation for their research data and processes.

## Secure Cloud Hosting on AWS

Recollective is hosted within the **Amazon Web Services** (AWS) cloud. AWS delivers a scalable cloud computing platform with high availability and dependability. Security responsibilities are therefore shared between Amazon and Recollective.

### AWS Infrastructure Security

Recollective leverages the robust infrastructure of Amazon Web Services (AWS) to ensure the highest levels of security for your research data. AWS prioritizes the security of its global infrastructure, encompassing the hardware, software, networking, and physical data centers that power its services.

AWS designs and manages its IT infrastructure in accordance with industry best practices and adheres to a comprehensive array of security standards and regulations, including:

- SOC 1/SSAE 16/ISAE 3402
- SOC 2
- SOC 3
- FISMA, DIACAP, FedRAMP
- DOD CSM Levels 1-5
- CI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level

While AWS data centers are not open for in-person visits, independent third-party auditors regularly assess and validate AWS's compliance with these rigorous standards. These audit reports, available at http://aws.amazon.com/compliance, provide transparency and assurance about AWS's robust security posture.

AWS maintains advanced environmental controls within its secure facilities to protect your data from physical and environmental threats. These controls include:

- Fire suppression systems
- Precise climate control
- Secure access points with multi-factor authentication and 24/7 security personnel

By partnering with AWS, Recollective ensures your research data benefits from world-class physical and digital security measures, giving you peace of mind.

## Recollective Network Security

Recollective sites are carefully deployed within AWS to maximize security through a wide range of automated tools, managed services and best practices. The goal is to maximize availability while preventing unauthorized access.

- **Network Isolation:** Within AWS, Recollective is isolated within its own Virtual Private Cloud (VPC) and security group.
- **Data Segregation:** Recollective offers a multi-layered approach to data segregation, prioritizing security for all customers. While all data benefits from logical separation within shared data stores like S3, we also offer dedicated clusters as a premium feature. This provides an additional layer of physical separation for sensitive compute and database resources, further enhancing data isolation and security.
- **Public Interfaces:** There are no public interfaces for Recollective servers beyond HTTPS connections which are proxied through redundant load balancers.

- **HTTPS Enforcement:** HTTP connections on port 80 are automatically redirected to HTTPS on port 443 to ensure encryption of all data in transit.

- **Data Access Control:** Data on AWS S3 is only accessible using signed CloudFront requests, and other data is only accessible through the Recollective application, which requires an authenticated session.

- **Continuous Monitoring:** We employ 24x7x365 monitoring using Amazon GuardDuty to detect any potential malicious activities.

- **Real-Time Audit Logs:** We conduct real-time audit log analysis, covering all of our AWS accounts, and follow CIS recommended practices to detect any suspicious or critical user activities.

- **Compliance and Standards:** To maintain compliance with industry standards, we continuously monitor our platform against the CIS AWS Foundations Benchmark v1.2.0 and adhere to AWS security guidelines.

- **Vulnerability Management:** With the help of AWS Inspector, we track host level CVEs and network exposure, allowing us to identify and address any potential vulnerabilities in a timely manner.

- **Secure SSH Access:** Secure SSH connections are available only to system administrators and these are available only over a VPN protected with MFA.

# Proactive Security Measures

## External Penetration Testing

Recollective performs periodic penetration testing of our information systems. These manual and automated penetration tests are conducted by an independent security firm and follow industry-recognized methodologies, such as those outlined by NIST.

These tests, which occur at least annually, identify vulnerabilities and assess our defenses against potential exploits, ensuring continuous improvement in our security posture. A recent penetration test certificate is available upon request.

The following is a list of activities performed during a penetration test:

- **Application Crawling and Scanning:** A comprehensive "crawl" of all authenticated and unauthenticated application screens is conducted using various test accounts. These screens are scanned in both passive and active modes using a commercial vulnerability scanner. All crawl requests are verified for false positives, and responses are recorded in a log file for each test account.

- **Code Walkthrough:** Business-critical application screens, components, and workflows are flagged for a manual code walkthrough to identify potential security flaws.
- **Vulnerability Exploitation:** Whenever appropriate, potential vulnerabilities are exploited for proof-of-concept purposes to determine their exploitability.
- **Privilege Escalation:** Attempts are made to escalate privileges within the application, along with attempts to gain unauthorized access to vulnerable systems and services.
- **Network Penetration Testing:** Includes network information gathering, scanning and host identification, port/service enumeration, user enumeration, and other techniques to identify network vulnerabilities.
- **Application Input Analysis:** Log files are parsed to determine the application inputs processed by each page (cookies, headers, GET/POST variables, etc.).
- **Input Validation Testing:** Each application input is tested for input-related vulnerabilities (fuzzing) and reviewed to ensure adequate protection against tampering and unauthorized disclosure.
- **Security Control Testing:** Each application screen is tested to ensure that applicable authentication and authorization requirements are correctly enforced, along with associated business logic controls.
- **Server Security Scanning:** Application servers are scanned to identify common vulnerabilities and/or insecure configurations.
- **Client-Side Code Review:** Any compiled client-side code is decompiled and tested for potential vulnerabilities.
- **Proof-of-Concept Documentation:** Proof-of-concept exploits are performed, and applicable screenshots are captured to illustrate vulnerabilities clearly.
- **Security Checklist Review:** The application is inspected against a comprehensive 120-point security checklist to ensure maximum coverage and adherence to security standards.

The web application penetration testing methodology can uncover the following flaws:

- Injection flaws
- Authentication flaws
- Session management flaws
- Cross-site scripting flaws
- Direct object reference flaws
- Server misconfiguration flaws
- Insecure data caching flaws
- Insecure data transmission flaws
- Information disclosure flaws
- Weak SSL/TLS ciphers

- Authorization and function level authorization flaws
- Cross-site request forgery flaws
- Unvalidated redirects and forwards
- Clickjacking flaws
- File upload/download flaw

## Security Monitoring

Proactive system monitoring provides Recollective with real-time tracking of the health of its infrastructure.

- **Intrusion Detection System (IDS):** Utilizes a threat detection service to continuously monitor for malicious activity.
- **External System Monitoring:** An external monitoring service verifies the health and response time of every load balancer and web server every 30 seconds, triggering alerts when response time thresholds are exceeded. Monitoring is performed from multiple points of presence worldwide.
- **Cascading Notifications:** Monitoring notifications are cascaded to on-call engineers for performance issues, server health alerts, network intrusion attempts, and other malicious activities. OpsGenie is used to trigger an auto-escalating set of notifications via email, SMS, and phone calls until system administrators acknowledge the issues.
- **Customer-Initiated Escalation:** Enables customers to initiate issue escalation directly, triggering an immediate alert to on-call system administrators. Escalations are submitted via http://recollective.com/911.
- **Anti-Malware Protection:** Anti-malware controls are maintained on all workstations to detect and prevent malicious activities.
- **Change Management:** A documented change management process is in place for evaluating, testing, and authorizing changes to information systems. This ensures that all changes are systematically reviewed and approved to maintain the integrity and security of the platform.
- **Incident Response:** An incident response plan is maintained to promptly address and recover from security incidents or cybersecurity events. Regular testing ensures the effectiveness of this plan.

# Data Security

This section outlines the key measures we take to protect your data throughout its lifecycle within the Recollective platform, covering everything from encryption and access control to secure storage and processing of various data types.

Various features are built into every Recollective site to maximize the security of the data imported and collected:

## System & Application Security

- **Encryption of Data in Transit:** Protects all transmitted data as it travels across the Internet via the Transport Layer Security (TLS) protocol version 1.2 or later.
- **Encryption of Data at Rest:** Protects all data stored within AWS via the industry-standard AES-256 encryption algorithm.
- **Encryption Key Management:** Recollective manages cryptographic keys through Amazon's Key Management Service (AWS KMS), utilizing different keys for encryption. AWS KMS maintains and manages these keys, generated per industry standards. Recollective's policy includes encryption use, key management, and cryptographic standards for various security objectives.
- **User Action Logging:** Tracks all user actions via study visit histories, web server logs, database logs, and off-site application event tracking.
- **Secure Routing:** Employs web application routing rules to block forced navigation attacks by ensuring dynamic resources can only be accessed by authorized users.
- **Brute Force Protection:** Utilizes dynamic request throttling to decrease the effectiveness of brute force attacks by actively blocking excessive requests from a single source.
- **Authentication Security:** Implements time-limited automatic authentication from trusted devices and email notices, which can be disabled for enhanced security.
- **Cross-Site Scripting (XSS) Prevention:** Employs aggressive content filtering of user inputs to prevent Cross-Site Scripting (XSS) and other similar attacks.
- **Cross-Site Request Forgery (CSRF) Prevention:** Leverages secure form tokens to prevent Cross-Site Request Forgery (CSRF) by ensuring end-users cannot be tricked into executing unwanted actions while authenticated.
- **Anti-Virus Protection:** Integrates an anti-virus protection service that scans all

user-submitted binary files during upload and notifies administrators of infected uploads.

- **Data Access Control:** Employs a model-driven architecture to safeguard business data by creating a single "gate" to proxy all requests to view, add, update, or delete data.
- **SQL Injection Prevention:** Utilizes a proprietary database abstraction layer to prevent SQL injection attacks that can leak data or cause data loss.

## Data Protection & Backup

- **Data Backup and Recovery:** Regularly backs up data to offsite locations and validates recovery procedures to ensure data integrity and availability.
- **Synthetic Data in Testing:** Utilizes synthetic data in non-production environments, eliminating the need for data obfuscation or masking and ensuring sensitive information is fully protected and never exposed outside of production systems.

### Securing Database Content

Recollective utilizes Amazon Relational Database Service (RDS), a highly secure and managed version of the MySQL database. Beyond the managed security of RDS, database replication is configured to span separate AWS regions.

All database instances are hardened and inaccessible outside the private network established in its AWS region. Recollective initializes the required data schema and handles future schema changes without the risk of manual intervention.

### Securing Binary File Content

Binary files uploaded to a Recollective site are stored on either Amazon Elastic File Store (EFS) or Amazon S3 and backed up within AWS.

An authenticated session is required to access binary files uploaded to a Recollective site unless it is a site asset for the design of the site, such as a custom site logo.

### Securing Video and Audio Content

Recollective supports two types of video submissions: asynchronous (video uploads and webcam capture) and synchronous (live video meetings). All video submissions are securely processed to prepare them for playback and analysis within the platform. This includes

advanced features such as extracting spoken words to create time-coded transcripts.

Asynchronous videos are transcoded and transcribed by Recollective. All processing of asynchronous video content is performed in Europe unless the site is located in the United States or Australia.

Synchronous videos are captured, recorded and transcoded by Twilio, Inc. Processing is completed in the US in a GDPR-compliant manner. Twilio's binding corporate rules function as a code of conduct for Twilio's data protection practices, based on strict principles established by EU data protection authorities. They enable the transfer of personal data to Twilio group members across borders in compliance with EU data protection laws.

Our video processing partners are never provided personal information and are not permitted to store video content for more than 60 days once processing has been completed.

Once processed, videos are stored in the same region as the Recollective site to which it was submitted and are secured within encrypted Amazon S3 repositories. Video playback and downloads require an authenticated session and also make use of encryption in transit.

## User Authentication and Access Management

Recollective requires that all end users be authenticated to gain access to a site. A site is made up of administrators (Analysts, Moderator and Clients) that are permitted to manage research participants (Panelists).

Panelists are assigned to Segments and Studies which control their access to the site. Clients and Moderators are administrative roles that must also be granted access on a study-by-study basis. Client-role administrators are essentially study observers unless they are granted additional permissions.

Below are some of the key security features related to identity and access management:

- **Centralized Access Control:** Access control is centrally managed in a Site Administration area that permits rapid provisioning and de-provisioning of user accounts without losing historic account access logs.
- **Defined User Roles:** User roles clearly delineate rights and permissions (Analyst, Moderator, Client, and Panelist).
- **Two-Factor Authentication (2FA):** 2FA significantly increases security by requiring a one-time code from a second device with each login. 2FA can be enabled by any user of the site and its use can be enforced for entire user roles or selected individuals.

- **Secondary Verification:** Sensitive account changes by end users, such as a change to their own username, email, or password, require secondary verification via email or 2FA.
- **Password Security:** Passwords are salted and hashed prior to storage in the database which meets NIST password guidelines for secure password storage.
- **Configurable Password Complexity:** Password complexity rules can be configured to meet existing customer standards.
- **Password Expiration:** Password expiry rules can be enforced while preventing password re-use for a configurable time frame.
- **Expiring Email Links:** Emailed links with special privileges, such as password reset links, automatically expire.
- **Automatic Account Lockout:** Automatic lockout of accounts prevents brute force attacks on account passwords. Administrators can customize the lockout sensitivity and lock period.
- **Session Logging:** Session logs identify each study visited and include a hash of the user's IP address (allowing for detection of identical IPs across sessions without revealing the actual address), device information, browser version, and session duration.
- **Session Expiration:** Session expiry limits can be set separately for panelist and administrative roles. Users are forcibly logged out at the end of their session.
- **Single Sign-On (SSO) Integration:** SSO integration can be enabled, as a premium option, which can help restrict account creation and user authentication.

## Session Management

Recollective personalizes the presentation of every page to ensure only permissible content and features are presented to an end user.

Once an authenticated session has been established, a session tracking cookie is set in the web browser which allows the user to remain logged in between requests. The duration of a session can be configured separately for administrators and panelists.

Recollective generates a random 128-bit session ID which is managed by Apache Tomcat, an industry leading Web Server and Java Servlet container. The session ID is stored by the Web browser as a temporary session cookie. The cookie and session ID do not contain any identifying information. Session IDs are regenerated upon session expiry and re-entry to the site and thus never reused.

# Recollective AI

Recollective has incorporated artificial intelligence (AI) to enhance our platform's capabilities while prioritizing user privacy and data security. Our commitment to transparency includes a detailed Privacy Impact Assessment (PIA) outlining our data collection and processing practices. We also offer our customers the ability to opt out of generative AI features, ensuring flexibility and control.

“Generative AI” in this context refers to artificial intelligence capabilities that produce new content, such as summaries, insights, or AI-moderated conversations. Opting out of generative AI disables these content-creation functions but does not affect tools like transcription or translation, which transform rather than generate data.

Recollective employs several key measures to protect user data during AI processing:

- **Use of Pre-trained AI Models:** Recollective utilizes pre-trained AI models that do not require additional training on customer-specific data, thereby minimizing the risk of data exposure.
- **Omission of PII:** Personally Identifiable Information (PII) such as email addresses and sensitive profile data are specifically omitted during AI data processing.
- **Data Encryption:** The platform employs rigorous encryption standards to protect all data in transit and at rest.
- **Strict Data Retention Policies:** Recollective maintains strict data retention policies, ensuring that all data is retained for a limited time only.
- **Sub-Processor Agreements:** Recollective has strict agreements with its AI sub-processors to ensure they adhere to high privacy and security standards. These agreements explicitly forbid any retention of customer data for training or research purposes.
- **Customer Opt-Out Option:** Recollective offers customers the ability to opt-out of generative AI features if they choose to do so.

These measures collectively ensure that Recollective's use of AI enhances its research capabilities without compromising the privacy and security of customer data. For a more comprehensive understanding of our privacy and security measures related to AI, please refer to the Privacy Impact Assessment (PIA) available in our Trust Center (trust.recollective.com).

# Secure Software Development

Application security begins with secure software development practices. Recollective follows an Agile development methodology ensuring frequent and consistent application updates.

## Source Code Management

Recollective's software code base is centrally managed in a private online code repository. Access to the source code is centrally managed and limited to the development team. All accounts are protected by multi-factor authentication.

Code changes are committed into one or more development branches. Branches segregate streams of work, clearly highlighting and grouping related updates in the source code. Over the course of time, every line of code can be attributed to a developer, release and development requirement.

## Code Reviews

Development branches are submitted for review when they are ready to be integrated and tested in a staging environment. A request to merge code ensures lead developers can scrutinize code changes and offer feedback prior to code integration.

General feedback and code-level comments are managed directly within the source code repository. Only once all identified improvements have been made will the code merge request be accepted. Code changes are then incorporated into a broader development branch related to the Agile development cycle called a Sprint.

## Build & Test Automation

All code changes in the main development branch trigger an automated software build process. Customized build scripts are used to trigger unit tests and static code analysis tools. Failed compilations and failed tests automatically halt the build process and alert the development team. Broken builds have high visibility as no additional work can be incorporated until build issues are rectified.

## Pre-Production Environments

Pre-production staging servers provide the opportunity to review a Recollective development branch within a secure hosting area that mimics the AWS production environment. Multiple development branches can be deployed and tested at the same time which provides early access and greater control to the quality assurance team.

Development changes are marked "ready to test" after code reviews and automated builds. Manual testing follows, with any identified issues tracked and addressed. Only after successful re-testing is a "Done" state assigned.

### Deployment Automation

Once a code package has been approved for release, CI/CD pipelines handle packaging and deployments. Various services assist with automatic scaling, load balancing and application health monitoring.

AWS collects health metrics and other attributes to determine the status of the Recollective application.

Amazon CloudWatch provides monitoring dashboards for review of key performance metrics such as latency, CPU utilization, and response codes. CloudWatch alarms allow notifications to be dispatched when metrics exceed key thresholds.

Additional external monitoring services are also employed to track overall uptime and the current validity of all SSL certificates in use by customer sites.

## Third-Party Risk Management

Recollective carefully selects and manages third-party service providers to protect our customers' data. We maintain a strict risk management process to ensure these providers meet our high security and privacy standards, safeguarding customer data throughout our supply chain.

Our comprehensive third-party risk management process includes:

- **Vendor Selection:** We conduct thorough due diligence during the selection process of third-party vendors. This includes evaluating their security, privacy, and confidentiality practices to ensure they meet our stringent standards.
- **Risk Assessment:** Periodic risk assessments are performed to identify and evaluate potential risks associated with third-party service providers. We assess the impact and likelihood of identified risks and the effectiveness of existing safeguards.
- **Contractual Safeguards:** We require all third-party service providers to adhere to robust contractual safeguards. These agreements mandate compliance with our security and privacy standards and include provisions for audits, data breach notifications, and data processing agreements (DPAs) where applicable.

- **Ongoing Monitoring:** Continuous monitoring of third-party vendors is conducted to ensure compliance with our security policies and procedures.
- **Incident Response:** In the event of a security incident involving a third-party service provider, we have established procedures to ensure a prompt and effective response. This includes coordinating with the vendor to mitigate any negative effects and restore normal operations.
- **Termination Procedures:** In cases where a third-party vendor no longer meets our security standards or their services are no longer required, we follow a defined process for the secure termination of the relationship. This includes ensuring that all data is securely returned or destroyed.

# Privacy

Recollective supports thousands of customers in dozens of countries. Our customers entrust the application with large amounts of sensitive information from a wide range of industries including financial services, insurance, healthcare, government, and technology.

## Privacy by Design

Essential privacy-related features have been incorporated deeply into Recollective. Recollective studies can, for example, be run anonymously without significantly compromising the user experience. To protect user privacy, session logging utilizes a hashing technique for IP addresses, allowing for the detection of identical IPs across sessions without revealing the actual IP address.

## Privacy by Default

Recollective studies are configured to share only usernames among participants of a research study. The amount of personal data shared can be increased or decreased as needed. Every report, transcript and data export utility provides the ability to anonymize the data for long-term storage and sharing.

## Obtaining Informed Consent

Most countries now require informed consent prior to the collecting and processing of personal data. Consent statements must be unambiguous, understandable and must provide comprehensive information on the processing of the user's personal data. Recollective provides an extensive Agreements feature to help customers obtain and track such informed consent from panelists in advance of their participation in a research study.

### Identifying Personal Data

Recollective allows custom profile fields to be identified as potentially containing personally identifiable information (PII). Such field-level identification ensures personal data can be selectively wiped when data anonymization features are utilized.

### Minimizing Personal Data

Minimal user identification is required within Recollective for it to be effective. Studies can even be conducted anonymously. Single sign-on (SSO) integration is also available which provides a way to store and manage personal data outside the platform.

### Personal Data Removal

Recollective allows for selective removal of personally identifiable information (PII) while preserving research contributions.During the process that anonymizes response data, Recollective also provides control over the removal of user-submitted photos and videos. It is possible to remove photos while preserving the photo captions and comments. Videos can also be removed while preserving the extracted audio and text transcripts.

### Full Data Removal

When a Recollective site subscription has ended, all database and file data for that site becomes inaccessible to its end users. The data for a closed site is retained and included in ongoing backup routines for a period of 90 days or such longer agreed period following the end of the subscription period (Retention Period).

Site data is permanently purged at the end of the Retention Period but may remain within backups for a further 90 days. Once purged, a site's data cannot be recovered.

## GDPR Compliance

Recollective actively supports its customers' compliance with Canadian and European data protection requirements, including those set out in the General Data Protection Regulation (GDPR), which replaced the EU Data Protection Directive (also known as "Directive 95/46/EC") and became enforceable on May 25, 2018.

If an organization collects, transmits, hosts or analyzes personal data of EU citizens, GDPR requires the organization to use third-party data processors who guarantee their ability to implement the technical and organizational requirements of the GDPR.

To learn more, please see our online Recollective resources:

- https://www.recollective.com/resources/online-research-recollective-and-the-gdpr
- https://www.recollective.com/resources/recollective-and-the-gdpr

## Data Processing Agreement

Recollective offers customers a Data Processing Agreement (DPA), governing the relationship between the customer (acting as a data controller) and Recollective (acting as a data processor). The DPA facilitates the customer's compliance with their obligations under EU data protection law.

Recollective contractual commitments guarantee that customers can:

- Respond to requests from data subjects to correct, amend or delete personal data.
- Be made aware of and report personal data breaches to relevant supervisory authorities and data subjects in accordance with GDPR timeframes.
- Demonstrate compliance with the GDPR as pertaining to Recollective's Services.

## Third-Party Sub-Processors

Recollective currently uses third-party sub-processors to provide some infrastructure services such as secure application hosting and email notifications. Recollective undertakes to use a commercially reasonable selection process by which it evaluates the security, privacy and confidentiality practices of proposed sub-processors that may have temporary access to personal data.

Recollective requires its sub-processors to satisfy equivalent obligations as those required from Recollective (as a Data Processor) as set forth in Recollective's DPA.

## Sub-Processor List

Recollective leverages the following GDPR-compliant sub-processors, carefully chosen for their robust security and privacy practices, to deliver specific infrastructure and service functionalities.

While the sub-processor's headquarters may be located in a specific country, Recollective leverages their global infrastructure to ensure data residency aligns with customer requirements. For instance, data for European customers opting for EU data residency will be processed and stored within AWS data centers located in the European Union.

Recollective uses the following sub-processors to host or process customer data:

- Amazon Web Services (USA)
- Microsoft Corporation (USA)
- Google LLC (USA)
- Salesforce.com Canada Corporation (USA)
- Twilio (USA)
- Zilliz, Inc. (USA)

### Data Breach Notification

In the unlikely event of a data breach, several key steps will be taken, including:

- Any immediate action required to protect impacted sites and their data such as closing access or resetting all user passwords.
- A detailed review of log files generated by intrusion detection devices, VPN access points, web servers, application servers, operating systems and databases to assess the impact of any reported incident.
- Formal notification to impacted customers within 24 hours of the data breach detection.

## Conclusion

At Recollective, we understand that your research data is invaluable. That's why we've built our platform from the ground up with a security-first mindset. More than just checking boxes, we strive to exceed industry standards and provide our clients with the assurance that their data is protected by the most robust security and privacy practices available. You can trust Recollective to be a reliable partner in safeguarding your research and maintaining the confidentiality of your participants.