Winterlight Privacy Notice

Last Updated: November 28, 2023

Privacy

Privacy is the right of individuals to be free from unwarranted intrusions into their personal lives. At Winterlight, your privacy is important to us and we aim to be totally transparent so you can understand how we collect, use and disclose your information.

We have policies and procedures in place to ensure your privacy is maintained. Those policies set out how we collect your information, how we protect your information, and how it is transmitted, stored, used, and disclosed. We adopt the CSA Model Code for the Protection of Personal Information as a guiding principle when developing our Privacy Governance Framework.

Personal Information and Personal Health Information

Personal Information (PI) refers to information which can be used to identify you, such as your name, email address, or a recording of your voice.

Personal Health Information (PHI) is a subset of PI, which identifies your health history and use of health services. This is also known as “protected health information” in the United States.

In the European Economic Area and the United Kingdom, “personal data” refers to both PI and PHI.

Collection

You directly provide us with most of the data we collect. We collect data and process data when you:

Use our website or contact us:

- Register online or place an order for any of our products or services.
- Voluntarily complete a customer survey or provide feedback through online forms or via email.
- Use or view our public website, or any user-accessible dashboard provided as part of our products and services, via your browser's cookies.
- Submit a general inquiry through the Information email address.
- Submit a question to the CPISO through the Privacy email address.

- Place a call over the phone to the Winterlight team.

Apply for a job at Winterlight:

- Submit a CV or resume to apply for a job at Winterlight Labs.

Participate in Clinical Research involving Winterlight technology:

- Complete speech tasks, surveys or other assessments through our data collection app or third-party crowd-sourced data collection platform, when participating in a Winterlight study or a study led by one of our partners.
- Send data to our application programming interface (API).

Our company may also receive your data indirectly from the following sources:

- Through our academic and commercial partners who run clinical research studies.
- Through our recruitment partners who source candidates for job postings.

Winterlight may collect one or more of the following types of PI/PHI:

- For clinical research participants:
  - Name and contact information
  - Geographic location
  - Audio recordings of your voice
  - Typed responses to linguistic tasks
  - Demographic data (e.g., your month and year of birth and your sex)
  - Your health history (e.g., cognitive and neuropsychiatric assessments, and diagnoses if applicable)
  - Responses to clinical assessments

- For employment candidates:
  - Demographic data (e.g., name, address, contact information, etc.)
  - Description of current and prior employment roles and responsibilities

Use

Winterlight may collect and use PI/PHI for one or more of the following purposes:

- Research: to support and conduct internal and external, academic and commercial clinical research and trials, in compliance with protocols approved by a Research Ethics Board (REB) or an Institutional Review Board (IRB);

- Commercial: to develop and improve Winterlight's tools, products, and services,

including our internal data processing, speech recognition, and machine learning algorithms, and statistical models used for analysing PHI, so we can continuously expand and improve upon the industry leading products and services we offer;

- Human Resources: to conduct recruitment and interviews to grow our team;

- Administrative: to diagnose and improve our public website; to manage incoming electronic and telephone communication; to answer requests for services; and, to manage our complaints processes.

Access

We only give access to your information to those company employees, employees of our affiliates, and contractors who require it as part of their job responsibilities. Staff are only allowed to access your information for authorized purposes. Here are some examples:

- Employees who are responsible for maintaining our infrastructure have access to the systems which store and process client information, such as our databases. That allows them to perform tasks like database upgrades and maintenance. These employees are prohibited from using these permissions to view the data unless it is necessary to do so as part of their job (e.g., to verify data integrity after an upgrade).
- Contracted Transcriptionists and Linguists perform data annotation, linguistic analysis and quality assurance. These contractors have access only to the data they require to provide their services (e.g., the audio data and/or transcripts), and they access it only through a secure platform with technical controls which prevent local data storage. We have confidentiality agreements and Data Processing Agreements in place with our contractors who may access your data.

To ensure compliance with our policies, we have access logging and other technical controls in place to allow us to monitor for unauthorized access or unacceptable use of the data.

We do not disclose your information to any third parties, unless you consent to it (e.g., if you are participating in a research study at a retirement home you may consent to disclosing information to a staff physician if we uncover information that suggests you may have an undiagnosed condition), or as may otherwise be permitted or required by law (e.g., if the data was collected as part of a research study, it may be reviewed for quality assurance by representatives of an Institutional Review Board to make sure that the required laws and guidelines are followed).

Storage

We store your data on infrastructure provided by our cloud service providers, Amazon Web Services ("AWS") and, in some cases, on Google Workspace ("Google"), Box.com ("Box") or Microsoft 365 ("Microsoft"). We have executed business associate agreements (BAA) and Data Processing Agreements (including the Standard Contractual Clauses) in place with them. These agreements require these providers to appropriately safeguard the data with the same or comparable level of protection as we do.

If we collect any paper-based data, such as cognitive assessments, we store the papers in locked cabinets. We require our employees to maintain a “clean desk” policy, which means storing all confidential materials in locked cabinets, as well as locking their workstations, laptops and other devices each time they leave their work area.

Retention

For participants in clinical or academic research:

> We retain your data per the terms of the agreement, study protocol (if applicable), and applicable legislation, or for a minimum of 25 years if no other policy applies. At the end of the data retention period, we will remove your data from the relevant records in our live databases and delete your audio files from file storage. Since we maintain backups of our databases, the data will temporarily persist in an inaccessible way as part of our automated backups to prevent unintentional data loss; backups are deleted over time (for example, if we keep 24 months of database backups, it would take 24 months for your data to be fully removed from all of our systems).

For job applicants and other individuals:

> We retain your data for as long as is necessary to carry out the purpose for which the data was collected.

Security

We adopt the ISO/IEC 27002:2013 (Code of Practice for Information Security Controls) as our guide to developing and deploying our information security management program.

Infrastructure

We use only HIPAA-eligible AWS services, and we have an executed BAA and DPA with AWS. We use a variety of technical controls following best practices for network security, such as blocking of unnecessary ports on our servers through AWS security groups and performing regular scans of our servers to detect network vulnerabilities (e.g., insecure data transmission protocols and expired digital certificates).

Data Security

We use the latest recommended secure cipher suites and protocols for data encryption in transit. Data is encrypted at rest.

Where applicable, based on regulatory and client requirements, we store collected data in the appropriate country or region.

Models

Unless indicated otherwise in a client agreement or data consenting process, aggregated and non-personally identifying data derivatives, such as variables we calculate from the raw data samples (e.g., number of nouns or duration of pauses), may be used to train cross-dataset statistical models. Such statistical models are trained and stored in the US data region on our cloud infrastructure, and may be used to provide services in any region.

Logging

We maintain extensive logs with respect to every component of our services, including applications, application programming interfaces (APIs), cloud services, servers, and management consoles. The logs contain information pertaining to security, monitoring, access, and other operational metrics. The logs are reviewed for privacy and security events on a periodic basis.

Authentication

Our mobile applications are protected with user credentials. User passwords must meet our password policy, which has requirements for password strength, length, and regular password rotation.

Devices

Company devices (e.g., workstations and laptops used by employees and contractors) have enabled firewall, up-to-date antivirus software with regularly scheduled scans, automatic OS security updates, disk encryption, and auto-locking after a period of inactivity.

Cross Border Transfers

Unless otherwise specified, Winterlight provides the services and accesses data from its headquarters in Cambridge, United Kingdom; Toronto, Ontario, Canada; and other parts of Canada. Winterlight hosts customers' data in production databases in either the United Kingdom, Canada or the United States. Notwithstanding where the data is

hosted, Winterlight accesses data from Canada for purposes of, for example: responding to support requests; fixing software issues; or, providing services to a customer on the back end of the platform (e.g., correcting errors in a participant record, providing custom statistical analysis services, or performing simulation testing of our disaster recovery plan).

Marketing

If you join one of our mailing lists, or otherwise opt-in to marketing communications from us, from time to time, we will send you information about products and services that we think you might like. You can always opt out of these communications at any time by following the unsubscribe instructions on the communication you have received.

What Are Your Data Protection Rights?

We would like to make sure you are fully aware of your data protection rights. Every user is entitled to the following:

- The right to access - You have the right to request for copies of your personal data. We may charge you a small fee for this service.
- The right to rectification - You have the right to request that we correct any information you believe is inaccurate. You also have the right to request that we complete information you believe is incomplete.
- The right to erasure - You have the right to request that we erase your personal data, under certain conditions.
- The right to restrict processing - You have the right to request that we restrict the processing of your personal data, under certain conditions.
- The right to object to processing - You have the right to object that we process your personal data, under certain conditions.
- The right to data portability - You have the right to request that we transfer the data that we have collected to another organization, or directly to you, under certain conditions.

Exercising Your Rights

If you would like to exercise any of these rights, follow the case that applies to you:

- Case 1 - If your information was supplied to Winterlight by your healthcare provider or another organization, then you should contact them directly.
- Case 2 - If you provided your information to Winterlight yourself, then you can send a request to our CPISO at privacy@winterlightlabs.com.

Cookies

Some of our products have user-accessible dashboards that use “technical cookies”, which allow us to recognize you as a user with each access. This data is not passed on to third parties.

On the Winterlight public website (https://winterlightlabs.com), we use Google Analytics cookies to help us to improve our website by collecting and reporting information on how you use it. The cookies collect information in a way that does not directly identify anyone.

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. You can disable or refuse all cookies on our website without affecting its functionality. Please note that when using any of the user-accessible dashboards as part of our products, if you disable or refuse cookies, some parts of the dashboard may become inaccessible or not function properly.

Personnel Practices

At Winterlight we do our best to practice the “principle of least privilege”. Meaning we restrict access to data on a “need to know” basis, even when it comes to our internal teams.

As an added layer of protection, all of our employees and contractors who have access to your information meet the following requirements:

- Complete a background check
- Sign a confidentiality agreement
- Receive privacy and security training
- Sign a DPA

Disaster Recovery

We use production databases with replication across multiple availability zones to ensure redundancy and smooth failover in the case of infrastructure failure in one zone. We use versioning and replication across multiple regions for our file storage solution to ensure high availability. This means that in the event of an infrastructure failure in one zone or region, our services should continue working with minimal downtime.

Incident Management and Response

We have an Privacy Incident Management Protocol in place to prevent, detect, respond to, and contain privacy/security incidents or breaches. In the event of a detected and confirmed privacy or security breach (e.g., your information was subject to unauthorized collection, access, use or disclosure), we will promptly notify either you directly, or your healthcare provider or other organization that provided your information to Winterlight (in which case it is their responsibility to notify you).

As part of our policy for prevention of privacy/security breaches, we engage an independent third-party firm to conduct regular penetration testing of our services.

GDPR and UK GDPR Compliance

As our company is based in Canada and processes personal data of data subjects who are in the European Economic Area and the United Kingdom, the General Data Protection Regulation and the UK GDPR (collectively the "GDPRs") apply to our processing of personal data. Accordingly, this Privacy Notice also provides you with the additional information as set out in the GDPRs. Our handling of personal data of data subjects who are in the UK or the EEA is in compliance with the GDPR.

EU Representative

As we are based outside of the EU, we have appointed the following EU Representative to act on our behalf when we undertake data processing activities to which the GDPR applies:

If you are in the European Union or the UK, you can still get in touch with our Chief Privacy and Security Officer at privacy@winterlightlabs.com with any questions you have. You can in addition or instead get in touch with our GDPR representative in the EU at WinterlightLabsGDPRrepresentative@mhc.ie or:

MHC GDPR Representative
Mason Hayes and Curran Professional Services Limited
South Bank House
Barrow Street
Dublin 4
Ireland
Tel: +353 (1) 614 5000

Lawful Basis

We will only use your personal data where we have a valid lawful basis to do so in accordance with the GDPRs. Where we mention our "legitimate interests", this is the lawful basis we rely on when we feel that it is necessary to use your personal data for a reason which is in our and/or your interests and which does not unfairly affect your rights over your personal data.

Providing the Service

The processing of personal data is based on Art. 6. (1) (a) GDPR your consent and Art. 6. (1) (b) GDPR the necessity of the processing for the performance of the contract. The legal basis for the processing of sensitive data (health data) is the Art. 9 (2) (a) GDPR, i.e. your explicit consent.

Research and Development

The processing of personal data is based on our legitimate interest in developing/improving, ensuring the technical functionality and the security of our services (art. 6 (1) (f) GDPR). Special categories of personal data (sensitive personal data) may be processed for statistical and research purposes focused on analysing, developing and improving technical functionalities, and ensuring the security of our services (art. 9 (2) (j) GDPR in accordance with the appropriate safeguards (such as: pseudonymization or anonymization – art. 89 GDPR).

Direct Marketing, Commercial Communications

The processing of personal data collected on the website for "*direct marketing, commercial communications*" is based on your consent (Art. 6. (1) (a) GDPR).

Personal Data Storage

All personal data of European data subjects is stored in cloud service providers located in Canada or the United States. We have put adequate measures in place in order to protect your personal data to an equivalent data protection standard as in the EEA.

Right to lodge a complaint with the competent EEA supervisory authority. If you are in the EEA, as a data subject, you have a right to lodge a complaint with the competent supervisory authority under the conditions provided in Article 77 GDPR or seek a remedy in the national courts if you think that your rights in relation to your personal data have been breached. However, we would be grateful if you could give us the opportunity to address your complaint in the first instance by using the contact details provided at the end of this Privacy Notice.

Privacy Policies of Other Websites

Our website contains links to other websites. Our privacy policy applies only to our website, so if you click on a link to another website, you should read their privacy policy.

Changes to our Privacy Policy

At Winterlight, we regularly review and update our privacy and security program - the policies and procedures we have in place – to keep it current. We place any updates on this web page. This Privacy Notice was last updated in November 2023.

How to contact us

If you have any questions about our privacy policy, your data, or you would like to exercise one of your data protection rights, please do not hesitate to contact us via email through privacy@winterlightlabs.com.

How to Contact Canadian Privacy Authorities

If you wish to report a complaint or if you feel that we have not addressed your concern in a

satisfactory manner, we hope you'll reach out to us first to give us a chance to make it right. However, you may also contact the Information Commissioner of Canada:

Email: general@oic-ci.gc.ca
Website: https://www.oic-ci.gc.ca
Address: 30 Victoria Street, Gatineau QC, K1A 1H3