Cybersun Applied Technologies LLC

PRIVACY POLICY

Last updated April 25, 2025

This Privacy Notice outlines how Cybersun Applied Technologies LLC ("we," "us," or "our") collects, uses, stores, shares, and otherwise processes your personal information when you engage with our services ("Services"). This includes:

- Visiting leetproctor.com or any of our websites that link to this Privacy Notice.
- Participating in assessments or interviews (also referred to as "exams") facilitated by our proctoring software, LeetProctor.

LeetProctor.com, our website, and LeetProctor, our software are both services offered by Cybersun Applied Technologies LLC. Our Services utilize Cybersun SecureLink, one of our separate products that installs a root certificate authority to ensure secure and reliable access to leetproctor.com services during the exams. This certificate enables assessments and interviews to operate within a Virtual Private Network, enhancing privacy and preventing dishonesty. LeetProctor, our proctoring software, leverages SecureLink to verify program integrity and maintain a secure environment during assessments or interviews. Details on the functionality of our proctoring software are provided in the section titled "System Check and Data Processing During Assessments or Interviews" under the section "6. DO WE OFFER ARTIFICIAL INTELLIGENCE-BASED PRODUCTS?"

Want to Engage with us in other related ways, including any sales, marketing, or events Questions or concerns? Reading this Privacy Notice will help you understand your privacy rights and choices. We are responsible for making decisions about how your personal information is processed. If you do not agree with our policies and practices, please do not use our Services. If you still have any questions or concerns, please contact us at privacy@leetproctor.com or at support@cybersun.us.

DEFINITIONS

Integrity Database: this is our database that stores previous exams, we only store a pseudo-anonymized, non-identifying value of your email and name and our findings from the assessment. When you scrolled down our privacy policy in the proctoring software and clicked “I Agree”, you agreed to a minimum retention of 2 years of this data. We are legally obligated to keep this data active for two years to provide integrity requests for our **Authorized Third Parties** that are outlined in our contracts and we have legal obligation to provide this database of previous records. Since your email and name become anonymized through the industry standard SHA-256 algorithm and a salt which is secured separately, there is a guarantee that these records cannot be reverse-engineered and will never give your email or full name. Our integrity lookup

tool will determine if your email and name was used for an exam and will only return if there were confirmed signs of cheating and the number of exams you took using our software.

Authorized Third Party: These are businesses or public organizations we might share your information with, like a company who considers you for an Interview or an assessment, These are typically government offices with a .gov email or hiring companies that help people find jobs. New businesses (less than 1 years old) must show us special papers, like their Articles of Organization, to prove they're real. Most importantly, they must have explicit consent from you to run your email and name when they ask for an **Integrity Request**. Additionally we may also call them **Authorized Partners.**

Exam Device: This is the device you take your assessment with.

Integrity Request: When an **Authorized Third Party** requests for us to run your name and email address in our **Integrity Database** they must have implicit consent from their hiring process or your explicit consent outlined in an agreement with you. If they only have implicit consent from you, then our service provides an email titled "Integrity Request from [company name]" where company name is the **Authorized Third Party.** We ask our **Authorized Partners** to append a signature area in their hiring process which you provide your signature to allow them to run your name and email on our **Integrity Database**. Regardless, if consent is not sufficient an email will ask for your explicit consent for the company to run your name and email address.

Authorized Institutions: These are places like public universities or research groups that we sell information with to advance research in improving the welfare of students and people.
Please see the example below.

Example of one Comma Separated Value entry (CSV)

UserID: 1, Violation Level 4, Flags: Used a virtual machine for the exam. Date: 4/13/2025, Time: 5:00 AM

The rest of the CSV will follow that format.

SUMMARY OF KEY POINTS

This summary provides key points from our Privacy Notice, but you can find out more details about any of these topics by clicking the link following each key point or by using our table of contents below to find the section you are looking for.

How do our Authorized Partners obtain your consent?

Our Authorized Partners can choose to:

- **Use our service to email you about an upcoming interview** which can state "Upcoming Assessment with [company name]." To proceed with the interview you would agree to use our proctoring software. Affirmative Consent is obtained when you read through the email and choose "Next steps" which take you to our website and

display the privacy policy in full. This process requires you to scroll down and press the "I Agree" button. Providing consent for the Authorized Partner and us.
- **On the day of assessment. Our Authorized Partners can provide a special link to you**, our proctoring software only downloads after displaying the privacy policy in full and you scrolled down and pressed the I Agree button.

What personal information do we process when taking an assessment or interview? Your full name and email address.

Do we process any sensitive personal information? No.

Do we collect any information from third parties? Yes, your name and email address from **authorized third parties**.

How We Use Your Information

We collect and process your information to:

- Deliver, enhance, and manage our services.
- Communicate with you effectively.
- Ensure security and prevent fraud.
- Comply with legal obligations.
- To respond to **Integrity Requests** from **Authorized Third Parties**
- Comply with **Federal Information Processing Standards (FIPS-3)**

When and With Whom We Share Your Information

We may share your information in specific cases, such as:

- When required by law or to protect our rights.
- When an **Authorized Third Party** creates an **Integrity Request**.

How We Protect Your Information

We protect your information by removing your data and anonymizing it as soon as possible with the industry standard SHA-256 algorithm and salt, we secure this salt separate from the database, we are committed to ensuring your data is protected. However, no online transmission or storage system is completely secure. While we take every reasonable step to protect your data, we cannot guarantee immunity from unauthorized access by hackers or other malicious actors. We follow guidelines from the United States Department of Commerce and its releases on FIPS-3 compliance and regulations.

Your Privacy Rights

Depending on your location, you may have rights related to your personal information, such as accessing, correcting, or deleting it. To understand your specific rights, check our comprehensive privacy rights section.

How to Exercise Your Rights

To exercise your privacy rights, simply email us at privacy@leetproctor.com or at support@cybersun.us and reach out through our contact channels. We'll review and respond to your request promptly, in line with applicable data protection laws.

Our contractual obligation to retain your data upon fraud or dishonesty.

In accordance with our contractual obligations to Authorized Partners, as defined in the Section ('Definitions'), if our proctoring system flags your assessment or interview for potential violations (e.g., unauthorized applications or suspicious activity) and our manual review confirms the flag's validity (e.g., a Level 4 Confirmed violation), we will retain a pseudonymous identifier (a SHA-256 hash of your name and email, with a separately stored salt) in our Integrity Database for a minimum of two years from the assessment date. This retention is necessary to ensure assessment integrity, fulfill our contracts with Authorized Partners (e.g., employers or hiring platforms), and prevent fraud in hiring processes. During this period, you may not opt out of this retention, as it is required to meet our legal and contractual commitments. You will be notified of any confirmed flags within 48 hours, with details on how to dispute them. After two years, or earlier if no longer required, the pseudonymous identifier will be securely deleted unless retention is mandated by applicable law (e.g., for audits or legal disputes). For details on your rights, including access or dispute processes, see Section ('Your Privacy Rights').

System Check and Data Processing During Assessments or Interviews

To maintain a secure and fair environment for your assessment or interview, we perform an initial system check to confirm that only authorized applications are active. By choosing "Close these apps for me," you authorize our system to automatically close any unnecessary applications detected during the process to prevent disruptions. While we strive for accuracy, our system may not always identify every application with absolute certainty. For example, if an application is found in the system32 folder (a critical Microsoft directory) or is an unrecognized system application, we verify its digital signature (an x509 certificate). If the signature is valid and issued by Microsoft, the application remains unaffected. If the signature is invalid, the application will be terminated to ensure security of the assessment environment. Memory is also scanned to ensure no malicious applications are running such as possible code injection or rootkits. These special flags are not recorded but are sent for more diagnostic information which will be marked as "INFORMATIONAL [app file location] has malformed memory. Diagnostic information was sent to leetproctor.com" your potential employer will not see this. This is purely for diagnostics and optimizations.

To safeguard your privacy, this system check is conducted offline whenever feasible. In rare instances where an unfamiliar system configuration or application requires further review, we may send limited diagnostic data to our servers to improve our system check process. This data includes only the application's certificate details, a SHA256 checksum, the application name, and its file path. If diagnostic information is sent, it will be logged as INFORMATIONAL with a note such as: "An application named [application name] contained a valid Microsoft signature but was located in an unexpected file path. Diagnostic information was sent to leetproctor.com" We are committed to handling your data responsibly, sharing only what is necessary to ensure a secure and equitable experience. This is noted on the results email when you receive it after taking your assessment or interview.

We also verify whether your system is running in a virtualized environment using third-party software, Since we may change the third party software at any time and to prevent over reliance on one virtual machine check, we only show its respective license during the initial launch of the proctoring software.

TABLE OF CONTENTS

1. WHAT INFORMATION DO WE COLLECT?

Personal information you consented to your Potential Employer or Hiring Platform.

In Short: We collect your name and email address from **Authorized Third Parties** with your consent defined in “DEFINITIONS” under “Authorized Third Party”. This is from your Potential Employer or Hiring Platform.

We collect your name and email address that you voluntarily provide to the **Authorized Third Party** when you continue with their hiring process, express an interest in obtaining information about your potential employer, or when you participate in activities on the Services, or otherwise when you contact them about job prospects. Your potential employer or hiring platform may use a different email such as your LinkedIn email or another email linked to you. In these instances we email you for your explicit consent defined in “DEFINITIONS” on the term “Integrity Request

In order for us to collect this information, you must scroll down and clicked “I agree”

The personal information we collect may include the following:

names, email addresses, authentication data

If you are a proctor or associate,

names, email addresses, organization, organization role, phone number, authentication data

Payment Data. We may collect data necessary to process your payment if you choose to make purchases, such as your payment instrument number, and the security code associated with your payment instrument. All payment data is handled and stored by stripe. You may find their privacy notice link(s) here: https://stripe.com/privacy.

The cost of proctoring assessments or interviews may be shared between you and your potential employer, hiring platform, or recruiter based on a predetermined ratio to which they choose. We will process payments from both parties in alignment with this agreed-upon split before taking the assessment or interview, ensuring transparency and fairness in the transaction. Your potential employer may pay in full and no payment is required on your part.

Information your potential employer sends us should be accurate and true. At any time when this information updates or is no longer valid then it is the duty of your future employer to resend the information accurately. You are warmly encouraged to inform your employer of such changes.

In Short: Your future employer or hiring platform with your consent may send us your full name and email address to create an assessment or interview for you and them. In the event you did not consent to this, please send email as soon as possible at privacy@leetproctor.com or at support@cybersun.us but no more than 3 months.

2. HOW DO WE PROCESS YOUR INFORMATION?

In Short: We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes with your consent. By using our services, you consent for us to do this.

We process your personal information for a variety of reasons, depending on how you interact with our Services, including:

To facilitate account creation and authentication and otherwise manage user accounts. We may process your information so you can create and log in to your account, as well as keep your account in working order. To deliver and facilitate delivery of services to the user. Your account login information is provided by the email confirmation labeled “Your Assessment Results #1”

We may process your information to provide you with the requested service.

To respond to your inquiries/offer support to you.

We may process your information to respond to your inquiries and solve any potential issues you might have with the requested service.

To send administrative information to you. We may process your information to send you details about our products and services, changes to our terms and policies, and other similar information.

To fulfill and manage your orders. We may process your information to fulfill and manage your orders, payments, and exchanges made through the Services.

To save or protect an individual's vital interest. We may process your information when necessary to save or protect an individual’s vital interest, such as to prevent harm.

To disclose to an **authorized third party** whether a user was flagged on a proctoring exam or interview, based on their full name and email address. When a potential employer requests verification of a candidate’s integrity for a proctored interview or hiring process, we use the candidate’s full name and email address to identify their exam record and share whether they were flagged for cheating, as determined by our proctoring system. We ask that your potential employer notify you when such information will be collected from our database. However, if no consent was provided, then please email us at privacy@leetproctor.com or at support@cybersun.us

3. WHAT LEGAL BASES DO WE RELY ON TO PROCESS YOUR INFORMATION?

In Short: We process your personal information only when necessary and when we have a valid legal basis under applicable law, such as with your consent, to comply with legal obligations, to fulfill our contractual obligations, to protect your rights, or to pursue our business interests.

If you are located in the EU or UK, this section applies to you.

The General Data Protection Regulation (GDPR) and UK GDPR require us to explain the legal bases we rely on to process your personal information. We may rely on the following legal bases:

Consent. We may process your personal information if you have given us specific permission (i.e., consent) to use it for a particular purpose. You can withdraw your consent at any time by emailing us at privacy@leetproctor.com or at support@cybersun.us

Performance of a Contract. We may process your personal information when necessary to fulfill our contractual obligations to you, such as providing our Services, or at your request before entering into a contract with you if you are doing business as an **Authorized Partner** with us.

Legitimate Interests. We may process your personal information when it is reasonably necessary to achieve our legitimate business interests, provided those interests do not override your fundamental rights and freedoms. For example, we may process your information to:

- Support employers in making informed hiring decisions by sharing limited, accurate, and relevant information about a candidate's exam integrity (e.g., confirmation of detected cheating). We balance this interest with your rights by ensuring transparency through our privacy notice and exam terms, limiting data shared to what is strictly necessary, and maintaining accuracy to foster fair and credible hiring processes that benefit all parties.

- Analyze usage patterns to improve our Services, ensuring data is pseudonymized where possible to minimize impact on your privacy.

- Prevent fraud or unauthorized access to our systems, protecting both our business and your account security.

Legal Obligations. We may process your personal information when necessary to comply with legal obligations, such as responding to lawful requests from law enforcement or regulatory authorities, exercising or defending our legal rights, or disclosing information as evidence in litigation where we are involved. Vital Interests. We may process your personal information when necessary to protect your vital interests or those of another person, such as in situations involving potential threats to safety.

If you are located in Canada, this section applies to you.

We may process your information if you have given us specific permission (i.e., express consent) to use your personal information for a specific purpose, or in situations where your permission can be inferred (i.e., implied consent). You can withdraw your consent at any time.

In some exceptional cases, we may be legally permitted under applicable law to process your information without your consent, including, for example: If collection is clearly in the interests of an individual and consent cannot be obtained in a timely way For investigations and fraud detection and prevention For business transactions provided certain conditions are met If it is contained in a witness statement and the collection is necessary to assess, process, or settle an insurance claim For identifying injured, ill, or deceased persons and communicating with next of kin If we have reasonable grounds to believe an individual has been, is, or may be victim of financial abuse If it is reasonable to expect collection and use with consent would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province If disclosure is required to comply with a subpoena, warrant, court order, or rules of the court relating to the production of records If it was produced by an individual in the course of their employment, business, or profession and the collection is consistent with the purposes for which the information was produced If the collection is solely for journalistic, artistic, or literary purposes If the information is publicly available and is specified by the regulations

4. WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?

In Short: We may share information in specific situations described in this section and/or with the following categories of third parties.

Vendors, Consultants, and Other Third-Party Service Providers. We may share your data with third-party vendors, service providers, contractors, or agents ("third parties") who perform services for us or on our behalf and require access to such information to do that work. We have contracts in place with our third parties, which are designed to help safeguard your personal information. This means that they cannot do anything with your personal information unless we have instructed them to do it. They will also not share your personal information with any organization apart from us. They also commit to protect the data they hold on our behalf and to retain it for the period we instruct.

WHAT OTHER THIRD PARTY CAN ACCESS MY DATA?

The categories of third parties we may share personal information with are as follows: Government Entities Hiring Services and Platforms

We authenticate Government Entities if they have an official .gov email. This is to comply with laws ahead of time instead of adapting it after laws are in effect.

We allow Hiring Services and Platforms to request data from our database. We authenticate these providers with an appointed representative of their choosing. Businesses which have been formed in the last one year are required to show us their Articles of Organization and their Operating Agreement.

We also may need to share your personal information in the following situations: Business Transfers. We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company.

5. DO WE USE COOKIES AND OTHER TRACKING TECHNOLOGIES?

In Short: We may use cookies and other tracking technologies to collect and store your information.

We may use cookies and similar tracking technologies (like web beacons and pixels) to gather information when you interact with our Services. Some online tracking technologies help us maintain the security of our Services and your account, prevent crashes, fix bugs, save your preferences, and assist with basic site functions.

You can opt out of these online tracking technologies by submitting a request as described below under section "DO UNITED STATES RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?"

Specific information about how we use such technologies and how you can refuse certain cookies is set out in our Cookie Notice.

6. DO WE OFFER ARTIFICIAL INTELLIGENCE-BASED PRODUCTS?

No. We don't want AIs proctoring a human to human interview or assessment.

7. IS YOUR INFORMATION TRANSFERRED INTERNATIONALLY?

In Short: We may transfer, store, and process your information in countries other than your own.

Our servers are located in the United States. If you are accessing our Services from outside the United States, please be aware that your information may be transferred to, stored by, and processed by us in our facilities and in the facilities of the third parties with whom we may share your personal information (see "WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?" above), in the United States, and other countries.

If you are a resident in the European Economic Area (EEA), United Kingdom (UK), or Switzerland, then these countries may not necessarily have data protection laws or other similar laws as comprehensive as those in your country. However, we will take all necessary measures to protect your personal information in accordance with this Privacy Notice and applicable law.

European Commission's Standard Contractual Clauses:

We have implemented measures to protect your personal information, including by using the European Commission's Standard Contractual Clauses for transfers of personal information between our group companies and between us and our third-party providers. These clauses require all recipients to protect all personal information that they process originating from the EEA or UK in accordance with European data protection laws and regulations. Our Standard Contractual Clauses can be provided upon request. We have implemented similar appropriate safeguards with our third-party service providers and partners and further details can be provided upon request.

8. HOW LONG DO WE KEEP YOUR INFORMATION?

In Short: We delete your personal information promptly after use and retain only anonymized data as needed for legitimate business purposes, unless required by law.

We retain your personal information (e.g., name, email address) only as long as necessary to deliver our Services, typically deleting it within 7 days after your assessment or interview results are sent to your employer or hiring platform, or within 12 months if your account becomes inactive (e.g., no new assessments). Anonymized data, such as a hashed identifier derived from your name and email, is retained for up to 2 years to verify assessment integrity for authorized third parties, as described in **Section 15**. If we have no ongoing business need for your data, we delete or anonymize it securely. Where deletion is not immediately possible (e.g., in backup archives), we isolate the data until deletion occurs. Retention periods may extend if required by law (e.g., for audits or legal disputes).

9. HOW DO WE KEEP YOUR INFORMATION SAFE?

In Short: We aim to protect your personal information through a system of organizational and technical security measures.

We have implemented appropriate and reasonable technical and organizational security measures designed to protect the security of any personal information we process. However, despite our safeguards and efforts to secure your information, no electronic transmission over the Internet or information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that hackers, cybercriminals, or other unauthorized third parties will not be able to defeat our security and improperly collect, access, steal, or modify your information. Although we will do our best to protect your personal information, transmission of personal information to and from our Services is at your own risk. You should only access the Services within a secure environment.

10. DO WE COLLECT INFORMATION FROM MINORS?

In Short: NO, We do not knowingly collect data from or market to children under 18 years of age.

We do not knowingly collect, solicit data from, or market to children under 18 years of age, nor do we knowingly sell such personal information. By using the Services, you represent that you

are at least 18 or that you are the parent or guardian of such a minor and consent to such minor dependent's use of the Services. If we learn that personal information from users less than 18 years of age has been collected, we will deactivate the account and take reasonable measures to promptly delete such data from our records. If you become aware of any data we may have collected from children under age 18, please contact us at privacy@leetproctor.com or at support@cybersun.us.

11. WHAT ARE YOUR PRIVACY RIGHTS?

In Short: Depending on your state of residence in the US or in some regions, such as the European Economic Area (EEA), United Kingdom (UK), Switzerland, and Canada, you have rights that allow you greater access to and control over your personal information. You may review, change, or terminate your account at any time, depending on your country, province, or state of residence.

In some regions (like the EEA, UK, Switzerland, and Canada), you have certain rights under applicable data protection laws. These may include the right (i) to request access and obtain a copy of your personal information, (ii) to request rectification or erasure; (iii) to restrict the processing of your personal information; (iv) if applicable, to data portability; and (v) not to be subject to automated decision-making. In certain circumstances, you may also have the right to object to the processing of your personal information. You can make such a request by contacting us by using the contact details provided in the section "HOW CAN YOU CONTACT US ABOUT THIS NOTICE?" below.

We will consider and act upon any request in accordance with applicable data protection laws.

If you are located in the EEA or UK and you believe we are unlawfully processing your personal information, you also have the right to complain to your Member State data protection authority or UK data protection authority.

If you are located in Switzerland, you may contact the Federal Data Protection and Information Commissioner.

Withdrawing your consent: If we are relying on your consent to process your personal information, which may be express and/or implied consent depending on the applicable law, you have the right to withdraw your consent at any time. You can withdraw your consent at any time by contacting us by using the contact details provided in the section "HOW CAN YOU CONTACT US ABOUT THIS NOTICE?" below.

However, please note that this will not affect the lawfulness of the processing before its withdrawal nor, when applicable law allows, will it affect the processing of your personal information conducted in reliance on lawful processing grounds other than consent.

Opting out of marketing and promotional communications: You can unsubscribe from our marketing and promotional communications at any time by clicking on the unsubscribe link in the emails that we send, or by contacting us using the details provided in the section "HOW

CAN YOU CONTACT US ABOUT THIS NOTICE?" below. You will then be removed from the marketing lists. However, we may still communicate with you, for example, to send you service-related messages that are necessary for the administration and use of your account, to respond to service requests, or for other non-marketing purposes.

Account Information

If you would at any time like to review or change the information in your account or terminate your account, you can:

Log in to your account from the email link sent to you after the completion of your assessment or interview, to update or terminate your account.

Upon your request to terminate your account, we will deactivate or delete your account and information from our active databases. However, we may retain some information in our files to prevent fraud, troubleshoot problems, assist with any investigations, enforce our legal terms and/or comply with applicable legal requirements.

Cookies and similar technologies: Most Web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove cookies and to reject cookies. If you choose to remove cookies or reject cookies, this could affect certain features or services of our Services.

If you have questions or comments about your privacy rights, you may email us at privacy@leetproctor.com or at support@cybersun.us.

12. CONTROLS FOR DO-NOT-TRACK FEATURES

Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track ("DNT") feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. At this stage, no uniform technology standard for recognizing and implementing DNT signals has been finalized. As such, we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online. If a standard for online tracking is adopted that we must follow in the future, we will inform you about that practice in a revised version of this Privacy Notice.

California law requires us to let you know how we respond to web browser DNT signals. Because there currently is not an industry or legal standard for recognizing or honoring DNT signals, we do not respond to them at this time.

13. DO UNITED STATES RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?

In Short: If you are a resident of California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey,

Oregon, Rhode Island, Tennessee, Texas, Utah, or Virginia, you may have the right to request access to and receive details about the personal information we maintain about you and how we have processed it, correct inaccuracies, get a copy of, or delete your personal information. You may also have the right to withdraw your consent to our processing of your personal information. These rights may be limited in some circumstances by applicable law. More information is provided below.

Categories of Personal Information We Collect

We have or will collected the following categories of personal information in the past twelve (12) months:

Category: A. Identifiers

Contact details, such as real name, alias, postal address, telephone or mobile contact number, unique personal identifier, online identifier, Internet Protocol address, email address, and account name

YES, Your Email address and IP Address are collected.

Category: B. Personal information as defined in the California Customer Records statute

Name, contact information, education, employment, employment history, and financial information

YES, your name is collected.

Category: C. Protected classification characteristics under state or federal law

Gender, age, date of birth, race and ethnicity, national origin, marital status, and other demographic data

NO

Category: D. Commercial information

Transaction information, purchase history, financial details, and payment information

NO

Category: E. Biometric information

Fingerprints and voiceprints

NO

Category: F. Internet or other similar network activity

Browsing history, search history, online behavior, interest data, and interactions with our and other websites, applications, systems, and advertisements

NO

Category: G. Geolocation data

Device location

NO

Category: H. Audio, electronic, sensory, or similar information

Images and audio, video or call recordings created in connection with our business activities

NO

Category: I. Professional or employment-related information

Business contact details in order to provide you our Services at a business level or job title, work history, and professional qualifications if you apply for a job with us

NO

Category: J. Education Information

Student records and directory information

NO

Category: K. Inferences drawn from collected personal information

Inferences drawn from any of the collected personal information listed above to create a profile or summary about, for example, an individual’s preferences and characteristics

NO

Category: L. Sensitive personal Information

NO

We may also collect other personal information outside of these categories through instances where you interact with us in person, online, or by phone or mail in the context of:

Receiving help through our customer support channels;

Participation in customer surveys or contests; and

Facilitation in the delivery of our Services and to respond to your inquiries.

We will use and retain the collected personal information as needed to provide the Services or for:

Category A - Full Names and IP Address, used in assessment results or interview results

We delete the data once the hiring platform or potential employer confirms they received the assessment or interview result. If not, the data is automatically deleted in 7 days after the completion of the assessment or interview.

Category B - Email Address, Assessment Results or interview results,

We delete the data once the hiring platform or potential employer confirms they received the assessment or interview result. If not, the data is automatically deleted in 7 days after the completion of the assessment or interview.

Sources of Personal Information

Learn more about the sources of personal information we collect in "WHAT INFORMATION DO WE COLLECT?" How We Use and Share Personal Information

Learn more about how we use your personal information in the section, "HOW DO WE PROCESS YOUR INFORMATION?"

Will your information be shared with anyone else?

We may disclose your personal information with our **Authorized Partners** pursuant to a written contract between us and each **Authorized Partner**.

Learn more about how we disclose personal information to in the section, "WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?"

We have disclosed the following categories of personal information to third parties for a business or commercial purpose in the preceding twelve (12) months:

- Category A. Identifiers

- Category B. Personal information as defined in the California Customer Records law

Note: Only the hashed value of your name and email is shared along with its record through a process we call **Integrity request**.

The categories of third parties to whom we disclosed personal information for a business or commercial purpose can be found under "WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?"

We have sold or will share the following categories of personal information to third parties in the preceding twelve (12) months:

The categories of third parties to whom we will sell or sold personal information are:

Non-Profit Public Universities
Research Institutions
Independent Researchers with accreditation
Hiring Services and Platforms Recruitment Services and Platforms

Note: as mentioned in the section “DEFINITIONS”, Your name and email is hashed and these Authorized Partners and Authorized Institutions only have the hash or CSV in that example provided.

The categories of third parties to whom we shared or sold records to view from the name and email from Category A and B with are:

Potential Employers or Hiring Platforms

These are applicable examples of "Potential Employers" or “Hiring Platforms” The company who is considering the user for a position in their company.

Examples: These are companies that are not affiliated with us and provided as an applicable example only.

Businesses (Cybersun Applied Technologies LLC, Apple, Amazon)
Staffing Agencies (Hawkins Personnel Group, Media Riders)
Hiring Services and Platforms (ZipRecruiter, LinkedIn)

In general:

When a business wants to use Leet Proctor. We require an official domain email from them.

When a business is formed for less than a year. We ask for their Articles of Organization with the state they registered their business with.

When a business is confirmed and becomes an Authorized Third Partner, we provide training documents and videos to ensure they use our services appropriately.

We comply with legal orders and will share with appropriate authorities.

Your Rights

You have rights under certain US state data protection laws. However, these rights are not absolute, and in certain cases, we may decline your request as permitted by law. These rights include:

Right to know whether or not we are processing your personal data

Right to access your personal data

Right to correct inaccuracies in your personal data

Right to request the deletion of your personal data

Right to obtain a copy of the personal data you previously shared with us

Right to non-discrimination for exercising your rights

Right to opt out of the processing of your personal data if it is used for targeted advertising (or sharing as defined under California's privacy law), the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects ("profiling")

We do not use your personal data for targeted advertising. Please report this at privacy@leetproctor.com or at support@cybersun.us

Depending upon the state where you live, you may also have the following rights: Right to access the categories of personal data being processed (as permitted by applicable law, including the privacy law in Minnesota)

Right to obtain a list of the categories of third parties to which we have disclosed personal data (as permitted by applicable law, including the privacy law in California, Delaware, and Maryland)

Right to obtain a list of specific third parties to which we have disclosed personal data (as permitted by applicable law, including the privacy law in Minnesota and Oregon)

Right to review, understand, question, and correct how personal data has been profiled (as permitted by applicable law, including the privacy law in Minnesota)

Right to limit use and disclosure of sensitive personal data (as permitted by applicable law, including the privacy law in California)

Right to opt out of the collection of sensitive data and personal data collected through the operation of a voice or facial recognition feature (as permitted by applicable law, including the privacy law in Florida) How to Exercise Your Rights

To exercise these rights, you can contact us by emailing us at privacy@leetproctor.com or at support@cybersun.us, or by referring to the contact details at the bottom of this document.

You can opt out from the selling of your personal information, targeted advertising, or profiling by disabling cookies in Cookie Preference Settings.

We will honor your opt-out preferences if you enact the Global Privacy Control (GPC) opt-out signal on your browser.

Under certain US state data protection laws, you can designate an authorized agent to make a request on your behalf. We may deny a request from an authorized agent that does not submit proof that they have been validly authorized to act on your behalf in accordance with applicable laws. Request Verification

Upon receiving your request, we will need to verify your identity to determine you are the same person about whom we have the information in our system. We will only use personal information provided in your request to verify your identity or authority to make the request. However, if we cannot verify your identity from the information already maintained by us, we may request that you provide additional information for the purposes of verifying your identity and for security or fraud-prevention purposes.

If you submit the request through an authorized agent, we may need to collect additional information to verify your identity before processing your request and the agent will need to provide a written and signed permission from you to submit such request on your behalf.

Please keep in mind, we do not use your personal data other than to authenticate and email you the assessment or interview results, we may also hash your data in case future employers ask us for it outlined in the section "DOES LEETPROCTOR.COM STORE MY EMAIL OR NAME IN ITS DATABASE AFTER MY EXAM IS OVER?"

Appeals

Under certain US state data protection laws, if we decline to take action regarding your request, you may appeal our decision by emailing us at privacy@leetproctor.com or at support@cybersun.us. We will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If your appeal is denied, you may submit a complaint to your state attorney general. California "Shine The Light" Law California Civil Code Section 1798.83, also known as the "Shine The Light" law, permits our users who are California residents to request and obtain from us, once a year and free of charge, information about categories of personal information (if any) we disclosed to third parties for direct marketing purposes and the names and addresses of all third parties with which

we shared personal information in the immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request in writing to us by using the contact details provided in the section "HOW CAN YOU CONTACT US ABOUT THIS NOTICE?"

14. DO OTHER REGIONS HAVE SPECIFIC PRIVACY RIGHTS?

In Short: You may have additional rights based on the country you reside in.

Australia and New Zealand We collect and process your personal information under the obligations and conditions set by Australia's Privacy Act 1988 and New Zealand's Privacy Act 2020 (Privacy Act).

This Privacy Notice satisfies the notice requirements defined in both Privacy Acts, in particular: what personal information we collect from you, from which sources, for which purposes, and other recipients of your personal information.

If you do not wish to provide the personal information necessary to fulfill their applicable purpose, it may affect our ability to provide our services, in particular: offer you the products or services that you want respond to or help with your requests manage your account with us confirm your identity and protect your account At any time, you have the right to request access to or correction of your personal information. You can make such a request by contacting us by using the contact details provided in the section "HOW CAN YOU REVIEW, UPDATE, OR DELETE THE DATA WE COLLECT FROM YOU?"

If you believe we are unlawfully processing your personal information, you have the right to submit a complaint about a breach of the Australian Privacy Principles to the Office of the Australian Information Commissioner and a breach of New Zealand's Privacy Principles to the Office of New Zealand Privacy Commissioner. Republic of South Africa At any time, you have the right to request access to or correction of your personal information. You can make such a request by contacting us by using the contact details provided in the section "HOW CAN YOU REVIEW, UPDATE, OR DELETE THE DATA WE COLLECT FROM YOU?"

If you are unsatisfied with the manner in which we address any complaint with regard to our processing of personal information, you can contact the office of the regulator, the details of which are:

The Information Regulator (South Africa) General enquiries: enquiries@inforegulator.org.za Complaints (complete POPIA/PAIA form 5): PAIAComplaints@inforegulator.org.za & POPIAComplaints@inforegulator.org.za

15. DOES LEETPROCTOR.COM STORE MY EMAIL OR NAME IN ITS DATABASE AFTER MY ASSESSMENT IS OVER?

In Short: No, we begin the process of deletion of your email and name immediately. We retain a hashed identifier for up to 2 years to verify assessment integrity, using secure methods to protect this data. See “Data Handling and Hashing Process” for further explanation on the deletion.

Technical Definitions:

Hash. a text that is the result from a SHA256 algorithm, these are algorithms that are industry standard. We also use a salting algorithm to ensure it cannot be reversed. We protect the salt values by keeping them separate from the **Integrity Database** and following proper security measures.

Pseudonymous identifier: Instead of recording your name and email on our database. We use the Hash which serves the purpose of record keeping

Data Handling and Hashing Process

We do not retain your email address or full name after your assessment or interview. Instead, we generate a secure hash using the industry-standard SHA-256 algorithm with a unique, cryptographically random 32-byte salt. This hash serves as a **pseudonymous identifier**, ensuring your data cannot be reverse-engineered. Your email and name are deleted from our active databases within 7 days after results are sent to your employer or hiring platform, or deleted immediately if you press “End Session” during an assessment, see Example 4 from the Section “DEFINITIONS” to further understand what happens to the data.

Consent and Data Retention By using our services, you agree to our data practices as outlined in this policy and our Privacy Policy. We collect and retain a hashed identifier derived from your assessment data for up to two years to verify your assessment history for employers or hiring platforms. This hash is a pseudonymous identifier designed to prevent re-identification without additional data we do not store. We use SHA-256, with a salting algorithm to remain compliant with the industry standard practices to ensure commercial protection on our database.

Salt Security

In Short: we use industry standard practices to protect your data.

To protect salt values, we generate them using a secure random number generator and store them encrypted with AES-256 in a hardened database with strict access controls. Encryption keys are managed via a secure key management system, such as a Hardware Security Module or trusted secrets platform. Salts are transmitted over TLS 1.3, and we minimize their exposure in application code. We conduct regular security audits and encrypt backups to ensure robust protection, maintaining compliance with data protection standards.

Why retain my records for two years?

Justification: We retain this data for two years to align with common compliance practices, similar to the Fair Labor Standards Act (FLSA), which requires U.S. companies to keep wage

records for two years to resolve disputes. While FLSA doesn't directly apply to assessment data, LeetProctor uses this timeframe to ensure fairness and address any issues with our **Authorized Partners** or **Users**. Additionally, this time frame allows our service LeetProctor to verify the integrity of past assessments for Authorized Third Parties (e.g., employers or hiring platforms) to ensure fair hiring decisions. It provides a reasonable period to address potential disputes, confirm the absence of dishonest behavior, and maintain trust in the assessment process, balancing user privacy with the needs of employers to make informed decisions. The use of secure, non-reversible hashing (SHA-256 with a salted algorithm) ensures that no personally identifiable information is stored, minimizing privacy risks while fulfilling contractual obligations to **Authorized Partners.** Users can control whether they want to be notified for requests, automatically grant requests with their explicit consent.

By default, after consent is provided, the User can update their account settings by emailing us at privacy@leetproctor.com or at support@cybersun.us

These **authorized partners** are defined in the section "DEFINITIONS"

You may opt out of data retention at any time by:

Selecting the "End Session" button during an assessment, which immediately voids and deletes the current assessment data from our database. The proctor will receive a notification stating, "Applicant requested cancellation of the assessment," distinct from technical issues like internet disruptions. Requesting deletion after the assessment via privacy@leetproctor.com or at support@cybersun.us. We process deletion requests promptly, typically within 10 business days, subject to legal obligations.

When authorized partners use our services. We put a baseline of 2 years to retain the data they provided to create your assessment or interview and build a database of previous proctoring assessments and results. We share the **Pseudonymous identifier** from your email and name to other authorized clients. By using our services and completing the assessment or interview. Then you gave your explicit consent for us to retain your data for the 2 years as required by our agreements with **Authorized Partners**. So if you make a request for your data deletion, we can only delete your data after two years.

Employers or hiring platforms may access your hashed identifier to verify your assessment history. We require them to notify you if our data influences their hiring decision, and we provide you with details of such access upon request.

Note: Our Automation is not Artificial Intelligence (AI).

Violation Flags and Their Classification Our system uses automated and human-reviewed processes to detect potential assessment violations, assigning flags categorized by certainty levels from 0 to 4.

These levels are:

Level 0: Informational. Records routine actions, such as agreeing to this policy or navigating the assessment platform, including metadata transmitted to our servers.

Level 1: Noted. Indicates a prior Level 2 flag downgraded after review, typically due to a false positive, with the rationale documented and available upon request.

Level 2: Flagged for Review. Denotes potential issues requiring investigation, such as detecting a virtual machine vendor in the system registry. We use automated algorithms to analyze patterns, recognizing legitimate uses of virtual machines. Level 2 flags are resolved as Level 1 (Noted) or escalated to Level 3 (Suspected with Evidence) after review. If human review is needed, we notify you and the employer of the outcome.

Level 3: Suspected with Evidence. Indicates additional evidence supporting a Level 2 flag, verified by algorithms and, where necessary, third-party providers (virtual machine analysis). This level suggests a higher likelihood of dishonest behavior, pending final review.

Level 4: Confirmed. Confirms dishonest behavior based on robust evidence, algorithmic verification, and human review. The flag includes a detailed explanation of the evidence, which you can access upon request. Flag Notification Process To ensure fairness, we notify you of any non-informational flags (Levels 1–4) via email within 24 hours of the assessment's completion, including details on how to review or dispute the flag. Employers receive flag data only after our review process is complete, typically limited to Level 4 (Confirmed) flags unless you consent otherwise. A flag counter in our software tracks non-informational flags for transparency, accessible in your account dashboard.

If a flag influences an employer's decision, we require them to inform you, and you can request a copy of the flag report at no cost. You may dispute any flag by emailing privacy@leetproctor.com or at support@cybersun.us, and we'll investigate with a response within 14 business days.

CAN AUTHORIZED THIRD PARTIES SELL OR MISUSE MY DATA?

Authorized Third Parties cannot sell your data and our **Integrity Request**. We allow our Authorized Partners to decide what to do with the information presented to them using the data we provide. Explicit consent is also required when running a name and email address on the **Integrity Database** and only accessible when the Authorized Third Party logs into their account**,** this process looks like.

Logged in as privacy@cybersun.us
Integrity Request Tool

Please enter a username and email.
Full Name:
Email:

Here are more examples from the Integrity Request Tool.

Example 1: If you have taken an assessment before and require Employers to ask you for permission in your account settings editable in your assessment result email:

Logged in as privacy@cybersun.us
Integrity Request Tool

A match WAS FOUND for:
Full Name: Billy Jones
Email: person@gmail.com
This user requests notification before retrieving their prior assessments. Send Request?

Example 2: If you have not taken an assessment with us before or if your info was deleted.
Logged in as privacy@cybersun.us
Integrity Request Tool

A match was NOT FOUND for:
Full Name: Billy Jones
Email: person@gmail.com

Example 3: If you are going to take an assessment and you gave explicit consent from the email labeled "Upcoming Assessment with [company name]."

Logged in as privacy@cybersun.us
Integrity Request Tool

A match was FOUND for:
Full Name: Billy Jones
Email: person@gmail.com
Consent was provided after reading the
privacy policy before an assessment on 4/13/2025 5:57 PM
Origin: Email reminder
Click to view results.

Example 4: When you press I Agree on the privacy policy displayed in the proctoring software before stating your assessment. It's been one year now and you applied for a new company which will use our services.

Integrity Request Tool

A match was FOUND for:
Full Name: Billy Jones
Email: person@gmail.com
Consent was provided after reading the
privacy policy before an assessment on 4/13/2024 5:57 PM
Origin: Email reminder
Click to view results.

It is important that you keep your account settings up to date with your preferences.

HOW OUR AUTHORIZED PARTIES KEEP YOUR DATA SAFE

We ensure our Authorized Third Parties get the least amount of access to our **Integrity Database**. Generally we only allow two people to access our Integrity Request Tool.

This is an example of what they can see when they view your results**.** Please note your Potential Employer is the one who makes the final decision.

Example 1 : A user that does not exist or when the account was deleted.
There is no way to access this.

Example 2 : A user without detections. (not flagged)
Found 1 entries from hash, parameters: Billy Jones, person@gmail.com.

- User exists in the database, has taken 3 exams, all clean.

Example 3: A user with detections. (flagged)
Found 3 entries from hash, parameters: Billy Jones, person@gmail.com.

- Exam on 1/13/2025 at 5:00 AM, Titled "Software Engineer Interview for Cybersun"
- Detection 1: Unauthorized Application named InterviewCheater with hidden graphics was terminated, on 1/13/2025 5:12 AM. The application was continuously terminated during the assessment.
- Detection 2: VPN from **Exam device** blocked a webrequest to https://api.openai.com/v1/model, on 1/13/2025 5:16 AM.
- Detection 3: Suspicious Application named notepad.exe signed by Microsoft, does not have a valid memory signature. Strong indication of Memory Carving.

Example 4: A first-time user who requested cancellation during an Exam with Company A and is a new applicant for Company B.
Found 0 entries from hash, parameters: Billy Jones, person@gmail.com.

Note: We completely void your session when you press End Session and delete the data immediately. We email you and Company A the cancellation confirmation, Company B will never know you cancelled, this is done to ensure zero bias. When your interviewer or proctor is done assessing you, they press “Assessment Complete”, and your assessment details are sent to our servers and the application is automatically stopped from your system.

Your Data Rights You have the right to:

Access: Request a copy of your hashed data and assessment history.

Delete: Request deletion of your data, which we process promptly unless required by law to retain it (e.g., for audit purposes).

Correct: Dispute and correct inaccurate data, including flags.

Opt Out: Prevent your data from being shared with employers or third parties, except where legally required. We will inform our authorized third parties that you have specifically requested your data cannot be accessed. Your potential employer may decide what to do with this information.

To exercise these rights, email privacy@leetproctor.com or at support@cybersun.us with your request. We provide these services free of charge, requiring only basic verification (e.g., confirming the email used for the assessment) to protect your security. We process requests within 10–30 days, depending on complexity, and notify you of any delays.

If you disagree with our data retention practices, you may contact us at appeals@leetproctor.com or at support@cybersun.us to discuss your concerns. We aim to resolve inquiries transparently and promptly. For users in jurisdictions with specific data protection laws (e.g., EU, California), we comply with all applicable requirements, including shorter retention periods or enhanced rights where mandated.

Commitment to Fairness We process data only to ensure assessment integrity and provide accurate verification to employers. If no violations are detected (i.e., no Level 4 flags), your data remains private and is not shared beyond the hashed identifier’s verification purpose. Our flagging system undergoes regular audits to minimize errors, and we publish anonymized research on our methods to promote transparency.

For questions or support, contact privacy@leetproctor.com or at support@cybersun.us. We’re committed to protecting your data and upholding honesty in assessments.

16. WHAT MEASURES DO YOU TAKE TO ENSURE PROTECTION AGAINST DATA BREACHES?

We are committed to safeguarding your data with robust security practices. These include: Strong Access Controls: We use a Zero Trust approach, meaning every request to access our systems is verified to ensure only authorized users and devices can connect. Data Encryption: Your data is protected with industry-standard encryption during transmission and storage to prevent unauthorized access. Regular Security Audits: We conduct annual audits of our systems by independent experts to identify and address potential vulnerabilities starting from January 14.

Continuous Monitoring: We actively monitor our systems for suspicious activity and maintain up-to-date defenses against threats like hacking and malware.

17. DO WE MAKE UPDATES TO THIS NOTICE?

In Short: Yes, we will update this notice as necessary to stay compliant with relevant laws.

We may update this Privacy Notice from time to time. The updated version will be indicated by an updated "Revised" date at the top of this Privacy Notice. If we make material changes to this Privacy Notice, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this Privacy Notice frequently to be informed of how we are protecting your information.

18. HOW CAN YOU CONTACT US ABOUT THIS NOTICE?

If you have questions or comments about this notice, you may contact us by post at:

Cybersun Applied Technologies LLC, 30 N Gould St Ste N Sheridan, WY 82801 United States

or by email at

privacy@leetproctor.com or at support@cybersun.us

19. HOW CAN YOU REVIEW, UPDATE, OR DELETE THE DATA WE COLLECT FROM YOU?

You have the right to request access to the personal information we collect from you, details about how we have processed it, correct inaccuracies, or delete your personal information. You may also have the right to withdraw your consent to our processing of your personal information. These rights may be limited in some circumstances by applicable law. To request to review, update, or delete your personal information, please notify:
privacy@leetproctor.com or at support@cybersun.us.