Certn Privacy Statement

We are a technology company providing background checks and identity verification services. As privacy is at the core of our business, we put a lot of effort into ensuring we adequately protect the personal information of the individuals interacting with us. Your trust is crucial for us, and we are confident that this privacy policy will give you the information you need.

Key points you should know when we process your personal information

Our role in processing your personal information

We act as a "data processor" when we provide services to clients (e.g., employers, landlords), following their instructions regarding the collection and processing of data. It is the clients' responsibility to obtain the necessary consent and ensure the accuracy of the data. We act as a "data controller" when you interact directly with us (e.g., using our services, visiting our website, applying for a job at Certn). In these cases, Certn is responsible for protecting your data and respecting your rights.

Main Processing activities:

Certn processes personal information for:

- Providing services (background checks, identity verification)
- Communicate with you
- Ensure security and prevent fraud
- Comply with legal obligations
- Manage job applications (if applicable)
- Improve our services

We only process information based on a legal basis, such as your consent, a contract, a legal obligation, or a legitimate interest. We do not use your information for automated decision-making.

Information relating to our processing activities:

Detailed information about specific processing activities, including biometric identification, the list of Certn's subcontractors, and details about individual controls (e.g., judicial review, OneID, etc.,), can be found in the full Privacy Policy below. You can also contact us directly for further information.

Key information security measures:

Certn maintains SOC2, SOC3, and ISO27001 certifications. We use robust security controls, including:

- Regular security audits and penetration tests
- A security audit and data protection training for staff, suppliers, and subcontractors
- Limited access to personal information
- Encryption for data at rest and in transit

Rights of data subjects and complaints handling:

We review all privacy-related requests free of charge and take steps to help you exercise your privacy rights such as the right to: (i) information, (ii) access, (iii) rectification, (iv) erasure, (v) restriction of processing, (vi) data portability, (vii) withdraw consent and object to processing, (viii) refusal to be subject to a decision based solely on automated processing, and (ix) the right to lodge a complaint.

To exercise any of these rights or file a complaint, please contact our Privacy Office at privacy@certn.co. For residents of specific jurisdictions (Canada, US, EU, Brazil, Australia), specific contact information is available in the full version of the Privacy Policy. We will respond to your request promptly and within the legally required timeframes.

Certn's Privacy Statement may be updated periodically. Please review it regularly for any changes.

Privacy Policy

Version 3 / Effective June 30, 2025

I. Who are we and does this policy apply to you?

- Certn is a technology company that provides background and identity verification services.
- This privacy policy explains how Certn collects, uses, and shares the personal information of individuals who apply for employment at Certn, those who undergo a background check through Certn, customers who use Certn's services, prospective customers and website visitors.
- Certn does not knowingly collect information from children under the age of 13.

Certn is an information technology company that provides a wide range of identity and background products and services (the "**Services**"). This Privacy Policy (the "**Policy**") describes how Certn Holdings Inc. and its subsidiaries, including Certn (Canada) Inc., Certn (USA) Inc., Certn UK Ltd. And any other wholly owned subsidiary (collectively "**Certn**" or "**we**" or "**our**"), collects, uses, discloses, and processes Personal Information in connection with Certn owned websites("**Website**(**s**)"), and its Services.

This Policy applies to you if you are:

a. A "**Candidate**": A person who applies for a position at Certn.
b. A "**Consumer**": A person about whom we have received information for the purpose of using our website(s) or performing our Services.
c. A "**Client**": A person representing an organization or an individual using our Services.
d. A "**Prospect**": A person representing an organization or an individual whom we contact to find out about your interest in using our Services.
e. A "**Website Visitor**": An individual, a Consumer or a Client of legal age accessing our websites.

Please note that we do not knowingly solicit information from anyone under the age of thirteen (13). If you become aware of any Personal Information shared by or on behalf of a child, please contact us using the contact details provided in the relevant section below.

II. What is Personal Information and what do we do with it?

- Personal information, or personal data, is any information allows a person to be identified directly or indirectly, excluding business contact details.
- Certn collects, uses, stores, and shares only the personal information necessary to provide its Services.
- Generally, we process your personal information (i) to provide our services, (ii) to communicate with you, (iii) for security and fraud prevention, and (iv) to comply with the law. We may also use Personal Information for other purposes, subject to your consent.
- We will not process your personal information unless we have the legal right to do so. We process your personal information based on legal grounds like consent, contract, legal obligation, or legitimate interest.
- Certn does not use your information for automated decision-making.
- You can choose to limit the personal information you share, but this could affect the Services Certn can provide.

For the purposes of this Policy, "**Personal Information**" or "**Personal Data**" means any information that identifies, relates to, describes, can be associated with or could reasonably be linked, directly or indirectly, to an identified or identifiable individual.

Personal information does not include business information, such as our clients' business address and telephone number.

We only process the personal information necessary to provide our services. The term "**processing**" (or "**processes**" or "**processed**") refers to any operation or set of operations performed on personal information, whether by automated means or otherwise. This includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, transfer, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal information.

Certain information, including criminal records, credit information, and biometric data, may be considered sensitive or subject to special protections in certain jurisdictions. This information will not be collected systematically or where prohibited by law. Where permitted, it will be collected and used only in accordance with applicable laws.

We do not make any decisions about you, whether automated or not, and we do not seek to analyze or predict your behavior, preferences, interests, health status, or any other personal characteristics. However, we may carry out automated processing at the instruction of our Client.

By using our website or services, you consent to the processing of your Personal Information in accordance with the provisions of this Policy. **If you do not agree to this policy or do not wish to provide us with your Personal Information, please do not use our website or services.**

If you choose to limit the scope of the Personal Information you provide to us, we may not be able to provide you with all of our Services or offer you the best experience on our Website.

Generally, we process your Personal Information (i) to provide our Services, (ii) to communicate with you, (iii) for security and fraud prevention purposes, and (iv) for law enforcement and compliance purposes. We may also use your Personal Information for other purposes, subject to your consent. We will only process your Personal Information if we are legally permitted to do so.

To process your Personal Information lawfully, we rely on at least one legal basis, in accordance with applicable law. Depending on your relationship with us, the legal basis for processing your Personal Information may include, among other things, your consent, the obligation to process data for the performance of a contract with you, compliance with a legal obligation, or a legitimate interest.

If your consent is our legal basis for collecting and using your Personal Information, you may withdraw or modify it at any time for future collection or use of your Personal Information. We will explain the consequences of such a decision. If we use your Personal Information for commercial or marketing purposes, you may ask us to stop this type of use at any time, and we will do so.

II.1. When Certn conducts verification on behalf of its clients

- Certn acts as a "data processor" for its clients (such as employers or landlords) who use its services for background and identity checks. This means that clients tell Certn what information to collect and how, ensure they have the necessary legal basis and consent for the collection, and are responsible for the accuracy and protection of the data. Certn responds to client requests, protects the data, and complies with applicable laws. When Certn interacts with individuals, it does so on behalf of its clients and may share information with them.

- Customers must have a legitimate purpose (e.g., employment, rental) for the processing of their data. Certn will not reuse data without consent, legal obligation, or compatibility with the original purpose.

- Personal information is collected with your knowledge and consent, except where permitted or authorized by law.

- It is clients' responsibility to obtain your consent if Certn does not do so directly. You can withdraw your consent, which doesn't invalidate any prior processing.

- Each verification requires different information; therefore, it is possible not all the information described in the policy will be collected during every verification. For more information, please refer to the section of this policy relevant to your verification.

Our clients, such as your employer or landlord, may ask you to use our Services for background or identity verification purposes. In this case, please note that Certn acts as a "processor" when processing your Personal Information. This means that we act solely on behalf of our clients as a service provider when processing your Personal Information.

More specifically, when we provide Services to clients:

- The Client provides instructions on what Personal Information to collect, and how to collect it;

- Where applicable, the Client shall ensure that Consumers are informed of or consent to the collection and processing of their Personal Information in accordance with applicable laws;

- The Client ensures that Personal Information is collected and processed lawfully, fairly and transparently, in accordance with the identified purposes;
- The Client confirms that the Personal Information is accurate and, if necessary, kept up to date, corrected or deleted; and
- The Client shall ensure that appropriate safeguards are in place to protect Personal Information.

We are generally responsible for the following aspects of collection and processing of Personal Information:

- We perform the Services requested by our Client or Consumer, in accordance with their instructions;
- We protect the Personal Information in our custody against loss, theft or any unauthorized access, disclosure, copying, use or modification, in a manner appropriate to its sensitivity and in accordance with our client's instructions and applicable laws;
- We comply with all legal obligations we may have as a data processor, custodian, service provider or under other similar concepts in accordance with applicable laws.

In this regard, please note that although we may interact directly with you in connection with the Services requested by our Clients, we do so on behalf of our Clients, and any information or request shared with us may be communicated to our Clients when necessary to provide the Services.

II.1.1. Authorised processing purpose

Our Clients must certify that they have a legitimate purpose before we can process Personal Information for the purpose of providing the Services. " **Legitimate purpose** " includes employment purposes, rental purposes, or processing in accordance with the written instructions of the consumer with whom the Client intends to contract.

We will not reuse Personal Information for purposes other than those for which it was collected, unless one or more of the following conditions are met:

- The new use is compatible with the original, which means you should reasonably expect it;
- We have informed you of the new use and given you the opportunity to object to it; or
- The new use is also permitted or required by law.

We collect, use, and disclose Consumers' Personal Information when they are informed of the permitted purpose of the processing of that Personal Information and have given their consent to that processing, except where the processing of personal information without consent is permitted or required by law. Subject to regulatory requirements, the operation of our Services in certain jurisdictions requires that we or our Clients obtain additional or specific consents in the form of additional forms, telephone calls, via an online platform, or by other means. Where the Consumer does not provide us with this consent or specific consent directly, but rather provides it to our Clients, we require that the Clients also obtain the

Consumer's consent before providing us with their Personal Information, subject to verification for any of our Services. The Consumer may withdraw this previously given consent at any time by contacting us. Withdrawal of this consent does not affect the lawfulness of any processing based on consent before its withdrawal.

You can find more information about the types of Services our Clients may ask you to use in the relevant section of this Policy. Please note that, depending on the type of verification our clients ask you to complete, we may not process all the Personal Information listed in that section. You can refer to the name of the verification you are required to complete in the Policy for more information about how your Personal Information is processed.

II.2. When interact directly with Certn

- Certn acts as a "data controller" of your personal information in certain situations, for example when you directly use our services, browse our website, consent to marketing contact, or apply for a job with us. In these cases, we are responsible for protecting your data and respecting your rights.
- We may process your personal information to provide services, manage applications, track our performance, comply with laws, improve our offerings, ensure quality, train employees, maintain security and prevent fraud.
- When providing services, we do not directly collect financial information; payments are securely processed by third-party providers.
- We may record calls for insurance and training purposes.

There are situations where Certn does not act on behalf of its Clients when processing your Personal Information. This can occur in the following cases:

- When you ask us directly to provide you with our Services or when you browse our Website.
- When you consent to be contacted by us for marketing purposes.
- When you apply for a job at Certn.

In these circumstances, we act as "data controllers" under applicable data protection laws. This has implications for you, because as data controllers, we are primarily responsible for respecting your rights regarding your Personal Information and for ensuring its adequate protection in accordance with applicable data protection laws.

In these circumstances, subject to your consent or the applicable legal basis and in accordance with applicable laws, we may process your Personal Information for the following purposes:

- To provide you with the requested services
- If you apply to Certn, to process your application or to contact you about job opportunities
- To monitor the performance of our Services and websites

- Comply with applicable laws and regulations
- To improve our services
- Quality assurance and quality controls
- To train our employees
- To ensure the security of our services, websites and assets
- Detecting and combating fraud

Additional information regarding call recordings: We may record calls for training and quality assurance purposes. While we rely on our legitimate interest to do so, we also ensure that you are informed beforehand about these recordings. If you do not wish your call to be recorded, you can use our chat agent or contact us by email at support@certn.co .

Additional information regarding quality assurance and controls: Our processes for collecting and transcribing Personal Information are automated to the greatest extent possible and are subject to rigorous quality controls. Information found to be inaccurate, either during our own audits or following your request for correction, is updated.

To ensure the effectiveness of our processes and systems, we audit them frequently. These audits may involve the processing of your personal information (for example, to ensure the accuracy of the checks performed).

Additional information regarding the provision of our Services: When registering for our Services, you may be asked to enter your full name, email address, company name and address, phone number, billing address, card address, and other customer-provided information via custom fields, if applicable. We never collect financial information, such as your payment method details (e.g., valid credit card number, card brand, expiration date), either through our website or otherwise. When processing payments, you are redirected to a secure page on the Stripe website or that of another PCI DSS-certified payment service provider. This page may feature our branding, but it is not managed by us. All financial information is processed by our payment processor. We encourage you to review their privacy policy and contact them directly with any questions.

More information regarding the performance tracking of our Services and Websites: When we monitor the performance of our Services and Websites, we use information that cannot directly identify you, including by aggregating it or using other depersonalization and anonymization techniques.

Please also note that we may record your operating system name and version, device identifier, browser type, operating system, IP (Internet Protocol) address, screen resolution, pages viewed on our websites, length of visit, access times, general location information such as city, state, or geographic area, and information about your use of and actions on our websites. We may use this information for fraud prevention and security purposes.

The collection of personal information for security purposes is carried out on the basis of our legitimate interest and our legal obligation to ensure the protection of the personal information in our custody.

II.2.1. Things to know when you use MyCertn Wallet

MyCertn Wallet is designed to give you greater control over your personal information. It allows you to order specific checks and decide when, to whom, and for how long you want to share the results of those checks.

Here are some key points you should be aware of when using MyCertn Wallet:

- Because we act on your instructions, it is your responsibility to ensure that you know and authorize the recipient before sharing your personal information via MyCertn Wallet. We recommend that you review the recipient's privacy policy before disclosing your personal information.
- You can access verification results, request their removal, dispute or correct any inaccuracies associated with your personal information in the MyCertn Wallet application.
- You can find more information on how we process your personal information based on the checks you order via MyCertn Wallet in the relevant section of this policy.

II.2.2. Certn's use of artificial intelligence

We use artificial intelligence technologies to automate and optimize our internal processes and the delivery of our Services. This includes the use of AI agents such as chatbots and AI voice agents. We do not use AI to make automated decisions that could have legal consequences or significantly affect you. Our AI implementation is designed to improve operational efficiency while ensuring full human oversight.

II.2.3. Use of cookies and similar technologies by Certn

Certn uses cookies to improve website functionality and personalize your experience. Some cookies are essential for the website to function, while others help us analyze your website usage and remember your preferences, with your consent. You can manage your cookie preferences through your browser settings.

Our website uses cookies and other similar technologies to provide functionality, analyze traffic, and personalize some of your web content**.**

II.2.3.1. What are cookies?

Cookies are small text data files that are sent to your computer or mobile device by a website when you browse.

There are different types of cookies with different functions:

- **Session cookies** :They are stored on your computer only during your web session. They are automatically deleted when you close your browser. They typically store an anonymous session ID that allows you to browse a website without having to log in on each page. They do not collect any information from your computer.
- **Persistent cookies** :A persistent cookie is a file stored on your computer that remains there even after you close your browser. It can be read by the website that created it on your next visit.
- **First-party cookies:** These are used to remember your preferences for a specific website with the entity that owns that website. They are stored and transmitted between Certn's servers and your computer's hard drive. They are used solely for the personalization you have defined. These cookies can be session cookies or persistent cookies.

- **Third-party cookies:** This type of cookie is used to remember your interactions with a particular website for an entity that does not own it. They are stored and transmitted between a third-party server and your computer's hard drive. These cookies are generally persistent.

First-party cookies are necessary for the proper functioning of our website. Our website also allows the use of third-party cookies, which can be read externally by other organizations. Therefore, we cannot be held responsible for third-party cookies, i.e., cookies that we do not use. Our service platforms, which we use to collect information from our consumers and clients, do not use third-party cookies.

II.2.3.2. Use of cookies

Necessary cookies: By using our website, you agree to our storing and accessing necessary cookies on your device. These cookies do not collect any information about you that could be used for marketing purposes or to remember your browsing history.

Statistical cookies: These are anonymous and do not allow us to identify you. They help us improve the functionality of our website and collect information about your use of the site (frequency of visits, links clicked, favorite pages, etc.). By accepting these cookies, we can generate anonymous statistical reports for the purpose of improving the website.

Preference cookies: To remember your choices (such as your selected language or saved username and password), to allow for faster browsing, and to offer you enhanced features, we need to enable preference cookies. The information collected by these cookies is generally anonymized.

Marketing cookies: These can be installed on websites by third parties. They do not store personal information, but identify your browser and connected device to allow advertisers to show you relevant ads.

Website log data: Certn's web servers record the following information when you visit our website: IP addresses, operating system type, time and duration of visit, web pages viewed, and browser type. We do not link server log information to any other information that could identify visitors to our website. In addition to analyzing these logs to provide you with a better experience on our website, they may be accessed for security purposes and, if necessary, to detect any unauthorized activity on our site. In such cases, server log data, including IP addresses, will be shared with law enforcement so they can identify users in their investigations of unauthorized activities.

II.2.3.3. How can I manage my Cookie preferences?

Information about our cookies will be presented to you during your first visit to our website, and then occasionally via the cookie banner. You can accept or reject all cookies at any time while browsing the website. You can choose and manage your cookies at any time through your browser settings. If you disable cookies, you may not be able to access or use certain parts or features of the website.

II.3. What you need to know depending on the type of checks carried out by Certn

- Certn processes a minimum of identifying information, including full name, date of birth, address history, telephone number, and email address, for all background checks to ensure their accuracy. We use this information, along with other data, to verify the identity of the individuals concerned.
- This section outlines the main checks carried out by Certn and may not contain information about the specific check you require or are asked to perform. Further information regarding specific checks, such as drug tests or Right to Work checks, is available in the relevant consent forms and documentation, or by contacting us.
- Each verification is unique and it is possible that we may not always process all of the listed Personal Information.
- The processing may also involve information from different jurisdictions depending on your personal circumstances.

All our controls require us to process, at a minimum, the following personally identifiable information:

- Full name, including maiden name and aliases
- Date of birth
- Address history
- Phone number and email address.

This information, combined with that required for any identity verification, allows us to ensure that the verification is for the correct person. If you are required to complete multiple verifications, you can use the sections below to obtain more information about the personal information we need to process, the reasons for this processing, the source of the information, and how long we retain your personal information. Please note that each verification is unique, and we may not process all the personal information listed below. Depending on your individual circumstances, we may also need to process your personal information from different jurisdictions (for example, if you have worked or lived in different countries).

The list below is not exhaustive and may not include information relevant to the check you are undergoing. For example, in some countries, such as the United States, Certn may offer drug screening tests, or in the United Kingdom, checks related to the Right to Work. For more information on how we process your personal information during these specific checks, please see the consent form and related documentation or contact us.

II.3.1. OneID

OneID	**Personal information concerned**	Full name, including maiden name and aliases
		Date of birth

		Address History
		Phone number and email
		Identity documents such as passport or driver's license
		Biometric data (facial characteristics)
	Purposes of the processing	Identity verification, fraud detection and prevention
	Source(s)	Provided by you
	Storage periods	30 days from the date of biometric data collection
		3 years from the date of collection of contact details and results of the check
	More information	For more information, please read our Biometric Notice .

II.3.2. Identity Verification

Identity verification	**Personal information concerned**	Full name, including maiden name and aliases
		Date of birth
		Address History
		Phone number and email
		Identity documents such as passport or driver's license
		Biometric data (facial characteristics)
	Purposes of the processing	Identity verification
		Fraud detection and prevention
	Source(s)	Provided by you

	Storage periods	30 days from the date of biometric data collection
		3 years from the date of collection of contact details and results of the check
	More information	For more information, please read our Biometric Notice .

II.3.3. Canadian Criminal Record Check

Canadian criminal record	**Personal information concerned**	Place of birth
		Police files
		Court files
		Criminal record
		Status of the sex offenders registry
	Purposes of the processing	Criminal background check
	Source(s)	Provided by you
		Law enforcement and government agencies
		Courts and public archives
	Storage periods	3 years from the date of collection
	More information	For more information, please read our Biometric Notice .

II.3.4. International Criminal Check

International criminal record check	**Personal information concerned**	Sex
		Police files

		Court files
		Criminal record
		Passport details or similar information such as identification number, visa information, and jurisdiction-specific documents
	Purposes of the processing	Criminal background check
	Source(s)	Provided by you
		Law enforcement and government agencies
		Courts and public archives
	Storage periods	3 years from the date of collection

II.3.5. Employment Verification

Employment verification	**Personal information concerned**	Employment history (including company name, contact information, fiduciary or managerial responsibilities, positions, titles, income, or start and end dates)
	Purposes of the processing	Verification of employment or activity history over a certain period of time
	Source(s)	Provided by you
		Previous employers
		Employment verification providers
		References you provided
	Storage periods	3 years from the date of collection

II.3.6. Education Verification

Education verification	**Personal information concerned**	Post-secondary information (including the name of the institution, the address of the institution, the title of the degree/certification and the dates of enrollment)
	Purposes of the processing	Checking educational or activity history over a certain period of time
	Source(s)	Provided by you or our client (as applicable)
		Educational institutions
		Education verification providers
		Government educational authorities
	Storage periods	3 years from the date of collection

II.3.7. Creditworthiness Report (Canada)

Creditworthiness Report (Canada)	**Personal information concerned**	Employment history (including name, contact information, fiduciary or managerial responsibilities, positions, titles, income, or start and end dates)
		Financial information (including credit history, bankruptcies or financial judgments)
	Purposes of the processing	Credit and bankruptcy history check
	Source(s)	Credit bureaus
		Government agencies
		public documents
	Storage periods	3 years from the date of collection

II.3.8. Income Verification

Income verification	**Personal information concerned**	Bank details (including bank name, account balance, account activity trends, account balance trends, recurring deposits, recurring payments, and account age)
		Income information (including income sources, average monthly income, estimated gross annual income, employer income, non-employer income, or income trends)
	Purposes of the processing	Verification of your income
	Source(s)	Financial institutions
		Revenue verification providers
	Storage periods	3 years from the date of collection

II.3.9. Verification of adverse media

Verification of adverse media	**Personal information concerned**	Activity on social media (posts, interactions, etc.)
		Mentions in online or print media
	Purposes of the processing	Verification of adverse media
	Source(s)	Print and digital media
		Law enforcement and government agencies
	Storage periods	3 years from the date of collection

II.3.10. Verification of politically exposed persons (PEPs)

Politically Exposed Persons (PEP) screening	**Personal information concerned**	Work address
		Inclusion on watchlists or sanctions lists
		Financial Conduct Authority reference number (if applicable)

		Family or business relationships with politically exposed persons
	Purposes of the processing	A check to determine if you hold or have held a prominent public position or role that exposes you to potential risks of corruption, bribery, or money laundering.
		Verification of global sanctions regimes and sanctions lists
		Verification of adverse media
	Sources	Global watchlists and registries
		Law enforcement and government agencies
		Regulatory bodies
	Storage periods	3 years from the date of collection

II.3.11. Global Sanctions and Watchlists

Global sanctions and watchlists	**Personal information concerned**	Inclusion on watchlists or sanctions lists
	Purposes of the processing	Verification of global sanctions regimes and sanctions lists
	Sources	Global watchlists and registries
		Law enforcement and government agencies
		Regulatory bodies
	Storage periods	3 years from the date of collection

II.3.12. Questionnaire

Quiz	**Personal information concerned**	Any additional information submitted voluntarily by you

	Purposes of the processing	Provide Certn's clients with the additional information they need during the requested audits.
	Sources	Provided by you
	Storage periods	3 years from the date of collection

III. How do we protect your Personal Information?

III.1. Our approach to data protection

At Certn, we are committed to protecting your privacy and personal information. We have implemented a comprehensive compliance framework based on key principles. We are responsible for protecting your information and have appointed a Data Protection Officer to oversee our practices and ensure compliance with applicable laws. We identify the purposes for collecting your information in advance and only collect it when permitted by law or with your consent. We limit data collection to what is strictly necessary, minimizing it throughout its lifecycle through strict retention policies. We ensure the accuracy of your data through technical controls and audits, allowing you to easily correct any inaccuracies. We protect your information with robust safeguards and train all individuals who handle it. We are transparent about our data protection practices and ensure our documentation is clear. We also respect your rights regarding your personal information and have implemented a complaints handling procedure. We regularly review our compliance. Our services are designed with confidentiality (state-of-the-art security), ease of management (individual data control) and predictability (transparent practices) in mind.

At Certn, we are committed to protecting your privacy and personal information. We have implemented a comprehensive framework that outlines our objectives and principles for handling personal information and defines our privacy governance as an organization. This framework is based on the following key principles:

- **Responsibility:** We take responsibility for protecting your personal information. We have established a privacy office to oversee our privacy practices and ensure that we comply with all applicable laws.
- **Identification of purposes:** We have put in place processes to ensure that the purposes for which your personal information is collected are identified beforehand.
- **Legal basis, including consent** : We only collect and use your information when permitted by law or when you give us your consent. We will ensure that you understand what you are agreeing to.
- **Limitation of the processing of personal information:** We only collect the personal information necessary for the purposes we have identified.

We also strive to minimize the amount of personal information required throughout its lifecycle. This is achieved, in particular, through the implementation of strict retention periods. You will find more information about our retention practices in the relevant sections of this policy.

- **Accuracy:** We ensure that your information is accurate and up-to-date, notably through rigorous technical and quality controls and audit processes. We make it easy for you to correct any errors or inaccuracies.
- **Guarantees** : We protect your information with strict security measures, including physical, technical, and administrative safeguards. We also ensure that all individuals who process your information are properly trained.
- **Transparency:** We are open about how we collect, use, and protect your Personal Information. We ensure that our documentation regarding the processing of your Personal Information is written in a clear and understandable format.
- **Rights of individuals:** You have rights regarding your Personal Information, including the right to access, correct, or delete it. We make it easy for you to exercise these rights.
- **Compliance challenges** : We have a procedure in place for you to file complaints or ask questions about our privacy practices. We also regularly review our own compliance with privacy laws.

We ensure that your personal information is processed in accordance with these principles.

Furthermore, in accordance with our privacy framework, our services are designed to pursue these three main objectives:

- **Confidentiality:** We implement state-of-the-art security measures to protect personal information and train our staff members on best practices.
- **Ease of management:** We design our services to allow individuals to control their Personal Information, including giving them the ability to modify, delete or selectively disclose it.
- **Predictability:** We maintain transparent practices that allow individuals to make reliable assumptions about how we handle their Personal Information.

III.2. How long do we keep your Personal Information?

Certn retains your personal information to the extent necessary to provide services, comply with legal obligations, and enforce agreements. We delete your account and data upon request, although some information may be retained for legal reasons. Unless otherwise instructed by our clients, consumer information is generally retained for a maximum of three years, with exceptions for specific data types such as biometric data (30 days) and applicant information (3 years).

In accordance with our retention policy, we will retain your information for as long as necessary to provide you with our services and/or to comply with our contractual and legal obligations, resolve disputes and enforce our agreements.

Data necessary to establish proof of a right or contract will be retained for the period stipulated by applicable law. Upon your request to close your account, we will deactivate or delete your account and information from our active databases. However, certain information may be retained in our files to prevent fraud, resolve issues, assist in investigations, enforce our terms and conditions, and/or comply with legal requirements.

Regarding Consumers' personal information, unless our Clients have requested its deletion or a different retention period, the retention and disposal period will not exceed three (3) years. More specific information about our retention periods, based on the controls we perform, can be found in the relevant section of this policy. Exceptions may exist for specific data sets, in accordance with regulatory requirements or the retention requirements of third-party data providers. For example, we will retain your biometric data for 30 days after the completion of your OneID identity verification. Where necessary, we may retain general log information and information for auditing purposes.

If you are a candidate, we will keep your personal information for a maximum of three years.

III.3. How do we protect your Personal Information?

We are SOC2, SOC3, and ISO 27001 certified and maintain advanced technical, administrative, and physical security controls that comply with these standards and protect your Personal Information from unauthorized access, loss, misuse, interference, or alteration during its collection, use, disclosure, and storage on our site. We regularly conduct security audits, vulnerability assessments, and penetration tests to ensure compliance with industry security practices and standards.

All our staff, suppliers, and subcontractors undergo background checks before being hired. All staff members are trained in data protection and are aware of their responsibilities. This training is provided repeatedly, either regularly or randomly, but at least once a year.

We limit access to Personal Information to individuals with a legitimate business need, consistent with the purpose and objective for which the information was provided. We implement various security measures to maintain the safety of your Personal Information when orders are placed or when you enter, submit, or access your personal information. For example, we use encryption at rest and in transit. All sensitive information provided is transmitted via Transport Layer Security (TLS) technology and then stored in our database. It is accessible only by individuals with special access rights to our systems, who are bound by confidentiality agreements.

In addition, we have implemented processes to encourage our clients to comply with applicable privacy laws and security standards. These processes include, among other things, entering into binding agreements with our clients and conducting random mutual audits of each other's internal procedures and practices to ensure that regulatory standards and security levels are mutually met and exceeded at all times.

IV. How and to whom can we disclose your personal informatio?

Certn processes personal information globally and stores data in Canada, the United States, the United Kingdom, and Australia. We may transfer data across borders to provide services such as employment or education verification. These transfers are based on adequacy decisions, contractual and security safeguards, consent, or other legal considerations. We take steps to ensure data security and comply with the specific requirements of regions such as California, Quebec, the United Kingdom, Australia, the EU, and the EEA. We may share personal information with auditors, affiliates, partners, and service providers such as payment processors and cloud providers. We do not sell or disclose personal information to governments, marketing services, or other clients unless required by law or as stated in this policy. We may disclose information to law enforcement authorities or similar bodies if legally required to do so.

IV.1. Does Certn process personal information cross-border?

Certn operates globally and may need to transfer your Personal Information across borders as part of its business operations. We rely on storage infrastructure in Canada, as well as in the United States, the United Kingdom, and Australia. We may also process your Personal Information across borders to provide you with the Services, for example, to verify your employment or education history. When we transfer Personal Information to you, we rely on, among other things, the following:

- Suitability decisions
- Appropriate safeguards, including contractual ones
- Your consent
- Other jurisdictional considerations.

In cases where our client is located, or the consumer resides or has resided, in the State of California, the Province of Quebec, the United Kingdom, Australia, the EU and/or the EEA, specific requirements may apply to the transfer of Personal Information.

We take all steps reasonably necessary to ensure that your Personal Information is treated securely and in accordance with this Policy, and we will not transfer Personal Information to an organization or country unless adequate controls are in place to ensure the security of your data.

If you are wondering whether your information will be processed abroad and/or if you have any restrictions or conditions regarding the disclosure of your information abroad, please contact us as soon as possible so that we can discuss your specific needs.

IV.2. Third Parties

We only share your personal information with third parties with your consent, or when permitted or required by applicable regulations.

In addition to the third parties listed in the section on types of controls, we may share or disclose your Personal Information to the following third parties in the course of our business activities:

- Auditors for conducting contractual audits or statutory compliance audits;
- Certn's affiliates and partners who participate in providing our Services; and
- Third parties who provide services for us or on our behalf, including, but not limited to, payment processing, marketing or advertising services, data analysis, email sending, software as a service providers, infrastructure as a service providers, or platform as a service providers.

When we provide Services to a Customer, the Consumer's Personal Information is processed and reported through our secure platform. In addition to our Customers and authorized Certn personnel who may access your Personal Information for the purposes described in this Policy, we may provide your Personal Information to authorities or partner companies that provide services to assist us in our business operations, such as offering customer service or processing your payment. For more information about the third-party companies that provide us with such services, please click here.

Finally, please note that we do not sell or disclose your Personal Information to governments, marketing or advertising services, other clients or any other person, except as described in this policy or when required by law.

IV.3. Government entities

In exceptional circumstances, we may be required to disclose personal information to law enforcement agencies, national security agencies, courts, or other similar institutions, as required by law. Upon receipt of a production order, subpoena, warrant, or any other enforceable request, we will act in accordance with applicable laws.

V. Essential information tailored to your country and how to contact us to assert your rights

- We are committed to protecting your privacy and ensuring your rights are respected. Regardless of where you live, you have the right to be informed, access, rectify, erase, restrict processing of, and obtain data portability, as well as the right to withdraw your consent, object to processing, not be subject to automated decision-making, and lodge a complaint. We will review your privacy requests free of charge and respond promptly, within the legally required timeframes. We may need to inform our clients or other third parties who have processed your data before complying with your request.
- You can contact our privacy office by email at privacy@certn.co or, if you reside in certain jurisdictions (Canada, USA, EU, Brazil, Australia), use the contact details provided for your place of residence.
- We may update this policy periodically, so please check it regularly.

V.1. Your rights

Certn is committed to ensuring that your rights regarding your Personal Information are respected in all jurisdictions where it operates.

Regardless of your jurisdiction, we grant the following rights to individuals whose Personal Information we process. If you reside outside the jurisdictions described below, please see the details provided to exercise your rights.

Regardless of where you live, we will review any privacy request free of charge and take steps to help you exercise your privacy rights: (i) information, (ii) access, (iii) rectification, (iv) erasure, (v) restriction of processing, (vi) data portability, (vii) withdrawal of consent and objection to processing, (viii) refusal to be subject to a decision based solely on automated processing, and (ix) lodging a complaint.

If you do not reside in one of the jurisdictions listed below, you can contact our Privacy Office at privacy@certn.co to exercise your privacy rights. If you reside in one of these jurisdictions, please use the contact information provided in the section that applies to your situation.

Upon receipt of a written request and after verifying that you are indeed the data owner, we will respond to requests, disputes, and complaints concerning your privacy rights as soon as possible and, in any event, within the time limits prescribed by law. However, if we refuse your request, we will send you a written explanation within 30 days of receiving it.

For compliance purposes and where required by law or contract, before complying with any privacy request, we will inform the Client involved in the request, if applicable, as well as any other third parties who may have processed your Personal Information. On their instructions, we will respond to your request accordingly. You may challenge their decision by contacting them directly or by contacting your local data protection or privacy authority.

V.1.1. Right to be informed

You have the right to be informed about the nature of the processing of your personal information. You have the right to know what personal information we process, with which third parties it may be shared, and how long we will retain it.

V.1.2. Right to access

Subject to the exceptions provided by applicable law, you have the right to access the Personal Information that Certn holds about you or on behalf of its Clients. You can request that we provide you with your Personal Information using the contact details provided in this Policy or the tools and forms we make available to you in our various Services.

V.1.3. Right to rectify, correct or update your Personal Information

Subject to the exceptions provided by applicable law, you have the right to access the Personal Information that Certn holds about you or on behalf of its Clients. You can request that we provide you with your Personal Information using the contact details provided in this Policy or the tools and forms we make available to you in our various Services.

V.1.4. Right to erasure or deletion

You have the right to request the deletion or erasure of your Personal Information. This right is exercised in accordance with applicable laws and may be limited depending on the nature, scope, and laws applicable to your request. Certn may retain some of your Personal Information when required or permitted by applicable laws. For example, we may need to retain your Personal Information to demonstrate our compliance with data protection or privacy laws. If you request the deletion of your Personal Information, we must retain certain information regarding your request for deletion and our compliance with your request.

V.1.5. Right to portability

You have the right to obtain your Personal Information in a structured, commonly used, and machine-readable format and to request that we transmit it to another qualified third party under applicable law. This right is limited to Personal Information that you have directly provided to us.

V.1.6. Right to withdraw your consent and right to object

Subject to the exceptions set forth in applicable law, you have the right to withdraw your consent if we rely on it to process your Personal Information. In this case, please note that we may no longer be able to provide the services. If the Services are requested for purposes authorized by the Client, such as employment or rental, this may affect related processes. Where possible, we encourage you to contact the tenant, employer, or organization that requested the verification to obtain further information about the consequences of withdrawing your consent.

You have the right to object to specific processing activities involving your personal information, depending on the legal framework that applies to your situation. For example, you have the right to object to the processing of your personal information for direct marketing purposes, including profiling.

V.1.7. Right to restriction of processing

Under the circumstances provided for by applicable laws, you have the right to ask us to restrict the processing of your personal information.

V.1.8. Right to not be subject to a decision based solely on automated processing

Certn does not use your Personal Information to make decisions based solely on automated processing.

V.1.9. Right to file a complaint

If you have any concerns about our data protection practices or the handling of your personal information, you can file a complaint with our Privacy Office. Contact information can be found in this Policy.

V.2. Canada Residents

You will find detailed information about our policies and processes relating to the protection and retention of your personal information in the relevant sections of this policy.

As indicated in the sections above, please note that Certn may transfer your personal information outside of Canada, including outside the province of Quebec, whenever necessary for the purposes for which it was collected.

V.2.1. Personal Information Agent (Quebec)

Certn is a registered Personal Information Agent in Quebec. In this regard, please note that:

- We hold personal information about other people.
- We may provide our Clients or other contracting parties with credit reports relating to your character, reputation or creditworthiness, and we may receive such information from our contracting parties such as our partners or service providers.
- You have the right to request access to or rectification of your Personal Information by following the procedure described in this policy.
- Certn ensures that your personal information is up-to-date and accurate by implementing rigorous technical controls such as automated processes, quality controls, and internal audits. Certn also offers you the opportunity to challenge or correct the information we collect about you, either directly with you or with our clients and partners.

V.2.2. Who to contact?

For any questions, complaints or requests regarding this policy you can contact our Privacy Officer at the following address:

CANADA Certn (Canada) Inc.	1006 Fort St Unit 300 Victoria, BC V8V 3K4 +1-844-987-0690 privacy@certn.co

V.3. Residents of the United States

V.3.1. Your rights under the Fair Credit Reporting Act

As a U.S. resident, please be aware that some of the personal information processed by Certn may be subject to the *Fair Credit Reporting Act* ("FCRA"), and that your state's privacy laws may be overridden by this federal law. Unless you have applied for a position at Certn, we do not make any decisions regarding your employment. For more information about the FCRA, your rights under this law, and how it may apply to your situation, please contact your employer.

V.3.2. California Residents

For the purposes of the California Consumer Privacy Act ("CCPA"), we do not sell consumers' personal information to third parties for direct marketing purposes. Personal information processed as part of a background check is not subject to the CCPA.

If you are a California resident and we have processed categories of your Personal Information beyond the CCPA exemption for a background check, you have the right to access, delete, disclose, refuse the sale of, and be free from discrimination against your Personal Information. You may contact us to exercise any of these rights. For compliance purposes, we may request additional information from you to fulfill your request.

V.3.3. Nevada residents

We do not sell consumers' personal information to third parties for direct marketing purposes.

V.3.4. Who to contact?

For any questions, complaints or requests regarding this policy, you can contact our Privacy Officer at the following address:

UNITED STATES Certn (USA) Inc.	Trust Center 1209 Orange Street Wilmington, New Castle County, Delaware, 19801 +1-844-987-0690 privacy@certn.co for any privacy-related questions

V.4. Residents of the EU, EEA, Switzerland and the United Kingdom

Given that we occasionally process Personal Information of residents of the EU, EEA, Switzerland and the UK, we have taken steps to comply with these jurisdictional standards and ensure that all recipients of such Personal Information provide an adequate level of data protection based on, but not limited to, commitments under standard contractual clauses and/or international data transfer agreements, as appropriate.

Consumers in the EU, EEA, Switzerland, and the UK have certain rights regarding the processing of personal information. If you are an EU/EEA/UK resident, you have:

- The right to request details of the personal information we hold about you;
- The right to request that we update your information if it is inaccurate or incomplete;
- The right to request that we delete your information under certain circumstances;
- The right to withdraw your consent to the use of your information when we rely on that consent;
- In certain circumstances, you have the right to receive some of your information in a usable format and/or to request that we transmit this data to a third party where technically possible;

- The right to request that we limit the processing of your Personal Information in certain circumstances; and
- The right to lodge a complaint with your local data protection authority if you feel we have not been able to help you.

If you wish to exercise your rights regarding your background report, we will respond to your request in our capacity as data processor and in accordance with our client who commissioned the report, acting as the data controller. In this case, please note that our clients are ultimately responsible for responding to your request.

To register your request, please contact us. We will contact you if we need additional information from you to provide the applicable information or to take specific actions to follow up on your request regarding the exercise of your rights.

V.4.1. Who to contact?

For any questions or requests regarding this policy, you can contact our data protection officer at the following address:

UNITED KINGDOM Certn (UK) Limited	160 London Road Sevenoaks, Kent, TN13 1BT +44 (0)1732 748 900 support@certn.co for general queries and dpo.emea@certn.co for privacy-related queries

V.5. Brazil

Residents of Brazil may be entitled to certain rights:

- Confirm whether we process your personal information;
- Request access to your personal information that we process;
- To correct incomplete, inaccurate or outdated personal information;
- Request the anonymization, blocking or deletion of unnecessary or excessive information or information processed in violation of the provisions of the LGPD (Lei Geral de Proteção de Dados Pessoais);
- Request data portability;
- To be informed of the third parties with whom your Personal Information has been shared; and
- Request a review of automated decisions that affect your interests.

To exercise your rights relating to your consumption report, we will support your request in our capacity as a subcontractor and in agreement with our client who ordered the report in their capacity as data controller.

To register your request, please contact us using the contact details provided below. We will contact you if we require further information from you to provide the applicable information or to take specific actions to honor your request and exercise your rights.

V.6. Australia

Certn conducts checks in Australia through its subsidiary InterCheck. For more information on how Intercheck handles your personal information, please visit: https://intercheck.com.au/privacy-policy/.

For any questions, complaints or requests regarding this policy, you can contact our privacy officer at the following address:

Australia	356 Collins Street Melbourne, 3000, Victoria +61 (03) 8820 4069 apac-privacy@certn.co for privacy-related questions or inquiries and help@intercheck.com.au for any other questions.

VI. How is the policy updated?

We reserve the right to modify this Policy at any time. All website visitors are encouraged to review this Policy regularly to stay informed of updates. By continuing to use our website and services after the posting of changes to this Policy, you accept the new revised policy and agree to be bound by it.