



TERRAHUB



Credivera

PRIVACY POLICY

Effective Date: June 10, 2026

1. Purpose and Scope

TerraHub Technologies Inc., doing business as Credivera ("Credivera", "we", "us", or "our") is committed to protecting the privacy of all individuals with whom we interact. This Privacy Policy ("Policy") describes how we collect, use, disclose, retain, and protect personal information across all of our products and services, including:

- Our website at www.credivera.com (the "Website")
- Our Credivera Wallet (native mobile app, iOS and Android)
- Our Credivera Exchange platform and web wallet
- Our Credivera Verification Services (identity, education, and criminal background verification)
- Our Credivera Access Services (verifiable credential-based authentication)
- Our Verifiable Credential Infrastructure (DID hosting, Status List, Key Manager)
- Any other services or tools we provide to individuals or organizations

Please read this Policy carefully. By using any of our services or providing personal information to us, you acknowledge that you have read and understood this Policy. If you do not agree with our practices, please discontinue use of our services.

This Policy may be updated from time to time. We will notify users of material changes by posting a revised version with an updated effective date. Continued use of our services after changes are posted constitutes acceptance of the revised Policy.

2. About Credivera

Credivera is a digital trust platform that enables the issuance, management, and verification of workforce credentials. Our services are designed to support individuals, employers, credential issuers (such as training providers and regulatory bodies), and verifiers (such as employers and compliance officers) across regulated industries including, but not limited to, healthcare, skilled trades, public sector, and real estate.

Our current products and services include:

- **Credivera Exchange:** A cloud-hosted digital trust platform enabling individuals to manage verifiable digital credentials via a server-side web wallet, while allowing organizations to maintain workforce compliance through credential issuance, verification, and compliance monitoring.
- **Credivera Verification Services:** A suite of identity, education, and criminal background verification services, each delivered via integrations with trusted third-party verification providers. Credivera does not conduct these checks in-house. Verification types include: Identity Document Verification (IDV); IDV+ (including lookups against government registries such as motor vehicle records); Education Verification (Canada, United States, and Global); and Criminal Background Checks (Canada, United States, and Global). Users are informed of the specific verification type and applicable third-party provider before any check is initiated.
- **Credivera Wallet (free):** A native mobile wallet application (iOS and Android) that allows individuals to claim, store, manage, and present verifiable digital credentials entirely on their local device. The Wallet collects no data and transmits nothing to Credivera without explicit user action.
- **Credivera Access Services:** A verifiable credential-based authentication service built on the Keycloak identity and access management platform, enabling passwordless authentication and access control via verifiable digital credentials.
- **Verifiable Credential Infrastructure:** The underlying technical infrastructure supporting verifiable credential operations, available as bundled platform components or standalone services. This includes: DID (Decentralized Identifier) creation and hosting; Status List management for tracking and publishing credential status; Key Manager for encryption key management; and transaction-based services for credential issuance and revocation.



TERRAHUB



Credivera

- **Trust Registry and Business Verification (KYB):** Credivera intends to offer trust registry listing services and automated business verification capabilities in the future. These services are not yet available. This Policy will be updated prior to launch to reflect any new data processing activities.
- **Professional Services:** Statement of Work engagements for custom development or professional services governed by the applicable statement of work and this Policy.

Credivera operates as a data processor and/or data controller depending on the context in which personal information is handled. We act as a controller with respect to information we collect directly from website visitors, Exchange users, and users of our other hosted services. We act as a processor on behalf of credential issuers, verifiers, and enterprise customers who use our Platform and APIs under contractual data processing agreements. When Verifiable Credential Infrastructure components are used as standalone services integrated into a customer's own systems, Credivera acts as a data processor for personal information processed through those integrations. For Credivera Verification Services, Credivera acts as an intermediary to the applicable third-party verification provider; that provider's own privacy policy applies to the processing it conducts, and users will be directed to that policy before any verification check is initiated.

Our Privacy Principles

Privacy is not an afterthought at Credivera — it is foundational to what we build and how we operate. Our approach to personal information is guided by four core principles:

- **Transparency:** We are open and honest about what personal information we collect, why we collect it, and how it is used. We do not obscure our practices in complex language.
- **Data Minimisation:** We collect only the personal information necessary to deliver our services. We do not collect data speculatively or for purposes beyond those described in this Policy.
- **User Control:** Credential Holders retain control over their own data stored in the Credivera Wallet (native mobile). For users of Credivera Exchange (web wallet), credentials and data are controlled by the Holder as part of their engagement with organizations that have licenced Credivera Exchange. Credivera Exchange is a passive conduit for your communication and interaction with these organizations. Credivera Exchange provides full control options to the Holder, the Issuer Representatives and the Verifier Representatives over how credentials and data are shared, updated and issued.
- **Security:** We apply industry-leading technical and organizational safeguards to protect the personal information entrusted to us and hold ourselves and our service providers to the same standard.

Privacy inquiries may be directed to our Privacy Officer at: privacy@credivera.com

3. Who This Policy Applies To

This Policy applies to the following categories of individuals whose personal information we may collect or process:

- **Credential Holders:** Individuals who use the Credivera Wallet or Credivera Exchange to , manage, and share their workforce credentials.
- **Website Visitors:** Individuals who visit www.credivera.com.
- **Issuer Representatives:** Individuals who act on behalf of credentialing organizations (e.g., training providers, regulatory bodies) that use the Credivera Platform to issue credentials.
- **Verifier Representatives:** Individuals who act on behalf of organizations (e.g., employers, compliance officers) that use the Credivera Platform to verify credentials.
- **API Users:** Developers or technical contacts who access Credivera services via API.

Personal information collected about individuals acting in a business capacity on behalf of organizations with whom Credivera has a contractual relationship is governed by those contracts and applicable agreements, in addition to this Policy.

4. Personal Information We Collect

"Personal information" means any information about an identifiable individual. The specific personal information we collect depends on how you interact with our services. The table below summarizes the main categories:

**TERRAHUB****Credivera**

Data Category	Examples	Who This Applies To
Contact Information	Name, email address, phone number, job title	Users of Credivera Exchange
Credential Information	Document number, credential type, issuing authority, issue/expiry date, country of issue, worker authorizations	Credential Holders
Biographic Data	Date of birth, nationality (where required by credential type)	Credential Holders
Occupational & Compliance Data	Occupational health credentials, background check results, training completions, professional accreditations	Credential Holders
Wallet & Identity Data	Decentralized identifiers (DIDs), cryptographic key references (not private keys), verifiable credential metadata	Credential Holders, Issuer/Verifier platforms
Usage & Event Data	Login events, credential acceptance, verification requests, API calls, feature usage, platform events	Website Visitors, Platform and API users (not collected via the mobile Application)
Technical Data	IP address, browser type, session identifiers	Website Visitors and Platform users only (not collected via the mobile Application)
Communications Data	Inquiries, support tickets, feedback, troubleshooting correspondence	Any user who contacts us
Issuer/Verifier Organization Data	Organization name, contact details, integration configuration, API credentials	Issuer & Verifier Representatives
Cookie & Tracking Data	Browser cookies, session data, analytics identifiers	Website Visitors

4.1 Sensitive Personal Information

Certain categories of personal information we process may be considered sensitive under applicable privacy law. We apply heightened protection to such data and process it only in accordance with applicable privacy law or as required for the performance of our services. Sensitive categories include:

- Occupational health credentials and background check results
- Identity document details and biographic data processed through Credivera Verification Services

- Criminal record information processed through Criminal Background Check services — treated as a distinct sensitive category under Personal Information Protection and Electronic Documents Act, Quebec Law 25, and GDPR.

Credivera Verification Services involves processing the following sensitive data categories, all conducted via integrations with trusted third-party providers:

- **Identity verification (IDV and IDV+):** Government-issued identity documents, biographic data, and where applicable, motor vehicle registry records. Conducted via a third-party IDV provider.
- **Education verification:** Educational records and credentials across Canadian, United States, and global jurisdictions. Conducted via third-party education verification providers.
- **Criminal background checks:** Criminal record information across Canadian, United States, and global jurisdictions. Conducted via third-party background check providers.

For all Verification Services, users will be informed of the specific verification type, the third-party provider involved, and the data to be processed before any check is initiated. Express consent is required before any check proceeds. In facilitating verification checks, Credivera may transiently handle personal information — including identity document images and, where required by the verification type, a facial image (selfie) for liveness verification purposes — in order to transmit it to the applicable third-party provider. Credivera does not retain this data beyond what is necessary to complete the transmission and maintain an audit record of the transaction.

4.2 Credential Holder Data

Credivera Wallet (native mobile): The native iOS and Android wallet application collects no data whatsoever. Credentials and documents are stored exclusively on the user's local device. Nothing is transmitted to Credivera's servers by the Wallet unless the user explicitly initiates a share with a third party. Credivera cannot access, read, share, or disclose any credential or document stored in the Wallet without the user's explicit, informed consent.

Credivera Exchange (web wallet): The web wallet component of the Exchange platform is server-side hosted. Credentials and documents managed in the Exchange web wallet are held on Credivera's infrastructure on behalf of the organization that has licensed the platform. The organization is the licensee and is responsible for managing access, retention, and compliance obligations in relation to that data. Credivera does not access, use, or disclose web wallet contents without direction from the licensing organization, except as required by law. Individual users who wish to request deletion, de-identification, or exercise any other data rights in relation to their Exchange web wallet data should direct that request to their organization. Credivera will action such requests as directed by the licensing organization in accordance with applicable law and the organization's contractual agreements with Credivera.

Users should be aware of which wallet product they are using, as the data architecture and the nature of Credivera's access to credential data differs between the two. Both products are covered by the security and access control commitments described in Section 13 of this Policy.

4.3 Information We Do Not Collect

- We do not collect biometric data (such as fingerprints or facial recognition data)
- We do not collect private cryptographic key material from users — Key Manager manages encryption keys for organizational use; individual users' private keys are never transmitted to or stored by Credivera
- The Credivera Wallet (native mobile) does not collect any data from users' devices

5. How We Collect Personal Information

Credivera Wallet: The Credivera Wallet (native iOS and Android) does not collect, transmit, or share any personal information with Credivera. All credential data entered into or stored within the Wallet remains exclusively on the user's device. The data collection practices described in this section apply to our Website and Platform only, except where the user explicitly initiates a credential share through the Wallet.

5.1 Provided by You

- When you create an account or register on the Exchange Platform or Credivera Access Services

- When you upload credentials or documents to the Exchange Platform or submit information for a Verification Services check
- When you complete a form on our Website (e.g., book a demo, contact us)
- When you contact us for support or with inquiries
- When you participate in surveys, feedback sessions, or research

5.2 Automatically

- Through cookies and tracking technologies on our Website (see Section 10)
- Through platform event logs generated during use of the Platform or API — note that the Credivera Wallet does not generate or transmit event logs to Credivera
- Through device and technical data collected when you connect to our services via the Website or Platform — the Credivera Wallet does not collect or transmit device or technical data

5.3 From Third Parties

- From credential issuers who submit credential information on behalf of workers
- From API integrations initiated by issuer or verifier organizations
- From identity verification services (where applicable and with consent)

6. How We Use Personal Information

We use personal information only for the purposes for which it was collected or as otherwise permitted by applicable law. Our primary purposes are:

6.1 Delivering Our Services

- To operate the Exchange platform and web wallet, allowing Credential Holders to store, manage, and share credentials
- To support the Credivera Wallet as a local-only wallet that does not transmit data to Credivera
- To facilitate credential issuance between authorized issuers and Credential Holders via the Exchange and Verifiable Credential Infrastructure
- To enable credential verification by authorized verifiers, including cross-format verification via Verifiable Credential Infrastructure
- To process credential-based authentication events via Credivera Access Services and maintain authentication event logs
- To manage and publish credential status via the Status List component of Verifiable Credential Infrastructure, whether as a bundled platform feature or standalone service
- To facilitate identity, education, and criminal background verification through Credivera Verification Services, acting as intermediary to the applicable third-party provider
- To establish and maintain user accounts
- To authenticate user identity and prevent unauthorized access

6.2 Security and Fraud Prevention

- To conduct device integrity checks and detect fraudulent activity on the Platform and API (these checks do not apply to the Credivera Wallet, which transmits no data to Credivera)
- To monitor for unauthorized access, abuse, or misuse of our Website and Platform
- To protect the security and integrity of the Credivera Platform

6.3 Platform Improvement and Analytics

- To analyze usage patterns and improve product functionality
- To generate aggregated, anonymized metrics about service performance
- To support product development and research

6.4 Communications

- To respond to support requests, feedback, and inquiries
- To send service-related notifications (e.g., credential expiry reminders)
- To send product updates or marketing communications (where consent has been obtained and an opt-out is available)

6.5 Legal and Compliance

- To meet obligations under applicable law, regulation, or court order
- To comply with audit, insurance, or regulatory requirements
- To enforce our terms of service and other agreements

6.6 Business Transactions

In connection with the proposed or actual financing, acquisition, merger, or other disposal of all or part of our business or assets, personal information may be disclosed to prospective purchasers or their advisors for evaluation purposes, subject to confidentiality obligations.

6.7 Automated Decision-Making

Credivera does not make decisions based solely on automated processing that produce legal or similarly significant effects on individuals. Where automated processing forms part of our service operations (for example, credential verification workflows or fraud detection signals), human review is applied before any consequential decision is made. If this practice changes, we will update this Policy and seek consent where required by applicable law.

6.8 Credivera Access Services — Authentication Event Data

When users authenticate via Credivera Access Services using a verifiable digital credential, Credivera logs the authentication event on its infrastructure. Authentication event logs may include the timestamp of the authentication, the type of credential presented, and the system or service accessed. This data is used to support security monitoring, audit requirements, and the integrity of the authentication service. Authentication event logs are not shared with third parties except as required by law or as necessary to provide the service to the customer organization under whose platform the authentication occurred.

6.9 Credivera Verification Services — Third-Party Processing

All Credivera Verification Services (IDV, IDV+, Education Verification, and Criminal Background Checks) are delivered through integrations with third-party verification providers. Credivera does not conduct these checks using its own infrastructure. When a user initiates a verification check, Credivera facilitates the transmission of relevant personal information to the applicable third-party provider as entered or consented by the user. This means Credivera is in the data flow — personal information, which may include identity document images and facial images (selfies) used for liveness verification, is transiently handled by Credivera's infrastructure for the purpose of transmitting it to the third-party provider who conducts the check and returns a result to Credivera. Credivera does not store this data beyond what is necessary to facilitate the transaction and maintain an audit record. Each third-party provider processes personal information under their own privacy policy and applicable data processing agreements with Credivera. Credivera contractually requires all third-party verification providers to implement data protection standards consistent with applicable privacy law and this Policy.

7. Disclosure of Personal Information

7.1 Sharing with Your Consent

Credential Holders may choose to share their verified credentials with third parties (e.g., employers, recruiters, professional organizations) directly through the Application. Such sharing is initiated by the user and is subject to the recipient's own privacy practices. Credivera will confirm to the user which organizations have received their credential information.

7.2 Service Providers and Sub-Processors

We may share personal information with trusted third-party service providers who perform functions on our behalf, including:

- Cloud infrastructure and hosting providers
- Analytics and monitoring services
- Customer support tools
- Security and fraud detection services

All service providers are bound by contractual obligations to process personal information only as instructed by us and in accordance with applicable privacy law. A list of our current sub-processors is available on request by contacting privacy@credivera.com.

Data Processing Agreement (DPA): Enterprise and platform customers who require a formal Data Processing Agreement governing Credivera's processing of personal information on their behalf may request one by contacting privacy@credivera.com.

7.3 Issuer and Verifier Organizations

Where a Credential Holder has initiated a credential issuance or verification workflow, relevant credential metadata (not the underlying document) may be shared with the issuing or verifying organization as part of that workflow. Full document sharing requires explicit user consent.

7.4 Verifiable Credential Infrastructure — Standalone Service Customers

Where Verifiable Credential Infrastructure components (Status List, Key Manager, DID creation and hosting) are deployed as standalone services integrated into a customer's own systems, Credivera acts as a data processor for any personal information processed through those integrations. In these contexts, the customer organization is the data controller and Credivera processes personal information only as instructed by that organization under a Data Processing Agreement. Individuals whose data is processed in this context should direct privacy inquiries to the customer organization in the first instance.

7.5 Legal Requirements

We may disclose personal information as required by applicable law, regulation, or legal process, including in response to lawful requests from public authorities, courts, or regulatory bodies.

7.6 What We Do Not Do

- We do not sell personal information to third parties
- We do not share personal information for advertising or targeting purposes
- We do not disclose Credential Holder documents without explicit user consent

8. Cross-Border Data Transfers

Credivera is headquartered in Canada. If you are located outside Canada, your personal information may be transferred to and processed in Canada or in other countries, including the United States, where our service providers operate.

8.1 Privacy Impact Assessments

Credivera conducts Privacy Impact Assessments (PIAs) in circumstances where personal information may be at risk, including when acquiring, developing, or deploying new technologies or information systems that involve personal information; when transferring personal information outside of Canada; and when a significant change to our data processing practices is proposed. PIAs help us identify and mitigate privacy risks before they materialize. Records of PIAs are maintained by our Privacy Officer and are available to applicable regulatory authorities upon request.



TERRAHUB



Credivera

9. Cookies and Tracking Technologies

We use cookies and similar tracking technologies on our Website to support site functionality, understand how visitors use our site, and improve user experience.

10.1 Types of Cookies We Use

- **Strictly Necessary:** Essential for the Website to function. Cannot be disabled.
- **Analytics:** Help us understand how visitors interact with our Website (e.g., page views, traffic sources). We use this data in aggregate only.
- **Functional:** Remember your preferences to improve your experience.

We do not use advertising or cross-site tracking cookies.

You can manage or disable cookies through your browser settings. Note that disabling cookies may affect the functionality of certain parts of our Website. When you first visit our Website, you will be presented with a cookie consent notice allowing you to accept or decline non-essential cookies.

10. Retention of Personal Information

We retain personal information only for as long as necessary to fulfill the purposes for which it was collected, subject to our legal obligations and applicable retention requirements.

When personal information is no longer required, it is securely deleted or anonymized in accordance with our data retention policy.

Users may delete the Credivera Wallet at any time, upon which locally stored credential data will be permanently removed from their device.

11. Your Privacy Rights

Depending on your location and applicable law, you may have the following rights with respect to your personal information. We will respond to requests within the timeframes required by applicable law.

The rights described in this section apply to personal information for which Credivera acts as a data controller. Where Credivera processes personal information on behalf of a licensing organization — for example, credentials and data held in the Credivera Exchange web wallet — Credivera acts as a data processor for that organization. In these cases, individual users should direct privacy rights requests to their organization in the first instance. Credivera will support the organization in fulfilling those requests in accordance with applicable law and the organization's contractual agreements with Credivera.

- **Right of Access:** The right to request confirmation of whether we hold personal information about you and to receive a copy of that information.
- **Right to Correction:** The right to request correction of inaccurate or incomplete personal information.
- **Right to Erasure:** The right to request deletion of your personal information, subject to our legal obligations and legitimate interests.
- **Right to Restrict Processing:** The right to request that we limit how we use your personal information in certain circumstances.
- **Right to Data Portability:** The right to receive your personal information in a structured, machine-readable format (EEA/UK users).
- **Right to Object:** The right to object to processing based on legitimate interests (EEA/UK users).
- **Right to Withdraw Consent:** Where processing is based on consent, the right to withdraw that consent at any time.
- **Right to Lodge a Complaint:** The right to lodge a complaint with your local data protection authority.
- **Right to De-indexation:** Quebec residents have the right to request that we cease disseminating personal information about them, or de-index any hyperlink attached to their name that gives access to information that

is injurious to their reputation or privacy. This right applies to information that is publicly accessible through our services.

To exercise any of these rights, please contact our Privacy Officer at privacy@credivera.com. We will verify your identity before processing your request and may ask for additional information to do so. Privacy Officers will respond to requests within 30 days of receipt, as required by applicable law, with the possibility of an extension for complex requests.

12. Security

The security of personal information is a priority for Credivera. We implement physical, technical, and organizational safeguards designed to protect personal information against loss, theft, unauthorized access, disclosure, copying, use, or modification. These measures include:

- Encryption of data in transit and at rest
- Access controls and authentication requirements for platform access
- Regular security assessments and monitoring
- Employee training on privacy and data handling
- Device-level credential storage architecture that limits server-side exposure

Credivera is SOC 2 certified. Our SOC 2 report validates that our security controls meet the requirements of customers in regulated industries, covering the principles of security, availability, and confidentiality. A copy of our SOC 2 report is available to enterprise customers under NDA — contact privacy@credivera.com.

While we take significant steps to protect personal information, no method of data transmission or storage is completely secure. We cannot guarantee absolute security and encourage users to take steps to protect their own account credentials.

In the event of a data breach that poses a risk to individuals, we will notify affected users and relevant regulators as required by applicable law.

13. Third-Party Websites and Services

Our Website and Services may contain links to, or integrations with, third-party websites and services that are not operated or controlled by Credivera. This Policy does not apply to such third-party services. We encourage you to review the privacy policies of any third parties before providing them with personal information or using their services.

When a Credential Holder shares verified credentials with a third party through the Wallet, that disclosure is subject to the third party's own privacy practices. Credivera is not responsible for how third parties handle personal information received through credential sharing.

14. Contact Us

For questions, concerns, or requests regarding this Policy or our privacy practices, please contact our Privacy Officer:

Privacy Officer

TerraHub Technologies Inc. dba Credivera

Email: privacy@credivera.com

Website: www.credivera.com

We will acknowledge receipt of your inquiry promptly and endeavor to respond within 30 days. For complex requests, we may require additional time and will notify you accordingly.

15. Changes to This Policy

We reserve the right to amend this Policy at any time. Material changes will be communicated to users by:

- Posting a revised version of this Policy with an updated effective date
- Providing in-app notification or email notice where required by applicable law

For significant changes that affect how we use personal information, we will seek fresh consent where required. Your continued use of our services following the posting of changes constitutes acceptance of the revised Policy.