

Privacy Policy

Version: v2

Effective Date: October 3, 2025

1. Introduction

Landa Solutions Ltd. DBA Kleerr, together with its affiliates and subsidiaries (collectively "Company", "we", "us", or "our") operates the website www.kleerr.com (the "Website") and provides related services (collectively, the "Services"). This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you visit our Website or use our Services and our practices for collecting, using, maintaining, protecting, safeguarding and disclosing your information.

We are committed to protecting your personal information and your right to privacy. If you have any questions or concerns about this Privacy Policy or our practices, please contact us at privacy@kleerr.com.

We are not a HIPAA Business Associate unless we have executed a Business Associate Agreement (BAA) with you. Please do not submit Protected Health Information (PHI) without an executed BAA.

We do not sell Customer Data. For Website personal information, we do not sell or share personal information for cross-context behavioral advertising as those terms are defined under California law. If our use of cookies or pixels is deemed "selling" or "sharing," we provide a "Do Not Sell or Share My Personal Information"/"Your Privacy Choices" link and we honor Global Privacy Control (GPC) signals by treating them as an opt-out of sale/sharing.

What we don't do:

- We do not sell Customer Data.
- We do not share personal information for cross-context behavioral advertising.
- We do not train generalized or third-party AI/ML models on identifiable Customer Data.

Please read this Privacy Policy carefully to understand our policies and practices for collecting, processing, and storing your information. If you do not agree with our policies and practices, your choice is not to use our Website. By accessing or using this Website, you indicate that you understand, accept, and consent to the practices described in this Privacy Policy. This Privacy Policy may change (see [Changes to This Privacy Policy](#)) to reflect changes in our practices from time to time. Your continued use of this Website after we make changes indicates that you accept and consent to those changes, so please check the Privacy Policy periodically for updates. Significant changes will be communicated to you and will require your consent if necessary. For Website data, we act as a controller. For Customer Data processed via the Services, we act as a processor to our customers (the controllers).

Regional applicability. We do not target the EEA/UK/Switzerland. However, if you access our Website/Services from those regions—or if those laws otherwise apply to our processing of your personal data—the GDPR/UK GDPR/Swiss FADP—specific sections of this Privacy Policy apply to that processing.

2A. California Notice at Collection

This Notice at Collection applies to California residents and summarizes our collection and use of personal information on the Website:

- **Categories Collected:** Identifiers (e.g., name, email, IP address), Internet/Network Activity (e.g., pages viewed, interactions), Commercial Information (if you transact with us), Geolocation (approximate), Inferences (to personalize content), and Device/Technical Data.
- **Sources:** You (forms you submit), your browser/devices (automatic collection via cookies/pixels), our service providers and integration partners (e.g., analytics, CRM, ecommerce).
- **Purposes:** To provide and secure the Website/Services, perform analytics, improve and personalize experience, communicate with you, and (if used) measure/serve advertising.
- **Sold/Shared:** We do not sell personal information. If our use of cookies/pixels is deemed “sharing” for cross-context behavioral advertising, you may opt out via the “Do Not Sell or Share My Personal Information”/“Your Privacy Choices” link in our footer, and we honor Global Privacy Control (GPC) signals.
- **Retention:** We retain personal information as described in §6, based on criteria such as account status, legal/tax requirements, security/fraud prevention, and product needs. Typical ranges include: site analytics logs 12–24 months, billing records 7 years, and account/contact records for the life of the relationship + up to 24 months.
- **Your Choices:** Use the “Do Not Sell or Share My Personal Information”/“Your Privacy Choices” link and “Cookie Settings” in our footer to control non-essential cookies and sharing; see Section 12A for additional opt-out information.

2. Information We Collect

We collect information from and about users of our Website and Services, including:

2.1. Personal Information

Identification Data: that we can reasonably use to directly or indirectly identify you, such as your name or company name, mailing address, e-mail address, telephone number, Internet protocol (IP) address used to connect your computer to the Internet, user name or other similar identifier, billing and account information to or provide to us through the Website (including through email, text, or other electronic messages between you and the Website), and any other identifier we may use to contact you (“personal information”);

We provide an opportunity for any user to unsubscribe or opt-out of contact for marketing purposes on an ongoing basis by using the unsubscribe mechanism at the bottom of our e-mails.

Account Credentials: Passwords and other security information for authentication and account access.

2.2. Non-Personal Information

Information that does not directly or indirectly reveal your identity or directly relate to an identifiable individual, such as demographic information, or statistical or aggregated information. Statistical or aggregated data does not directly identify a specific person, but we may derive non-personal statistical or aggregated data from personal information. For example, we may aggregate personal information to calculate the percentage of users accessing a specific Website feature;

2.3. Usage Data

Information about your interactions with our Website and Services, including the full Uniform Resource Locators (URLs), clickstream to, through and from our Website (including date and time), products you viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), methods used to browse away from the page, pages visited, links clicked, and other usage statistics.

2.4. Device and Technical Data

Device Information: IP address, browser type, operating system, device type, unique device identifiers, and other diagnostic data.

2.5. Cookies and Tracking Technologies

We use cookies, web beacons, pixels, and other tracking technologies to collect information about your browsing and usage activities. For more details, please refer to Cookies and Tracking Technologies below.

3. How We Use Your Information

We use the information we collect for various purposes, including:

- To Provide and Maintain Our Services: To operate, improve and administer our Website and Services.
- To Personalize Your Experience: To tailor content and features to your preferences.
- To Communicate with You: To send administrative information, respond to inquiries, and provide customer support.
- For Marketing and Advertising: To send you promotional materials and offers, and to analyze the effectiveness of our marketing campaigns.

- To Analyze and Improve Our Services: To understand how users interact with our Website and Services and to enhance user experience.

We improve the Services using Aggregated Data and Service Data, not Customer Data in identifiable form.

- To Enforce Our Terms and Policies: To comply with legal obligations and protect our rights and interests.
- To Detect and Prevent Fraud: To monitor for security breaches and protect against malicious, deceptive, fraudulent, or illegal activity.
- For any other purpose with your consent.

By using our Website, you consent to your personal information being collected, held and used in this way and for any other use you authorize. We will only use your information for the purposes described in this Privacy Policy or with your express permission.

We may also use your information to contact you about our own and third-party services that may be of interest to you, as permitted by law. If you do not want us to use your information in this way, please use the unsubscribe mechanism at the bottom of our e-mails.

AI Features and Automated Decision-Making

We do not use your Customer Data to train generalized or third-party AI/ML models.

Any AI features operate on inputs to provide user-facing functionality and outputs; we do not make decisions with legal or similarly significant effects on individuals based solely on automated processing.

When third-party AI services are invoked, we instruct providers not to train on your data.

4. Disclosure of Your Information

We may disclose aggregated information about our users, and information that does not identify any individual, without restriction.

We may disclose your personal information in the following circumstances:

- Service Providers: To contractors, affiliates, service providers, and other third parties who assist us in operating our business and providing our Services, and who are contractually obligated to keep personal information confidential, use it only for the purposes for which we disclose it to them, and to process the personal information with the same standards set out in this Privacy Policy.
- Business Transfers: In connection with a merger, sale of company assets, reorganization, financing, or acquisition of all or a portion of our business to another company whether as a going concern or as part of bankruptcy, liquidation, or similar

proceedings, in which personal information held by us about our customers and users is among the assets transferred.

- Legal Obligations: To comply with any legal obligations, court orders, or governmental requests.
- Protecting Rights: To enforce our Terms and Conditions, protect our rights, privacy, safety, or property, and/or that of our affiliates, you, or others.
- Consent: With your explicit consent for any other purposes disclosed by us when you provide the information.

We may also disclose your personal information:

- To comply with any court order, law, or legal process, including to respond to any government or regulatory request, in accordance with applicable law.
- To enforce or apply agreements, including for billing and collection purposes.
- If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of our Company, our customers, or others. This includes exchanging information with other companies and organizations for the purposes of fraud protection and security risk reduction.

5. Transferring Your Personal Information

We may transfer personal information that we collect or that you provide as described in this policy to contractors, service providers, and other third parties we use to support our business (such as analytics and search engine providers that assist us with Website improvement and optimization) and who are contractually obligated to keep personal information confidential, use it only for the purposes for which we disclose it to them, and to process the personal information with the same standards set out in this Privacy Policy and as applicable to the processing at issue under PIPEDA, HIPAA, GDPR, CCPA/CPRA, and other regional privacy laws and regulations where we operate.

Current hosting region: United States (AWS). Additional regions may be added, and this notice will be updated prior to activation. Cross-border transfer assessments are available upon request.

Hosting location does not change our role as controller for Website data or processor for Customer Data, nor your rights under applicable law.

Website Data (Controller). If (and only if) EEA/UK/Swiss data protection law applies to a transfer of Website personal information, we use appropriate transfer tools (e.g., SCCs Module 1 or Module 2, as applicable, the UK Addendum, and where required Swiss FDPIC addendum terms).

Customer Data (Processor). Where EEA/UK/Swiss data protection law applies to a transfer of Customer Data, restricted transfers are governed by the DPA and use SCCs Modules 2 and/or 3

(as applicable), the UK Addendum, and any required Swiss FDPIC addendum; Annexes I–III of the DPA serve as SCC Annexes.

We may process, store, and transfer your personal information in and to a foreign country, with different privacy laws that may or may not be as comprehensive as Canadian law. In these circumstances, the governments, courts, law enforcement, or regulatory agencies of that country may be able to obtain access to your personal information through the laws of the foreign country. Whenever we engage a service provider, we require that its privacy and security standards adhere to this Privacy Policy and applicable Canadian privacy legislation.

We use a third-party web hosting service provider, Amazon Web Services (AWS) located in the United States to host your personal information.

Cross-border processing. We store and process personal information in the United States (Amazon Web Services) and may use service providers in other jurisdictions. As a result, personal information may be subject to the laws of those jurisdictions and available to their authorities under lawful process. We use contractual, technical, and organizational safeguards appropriate to the information's sensitivity. Questions about our cross-border practices can be directed to privacy@kleerr.com.

You consent to this potential transfer, storage, or processing by submitting your personal information or engaging with the Website.

Upon request, we will provide you with a list of third-party service providers used to host your personal information and the countries in which our servers are located.

If—and only if—you are subject to EEA/UK/Swiss data protection law and a restricted transfer occurs, the European Commission's Standard Contractual Clauses (Modules 2 and/or 3, as applicable) and, for UK transfers, the UK International Data Transfer Addendum apply.

6. Data Retention

Except as otherwise permitted or required by applicable law or regulation, we will only retain your personal information for as long as necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements and we ensure the secure disposal of information no longer required.

De-identification commitments. Where we de-identify data, we (i) take reasonable measures to ensure the information cannot be associated with a consumer or household, (ii) publicly commit not to re-identify the information, and (iii) contractually prohibit downstream recipients from trying to re-identify it.

Under some circumstances, we may anonymize your personal information so that it can no longer be associated with you. We reserve the right to use such anonymous and de-identified data for any legitimate business purpose without further notice to you or your consent.

7. Security of Your Information

The security of your personal information is very important to us. We take reasonable administrative, electronic, technical, and physical measures to protect your personal information from unauthorized access, use, alteration, loss, theft, and disclosure. These measures include encryption, access controls, and secure hosting environments. The safety and security of your information also depend on you. Where we have given you (or where you have chosen) a password for access to certain parts of our Website, you are responsible for keeping this password confidential. We ask you not to share your password with anyone. We urge you to be careful about giving out information in public areas of the Website like message boards, which any Website visitor can view, or in communications with other users on the Website. It is your responsibility to keep your password or other forms of authentication to the website safe. You agree to notify us as soon as possible if you become aware of any misuse of your password and immediately change your password within the Website. We maintain a confidentiality incident register and perform privacy impact assessments where required (including Québec Law 25).

If we become aware of a Security Incident (as defined in our Terms) involving personal information, we will notify affected customers and/or individuals without undue delay, consistent with applicable law.

Unfortunately, the transmission of information via the Internet is not completely secure. Although we do our best to protect your personal information, we cannot guarantee the absolute security of your personal information transmitted to our Website.

8. Your Rights

Depending on your jurisdiction, you may have certain rights regarding your personal information.

8.1. European Economic Area (EEA) Residents

Scope. This section applies only where the GDPR/UK GDPR/Swiss FADP applies to our processing of your personal data (for example, if you access our Website/Services from the EEA/UK/CH or we otherwise process personal data subject to those laws).

Under the General Data Protection Regulation (GDPR), you have the right to:

- Access: Request access to your personal data.
- Rectification: Request correction of inaccurate or incomplete data.
- Erasure: Request deletion of your personal data under certain conditions.
- Restriction: Request restriction of processing your personal data.
- Data Portability: Receive a copy of your personal data in a structured, commonly used, and machine-readable format.
- Objection: Object to the processing of your personal data for certain purposes.
- Withdraw Consent: Withdraw consent at any time where we are relying on consent to process your personal data.

To exercise these rights, please contact us at privacy@kleerr.com.

Legal Bases: Depending on the processing activity, we rely on one or more of the following: performance of a contract (e.g., to provide the Services), legitimate interests (e.g., to secure and improve the Services), consent (e.g., non-essential cookies/marketing), and compliance with legal obligations.

8.2. California Residents

Under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), California residents have the right to:

- Know: Request disclosure of categories and specific pieces of personal information collected.
- Correct: Request correction of inaccurate personal information.
- Delete: Request deletion of personal information.
- Opt-Out: Opt-out of the sale of personal information. If we use cross-context behavioral advertising, you may opt-out of sharing via the “Do Not Sell or Share My Personal Information” link. We process Global Privacy Control (GPC) signals where legally required.
- Non-Discrimination: Not be discriminated against for exercising their privacy rights.

We do not sell personal information as defined under the CCPA/CPRA. To exercise your rights, please contact us at privacy@kleerr.com.

Sensitive Personal Information. We do not use or disclose sensitive personal information for purposes requiring a “Limit the Use of My Sensitive Personal Information” link under California law; when collected (e.g., account credentials), it is used only for permitted security and authentication purposes.

Minors. We do not knowingly sell or share the personal information of consumers under 16 years of age. If we learn a consumer is under 16, we will cease sale/sharing unless we receive the required opt-in (affirmative authorization for ages 13–15; verifiable parental consent for under 13).

Authorized agents. You may use an authorized agent to submit a request; we will require proof of the agent’s authority and may need to verify your identity directly.

Financial incentives. We do not offer financial incentives for personal information. If we do in the future, we will provide a Notice of Financial Incentive describing the material terms.

8.3. Canadian Residents

Under the Personal Information Protection and Electronic Documents Act (PIPEDA), you have the right to:

- Access: Request access to your personal information.
- Correction: Request correction of inaccurate or incomplete personal information.
- Withdrawal of Consent: Withdraw consent to the collection, use, or disclosure of your personal information, subject to legal or contractual restrictions.

To exercise these rights, please contact us at privacy@kleerr.com. We may request specific information from you to help us confirm your identity and your right to access, and to provide you with the personal information that we hold about you or make your requested changes. Applicable law may allow or require us to refuse to provide you with access to some or all of the personal information that we hold about you, or we may have destroyed, erased, or made your personal information anonymous in accordance with our record retention obligations and practices. If we cannot provide you with access to your personal information, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

8.4. U.S. State Privacy Rights (e.g., VA/CO/CT/UT)

Residents of certain U.S. states may have rights to access, correct, delete, and obtain a portable copy of personal information, and to opt out of targeted advertising, sale, and certain profiling.

To exercise these rights, contact privacy@kleerr.com. We will verify requests as required by law. If we deny your request, you may appeal by replying to our decision or emailing privacy@kleerr.com with the subject line "Privacy Appeal." We will respond to appeals within the timeframe required by law.

9. Cookies and Tracking Technologies

As you navigate through and interact with our Website, we may use cookies or other automatic data collection technologies to collect certain information about your equipment, browsing actions, and patterns, including:

- Details of your visits to our Website, including traffic data, location data, logs, and other communication data and the resources that you access and use on the Website.
- Information about your computer and internet connection, including your IP address, operating system, and browser type.

Some of this information is aggregated; if we associate it with an identifiable person, we treat it as personal information. This information helps us improve our Website and deliver a better and more personalized service, including by enabling us to:

- Estimate our audience size and usage patterns.
- Store information about your preferences, allowing us to customize our Website according to your individual interests.
- Speed up your searches.

- Recognize you when you return to our Website.

The technologies we use for this automatic data collection may include:

- Cookies (or browser cookies). A cookie is a small file placed on the hard drive of your computer. You may refuse to accept browser cookies by activating the appropriate setting on your browser. However, if you select this setting you may be unable to access certain parts of our Website. Unless you have adjusted your browser setting so that it will refuse cookies, our system will issue cookies when you direct your browser to our Website.
- Web Beacons. Pages of our Website and our e-mails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit the Company, for example, to count users who have visited those pages or opened an email and for other related website statistics (for example, recording the popularity of certain website content and verifying system and server integrity).

You may always choose not to provide Personal Information to us, but it may mean that we are unable to provide you with our services or access to the Website.

You can manage non-essential cookies via the “Cookie Settings” link in our site footer. Where required by law and technically supported, we honor Global Privacy Control (GPC) and other recognized Universal Opt-Out Mechanisms by treating them as an opt-out of sale/sharing/targeted advertising for that browser. Our controls are designed to disable non-essential ad/retargeting technologies when an applicable opt-out is effective.

You may choose to limit certain analytics and advertising cookies using in-product controls; essential cookies (e.g., for authentication, security, fraud prevention) may still operate.

10. Third-Party Links

Our Website may contain links to third-party websites, plug-ins, applications, or services that are not owned or controlled by us. Clicking on those links or enabling those connections may allow the third party to collect or share data about you. If you follow a link to a third-party website or engage a third-party plugin, please note that these third parties have their own privacy policies, and we do not accept any responsibility or liability for these policies. We do not control these third-party websites. We are not responsible for the privacy practices of such third parties. We encourage you to review the privacy policies of every website you visit.

11. Children's Privacy

Our Services are intended for business use and not for children. We do not knowingly collect personal information from individuals under the age of 16. If we become aware that we have collected personal information from a child under 16, we will take steps to delete such

information promptly. If you believe we might have any information from or about a child under 16, please contact us at privacy@kleerr.com.

12. Withdrawing your Consent

Where you have provided your consent to the collection, use, and transfer of your personal information, you may have the legal right to withdraw your consent under certain circumstances. To withdraw your consent, if applicable, contact us at privacy@kleerr.com. If you do not want us to collect your information for marketing, you may opt out at any time by clicking the "unsubscribe" link at the bottom of our emails. Note that transactional or service emails may still be sent. Opting out of the Website's collection of location information will cause its location-based features to be disabled. Please note that if you withdraw your consent we may not be able to provide you with a particular service. We will explain the impact to you at the time to help you with your decision.

12A. California Right to Opt-Out of Sale/Sharing & Global Privacy Control (GPC)

If we engage in cross-context behavioral advertising, you may opt-out via the "Do Not Sell or Share My Personal Information" / "Your Privacy Choices" link (where provided).

We honor GPC and other recognized Universal Opt-Out Mechanisms (UOOMs) where required by law and supported by our consent management platform by treating them as an opt-out of sale/sharing/targeted advertising for that browser.

Opt-out choices apply to the device/browser where you set them and may not carry across devices unless you are logged in and we offer account-level controls.

We also process Universal Opt-Out Mechanisms (UOOMs) recognized by applicable law (e.g., Colorado, Connecticut) by treating them as an opt-out of targeted advertising/sale for that browser.

Hashed identifiers. When an opt-out of sale/sharing/targeted advertising is effective, we do not disclose identifiers (including hashed email or device IDs) to advertising platforms for audience matching or targeted advertising.

Do Not Track (DNT). While industry standards for DNT are not uniform, we honor GPC and other recognized UOOMs as described above.

13. Changes to This Privacy Policy

We reserve the right to update or modify this Privacy Policy at any time. We will notify you of any material changes by posting the new Privacy Policy on this page and updating the "Last Updated" date at the top. Your continued use of the Website and Services after any changes constitutes your acceptance of the revised Privacy Policy.

You are responsible for ensuring we have an up-to-date, active, and deliverable email address for you, and for periodically visiting our Website and this Privacy Policy to check for any changes.

14. Contact Us

Privacy Officer

Email: privacy@kleerr.com

Privacy Officer (Landa Solutions Ltd. DBA Kleerr) is responsible for overseeing compliance with this Privacy Policy and applicable law.

We have procedures in place to receive and respond to complaints or inquiries about our handling of personal information, our compliance with this Privacy Policy, and with applicable privacy laws. To discuss our compliance with this policy please contact us at privacy@kleerr.com.

15. Processing of Visitors' Data (on behalf of Customers)

When our analytics Services collect data from end-users visiting our Customers' properties, we act as a processor to the Customer (controller). We process such data only per the Customer's instructions to provide the Services.

Types of data may include IP address, device/browser info, pages visited, referral URLs, and interaction events.

Customers are responsible for having a lawful basis (e.g., consent/legitimate interests) and required disclosures; we assist with requests as described in our DPA.

Data may be transferred internationally with appropriate safeguards (e.g., SCCs); we apply technical and organizational measures such as encryption at rest/in transit, access controls, and logging.

We retain Visitors' data only as long as necessary to provide the Services or as required by law; after termination we delete or de-identify it per the DPA.

16. Compliance with Google API Services User Data Policy (Limited Use)

Where we use Google APIs, we comply with Google's API Services User Data Policy, including Limited Use requirements.

We use Google API data only to provide or improve user-facing features; we do not sell it or use it to train generalized AI/ML models; human access is restricted as required by the policy.

We retain such data only as long as necessary to provide the enabled features and protect it with industry-standard security.