

landng

PRIVACY POLICY

Last Updated: June 9, 2026

1. WELCOME

Landng Inc. ("Landng," "we," "us," or "our") operates the RealClicks.AI platform, available at realclicks.ai and associated subdomains, including the product suite, analytics dashboards, attribution and click validation services, and other related products and services offered through RealClicks.AI (collectively, the "Services"). Landng also operates its corporate and marketing website, including any Landng-branded website or webpage used to describe or promote the Services (collectively with RealClicks.AI, the "Site"). This Privacy Policy describes how we collect, use, disclose, and protect your personal information in compliance with the California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), General Data Protection Regulation (GDPR), UK GDPR, and other applicable privacy laws. By using our Services, you consent to the practices described in this Privacy Policy. If you do not agree, please do not use our Services.

1.1 Who This Privacy Policy Applies To

This Privacy Policy applies to:

- **Platform Customers.** Platform Customers are businesses, brands, agencies, publishers, creators, or other organizations that create accounts or otherwise use RealClicks.AI to access analytics dashboards, attribution tools, click validation services, campaign measurement tools, and related Services. When you register for or use the Services as a Platform Customer, we collect the information described in Sections 2.1–2.4 below, including account registration information, business contact information, billing or subscription information, authentication information, platform usage information, and information you provide to us in connection with your account or use of the Services.
- **Processing on Behalf of Platform Customers.** In certain contexts, Landng processes personal information on behalf of Platform Customers as a service provider or data processor, including where Platform Customers use the Services for attribution, analytics, campaign measurement, click validation, or related purposes. In those contexts, Platform Customers are responsible for determining the purposes and means of processing and for ensuring that their collection and use of personal information complies with applicable law, including providing required notices and obtaining any required consents. Our processing in those contexts is governed by our agreement with the Platform Customer and is limited to the purposes specified in that agreement.

1.2 Scope of Data Collection

The scope of data we collect depends on your relationship with Landng and your use of the Services. For Platform Customers and other account users, we may collect account registration information, business contact information, authentication information, billing or subscription information, platform usage information, and communications information. For

data processed through the RealClicks.AI analytics, attribution, click validation, and campaign measurement tools, we collect and process the limited data necessary to provide those Services, as described in this Privacy Policy and in our agreement with the applicable Platform Customer.

2. INFORMATION WE COLLECT

2.1 Account Registration Information

If you wish to register for an account, we will ask you to provide your username, email address, and password. For Platform Customers who subscribe to paid services, we also collect billing information in connection with payment processing. We use Stripe, Inc. ("Stripe") to process payments on our behalf. Landng does not store full credit card numbers, CVV codes, or other sensitive payment card data on its systems. Payment card information is collected directly by Stripe and is subject to Stripe's Privacy Policy, available at stripe.com/privacy.

2.2 Account Credentials and Authentication Information

When you create or access your account, we collect information used to authenticate and secure your account, such as your username, password, and information used for two-factor authentication. We use this information to verify your identity, enable account access, protect the security of the Services, and help prevent unauthorized access to your account.

2.3 Third-Party Account Information

If you register or log in to your account through a third-party service, such as Google, we will have access to certain information from that service, including your name, email address, and other account details, as provided by that service. You can disable the connection between our Services and your third-party account at any time.

2.4 Automatically Collected Information

When you use our Services, we may collect certain information automatically from you, which may include device and usage information, such as your IP address, browser and device characteristics, operating system, language preferences, referring URLs, device name, country, location, information about when and how you use our Services, and other technical information. When you access our Services through a mobile device, we also automatically collect certain mobile device information, including the type of device, your mobile operating system, and your mobile Internet browser.

2.5 Click Data and Attribution Data

In connection with our click tracking, attribution, analytics, and campaign measurement services, we may collect the following data when a user clicks, views, interacts with, or is otherwise measured through a link, campaign, advertisement, digital property, or other asset configured by or on behalf of a Platform Customer:

- Click event data: timestamp of the click event, referring source, URL parameters, campaign metadata, and link identifier.
- IP address: we may collect an IP address at the point of a link click or related event for attribution, click validation, bot detection, fraud prevention, security, and analytics purposes. Where appropriate, IP addresses may be truncated, aggregated, or deleted after the operational period needed to provide the Services.
- Conversion event data (Ecommerce Attribution): if a Platform Customer has implemented or enabled tracking technology on its ecommerce, partner, or other

digital property, we may receive information about user activity on that property, including page views, conversion events, session data, and related analytics information, for the purpose of attributing those events to an original click, campaign, or other measured interaction.

- Anonymized visitor identifiers: we assign anonymized identifiers (e.g., "User 12345ABCD") to support session-level analytics, attribution, fraud prevention, reporting, and campaign measurement. These identifiers are not intended to be linked to names, email addresses, or other direct personal identifiers by Landng.

2.6 Online-to-Offline Attribution Data

As part of our online-to-offline attribution service, we may match a click event IP address against a batch file of IP addresses provided by a third-party attribution vendor to determine whether a user who clicked a Platform Customer's link subsequently visited the Platform Customer's physical store location.

- A third-party vendor provides Landng with a batch file of IP addresses associated with device activity at a Platform Customer's physical store location.
- Landng performs an isolated comparison of the click event IP address against the vendor batch file.
- Landng records whether a match was found (match/no-match).
- The vendor batch file is deleted immediately after the scan, regardless of whether a match is found.
- Landng retains only the match result and does not retain the raw IP addresses from the vendor batch file beyond the matching process.

IP addresses may constitute personal data under applicable law, including the GDPR and UK GDPR. We treat IP addresses processed in this context with appropriate safeguards, including data minimization, access controls, and purpose limitation.

2.7 Meta API Data

Landng integrates with the Meta Platforms API to layer Meta-derived analytics data into the RealClicks.AI analytics dashboard. This integration may provide Platform Customers with data about the performance of their campaigns on Meta platforms, including engagement metrics and attribution data. Meta API data is not used for login authentication.

2.8 Data Pipeline and Infrastructure Data

The Services use data pipelines, a Delta Lake data architecture, and a Delta Sharing Protocol for downstream data ingestion and processing. Personal information processed through the Services may pass through these infrastructure components. Data processed through these systems is subject to the same security, retention, and access controls described in this Privacy Policy.

2.9 Communications

We collect your email address if you sign up to receive emails, invites, and newsletters from us regarding our activities. We collect information, such as your name and email address, to the extent necessary to provide the Services you have requested and/or to provide customer support.

3. HOW WE USE YOUR INFORMATION

We use the information we collect for the purposes described in this Privacy Policy, which may include to:

- Provide and deliver products or services

- Operate and improve our operations, systems, products, and services
- Respond to your comments and questions and provide customer service
- Provide administrative service and support (e.g., sending confirmations, technical notices, updates, security alerts, and other administrative messages; providing customer support and troubleshooting)
- Communicate with you about promotions, upcoming events, and news about products and services offered by Landng and our selected partners
- Enforce our terms and conditions or protect our business, partners, or users
- Protect against, investigate, and deter fraudulent, unauthorized, or illegal activity
- Validate clicks and detect automated, fraudulent, or bot-generated traffic
- Perform digital attribution, including click-to-conversion and online-to-offline attribution
- Process payments and maintain financial records in connection with paid Services
- Integrate and present Meta API-derived analytics data within the RealClicks.AI dashboard
- Provide Platform Customers with attribution reports and campaign performance data
- Perform data matching for online-to-offline attribution on behalf of Platform Customers

In line with the above purposes and as permitted by applicable law, we may communicate with you via electronic messages, including email or text messages, to provide you with the Services. Message and data rates may apply for any text messages sent to or received from us, and we are not responsible for the cost of those messages.

4. LEGAL BASES FOR PROCESSING

If you are located in the EEA, United Kingdom, or Switzerland, we process your personal data only when we have a valid legal basis to do so. Depending on the context, we rely on the following legal bases:

- **Performance of Contract.** We process personal data when necessary to provide the Services, administer accounts, process payments, provide customer support, and take other steps needed to perform our agreement with you or the organization you represent.
- **Legitimate Interests.** We process personal data when necessary for our legitimate business interests, provided those interests are not overridden by your rights and freedoms. This includes processing personal data to validate clicks, detect bots and invalid traffic, prevent fraud, maintain security, provide analytics and attribution services to Platform Customers, improve the Services, create aggregated or de-identified insights, and manage our business operations.
- **Consent.** We process personal data based on consent where required by law, including where consent is required for cookies, pixels, local storage, or other device-side tracking technologies, or where a Platform Customer or other third party has obtained consent before providing data to us. You may withdraw your consent at any time where our processing is based on consent.
- **Legal Compliance.** We process personal data when necessary to comply with applicable legal obligations, respond to lawful requests, enforce our agreements, or establish, exercise, or defend legal claims.

5. DISCLOSURE AND SHARING OF INFORMATION

We do not share, sell, or rent your information to third parties except as outlined in this Privacy Policy.

5.1 Service Providers

Like many businesses, we sometimes hire other companies to handle certain activities so we can focus on our main work. These activities include website evaluation, data analysis, data visualization, AI marketing automation and distribution, data cleansing, and distribution of marketing and promotional materials. These service providers are contractually required to use your information solely to provide services to us (and no other purpose) and to comply with appropriate security measures.

5.2 Business Transfers

We may sell, assign, buy, transfer, or otherwise acquire or dispose of certain of our businesses or corporate assets. In the event of such or a similar event, the personal data we collected from you may be part of the transferred assets. We may also share personal data with our auditors, attorneys, or other advisors in connection with the foregoing corporate transactions. You acknowledge and agree that any successor to or acquirer of us will continue to have the right to use your personal data and other information in accordance with the terms of this Privacy Policy.

5.3 Third-Party Platforms

We may provide you with the option to connect with third-party services, including websites, applications, and services through “plug-ins,” widgets, buttons, and other third-party features on our websites, communications, or products. To do this, we may share your account registration information with these third-party platforms so they can authenticate your account. These linked third-party platforms may have different data practices from ours. This Privacy Policy does not apply to the activities of third parties when they collect or use data for their own purposes or on behalf of others.

5.4 Aggregate Data

Aggregate data does not identify you personally. We may share aggregated or de-identified analytics, attribution, performance, engagement, campaign measurement, or reporting data with Platform Customers and other business partners. Aggregate data will not be treated as personal data under this Privacy Policy.

5.5 Analytics Services

We use third-party web analytics services, including Snowplow Analytics and Google Analytics, in our online services. Information collected may be automatically sent to these analytics providers, which may use cookies to assist with the analysis. Google Analytics can also provide demographic, interest-related, geographic, and referral data that Landng may use to better understand our customer base. Session User ID tracking and stitching may also be used to gain further insights into how our users access our websites from different devices.

5.6 Legal Requirements

We may disclose your personal data if required to do so by law (including responding to a subpoena or request from law enforcement, court, or government agency or other public authorities) or in the good faith belief that such action is necessary to (i) comply with a legal obligation, (ii) protect or defend our rights, interests, or property or that of other customers or users, (iii) act in urgent circumstances to protect the personal safety of users of the Services or the public, or (iv) protect against legal liability or potential fraud, as determined in our sole discretion.

5.7 With Your Consent

If we intend to use any of your personal data in a way that is not specified here, we will notify you of such intended use before or at the time of data collection, or we will obtain your consent after collection but before such use.

5.8 Payment Processors

We use Stripe, Inc. to process payments for paid Services. When you make a payment, your payment card information is submitted directly to Stripe and is not stored on Landng's systems. We may receive a payment confirmation, the last four digits of your card, and billing address information. Stripe's privacy and security practices are available at stripe.com/privacy.

5.9 Attribution Matching Vendors

For online-to-offline attribution services, we engage third-party vendors who provide batch files of IP addresses associated with device activity at Platform Customer store locations. These vendors act as our service providers and are contractually required to process data only for the purpose of attribution matching, implement appropriate security measures, and delete batch files after the matching process is complete.

5.10 Meta Platforms

Landng integrates with the Meta Platforms API. Data shared with or received from Meta through this integration is subject to Meta's Platform Terms and Privacy Policy. Landng does not use Meta API data for login authentication.

5.11 Data Pipeline and Delta Sharing

Platform Customers may elect to ingest attribution and analytics data via API, data pipelines, or the Delta Sharing Protocol. When Platform Customers use these features to export or integrate their data, they control that data and are responsible for its handling once exported from the RealClicks.AI platform.

6. INTERNATIONAL DATA TRANSFERS

Sharing of information sometimes involves cross-border data transfers to the United States and other jurisdictions. Landng may also subcontract processing to, or share your personal data with, third parties located in countries other than your home country or your country of residence. Your personal data, therefore, may be subject to privacy laws that are different from those in your country of residence.

Our Services are hosted on Amazon Web Services ("AWS"). For more details of AWS' privacy and security processes and its efforts to comply with international privacy laws and regulations (including GDPR), please visit <https://aws.amazon.com/compliance/data-privacy/>.

Where our Services are available to users in the European Economic Area ("EEA"), UK, or Switzerland, and when we transfer their personal data to countries outside of these regions as processors, we do so in accordance with applicable privacy laws. This includes implementing appropriate contractual, technical, and organizational measures as outlined in the Standard Contractual Clauses approved by the EU Commission. Standard Contractual Clauses are commitments between companies transferring personal data, ensuring they protect your data's privacy and security.

7. DATA RETENTION

We retain personal data only for as long as necessary to provide the Services you have requested and thereafter for a variety of legitimate legal or business purposes. These might include retention periods (i) mandated by law, contract, or similar obligations applicable to our business operations; (ii) for preserving, resolving, defending, or enforcing our legal/contractual rights; or (iii) needed to maintain adequate and accurate business and financial records.

Specific retention periods include:

- Account registration and Platform Customer account information: Life of the account plus 90 days after closure
- Financial and transactional records: Up to 7 years for tax and accounting compliance
- Marketing and communication data: Up to 2 years unless you opt out sooner
- Customer support records: 3 years after case closure
- Full IP addresses for bot detection/click validation: generally retained for no more than 7 days, then truncated or deleted.
- Full IP addresses, click event data, and attribution logs for attribution: retained for up to 90 days from the click event, then truncated, aggregated, or deleted.
- Vendor batch files for online-to-offline attribution: deleted immediately after the matching scan, whether or not a match is found.
- Online-to-offline match results: retained as part of the Platform Customer's attribution record for up to 90 days, then aggregated or deleted.
- Aggregated/anonymized analytics data: may be retained indefinitely; no individual identifiers retained beyond the applicable periods above

8. YOUR PRIVACY RIGHTS

8.1 Rights for All Users

Regardless of your location, you have the following rights:

1. Access. Request confirmation of whether we process your personal information and access to such information
2. Correction. Request correction of inaccurate personal information
3. Deletion. Request deletion of your personal information, subject to legal exceptions
4. Opt-Out of Marketing. Unsubscribe from marketing communications using the link in emails or adjusting account settings
5. Non-Discrimination. We will not discriminate against you for exercising your privacy rights

8.2 California Residents (CCPA/CPRA)

If you are located in the United States, this Privacy Policy explains how we collect, use, and disclose your personal data under the privacy laws of California, Colorado, Connecticut, Montana, Oregon, Texas, Utah, and Virginia. Although we are not yet subject to all U.S. Privacy Laws, given our level of activity, our Privacy Policy describes rights similar to those afforded under these laws. We do not sell personal information. We do not share personal information for cross-context behavioral advertising purposes unrelated to the attribution, analytics, and advertising measurement services described in Section 8.5. We do not

disclose personal data to third parties for targeted advertising. California residents have the following rights under CCPA/CPRA:

1. Right to Know. Request disclosure of:
 - Categories of personal information collected
 - Categories of sources from which personal information is collected
 - Business or commercial purposes for collecting or sharing personal information
 - Categories of third parties to whom we disclose personal information
 - Specific pieces of personal information we have collected about you
2. Right to Delete. Request deletion of personal information we have collected from you, subject to certain exceptions (e.g., completing transactions, detecting security incidents, complying with legal obligations, internal uses reasonably aligned with your expectations)
3. Right to Correct. Request correction of inaccurate personal information we maintain about you.
4. Right to Opt-Out. Opt out of the sale or sharing of personal information. We do not sell or share personal information.
5. Right to Limit Use of Sensitive Personal Information. Limit our use and disclosure of sensitive personal information to permitted purposes. We do not intentionally collect or process sensitive personal information except where necessary to provide the Services or where such information is voluntarily provided to us.
6. Right to Non-Discrimination. We will not discriminate against you for exercising your CCPA/CPRA rights.
7. Authorized Agents. California residents may designate an authorized agent to submit requests on their behalf by providing written authorization to contact@landng.com. We may require you to verify your identity directly with us and confirm that you authorized the agent to submit the request.

8.3 Response Time and Verification. We will confirm receipt within 10 business days and respond within 45 days (extendable by 45 days with notice). We will verify your identity before fulfilling your requests by comparing the information you provide with the information we maintain.

8.4 Categories of Personal Information Collected (Last 12 Months).

Category	Examples	Collected	Business Purposes
Identifiers	Name, email address, username, IP address, device identifiers	Yes	Provide Services, attribution, bot detection, customer support, security, and analytics
Personal information (Cal. Civ. Code § 1798.80(e))	Name, email address, billing address	Yes	Provide Services, customer support, payment processing

Commercial information	Subscription information, billing records, campaign data, attribution records, conversion event data	Yes	Provide Services, attribution analytics, billing, and reporting
Internet or network activity	Browsing history, search history, interaction with Services, click data, referring source, URL parameters, conversion events, engagement data on Platform Customers or partner sites (where tracking is implemented)	Yes	Analytics, service improvement, security, attribution, bot detection
Geolocation data	City/country location, IP-based location, store-visit matching (online-to-offline attribution)	Yes	Provide Services, attribution
Financial Data	Billing address, last four digits of payment card	Yes	Payment processing
Professional information	Business name, role, title or business contact information	Yes	Provide Services, account administration, and customer support

8.5 Attribution, Analytics, and Advertising Measurement Disclosures. We may disclose personal data to Platform Customers, advertising platforms, analytics providers, integration partners, and other service providers to provide attribution, analytics, advertising measurement, click validation, fraud prevention, and online-to-offline attribution services. These disclosures may include identifiers, click event data, IP address information, device or browser information, engagement data, attribution data, match results, and related analytics data. We do not sell personal information as defined under applicable law. We have not sold personal information in the preceding 12 months. We do not share personal information for cross-context behavioral advertising purposes, as defined under the California Privacy Rights Act, unrelated to the attribution, analytics, and advertising measurement services described above.

For individuals in the EEA, United Kingdom, or Switzerland, we rely on legitimate interests where appropriate to provide attribution, measurement, analytics, security, and fraud-prevention services, subject to any consent required under applicable law, including for cookies, pixels, local storage, or similar technologies. Where consent is required, the applicable Platform Customer or we must obtain consent before the relevant processing occurs.

8.6 EEA, Switzerland, and UK Residents (GDPR/UK GDPR)

If you are located in countries that are within the European Economic Area (the “EEA”), Switzerland, or the UK, GDPR and its Swiss and UK GDPR counterparts provide you rights with respect to your personal data, subject to any exemptions provided by the law, including the following rights:

1. Right to Access. Request access to your personal data.
2. Right to Correction. Request correction or deletion of your personal data.
3. Right to Limit Use. Request that we limit our use and processing of your personal data.
4. Right to Data Portability. Request portability of your personal data.
5. Right to Withdraw Consent. Where processing is based on consent, you have the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before withdrawal.
6. Right to Object. You have the right to object to processing based on legitimate interests or for direct marketing purposes. We will cease processing unless we demonstrate compelling legitimate grounds that override your interests, rights, and freedoms, or for the establishment, exercise, or defense of legal claims.
7. Right to Lodge a Complaint. Users located in EEA, United Kingdom, or Switzerland have the right to make a complaint to a government supervisory authority.

8.7 Automated Decision-Making.

We may use limited automated processing to provide analytics, attribution, click validation, fraud prevention, bot detection, and campaign measurement services. We do not rely solely on automated decisions that have legal effects or similarly significant effects on individuals.

8.8 Contacts to Exercise Privacy Rights.

- **Data Protection Officer.** For GDPR and UK GDPR inquiries, you may contact our Data Protection Officer at dpo@landng.com
- **EU Representative (Article 27 GDPR).**
Please contact VeraSafe using its contact form at <https://verasafe.com/public-resources/contact-data-protection-representative> or by telephone at +420 228 881 031.

Alternatively, VeraSafe may be contacted at:
VeraSafe Ireland Ltd.
Unit 3D North Point House
North Point Business Park
New Mallow Road
Cork T23AT2P
Ireland

- **UK Representative (Article 27 UK GDPR).**
Please contact VeraSafe using its contact form at <https://verasafe.com/public-resources/contact-data-protection-representative> or by telephone at +44 (20) 4532 2003.

Alternatively, VeraSafe may be contacted at:
VeraSafe United Kingdom Ltd.
37 Albert Embankment

London SE1 7TL
United Kingdom

- **Supervisory Authorities.**

For UK GDPR matters:

Information Commissioner's Office (ICO)
Wycliffe House
Water Lane Wilmslow
Cheshire SK9 5AF, United Kingdom
Tel: +44 303 123 1113
Website: <https://ico.org.uk>

For EEA supervisory authorities:

https://edpb.europa.eu/about-edpb/board/members_en

8.9 How to Exercise Your Rights

You can access, correct, or delete your personal data by contacting us at contact@landng.com. We will consider all such requests and provide our responses as soon as we can. Please note, however, that personal information may be exempt from such requests in certain circumstances, which may include circumstances where we need to keep processing your personal information for our legitimate interests or to comply with legal obligations.

To exercise your rights:

- **Email:** contact@landng.com
- **Subject Line:** "Privacy Rights Request – [Type of Request]"
- **Include:** Your name, email address associated with your account, description of your request, and jurisdiction (if applicable)

We will respond to verified requests within the timeframes required by applicable law:

- California residents: 45 days (extendable by 45 days with notice)
- GDPR/UK GDPR: 30 days (extendable by 60 days for complex requests with notice)

9. COOKIES AND TRACKING TECHNOLOGIES

9.1 Overview

The RealClicks.AI platform is designed to rely primarily on server-side data collection. Certain Services, such as click validation and attribution, may capture click event data on the server side without accessing or storing information on a user's device.

9.2 Types of Cookies We Use

The Site and Services may use cookies or similar technologies depending on the functionality being used. Server-side event collection that does not access or store information on a user's device does not require cookie consent under the ePrivacy Directive. Where cookies, pixels, local storage, or similar technologies are used, Landng or the applicable Platform Customer is responsible for obtaining any consent required by applicable law.

- Strictly Necessary Cookies. These cookies are necessary to allow us to operate our Services as you have requested.

- Statistics Cookies. We use cookies and other similar technologies to analyze how our Services are accessed, used, or performing. We use this information to maintain, operate, and continually improve our Services. We may also obtain information from our email newsletters or other communications we send to you, including whether you opened or forwarded a newsletter or clicked on any of its content. This information tells us about our newsletters' effectiveness and helps us ensure that we're delivering information that you find interesting.
- Preference Cookies. These cookies help us remember your preferences and settings to enhance your user experience.

9.3 Platform Customer Sites

For e-commerce attribution, campaign measurement, and online-to-offline attribution services, Platform Customers may implement a tracking pixel, tag, API integration, or other tracking technology on their own e-commerce, partner, or other digital properties. If a Platform Customer has implemented such technology, Landng may receive conversion event data or related analytics information from that technology. The Platform Customer is responsible for ensuring that its deployment of any tracking technology on its own properties complies with applicable law, including providing required notices and obtaining any required user consents. Landng's processing of data received from Platform Customer technologies is governed by our agreement with the Platform Customer.

9.4 Managing Cookies

It may be possible to use certain portions of our Site or Services without cookies. You can disable the storage of cookies in your browser, restrict them to certain websites, or configure your browser to notify you when a cookie is sent. You can also delete cookies from your device at any time. Please note that doing so may result in limited page display and reduced user guidance. To learn more about cookies, including how to see what cookies have been set and how to manage and delete them, visit <http://www.allaboutcookies.org/>

9.5 Do Not Track

"Do Not Track" is a feature enabled on some browsers that sends a signal requesting a web application to disable its tracking or cross-site user tracking. Currently, Landng does not respond to or change its practices when a Do Not Track signal is received.

9.6 ePrivacy Compliance

For users in the European Economic Area and United Kingdom, we adhere to ePrivacy Directive requirements. Consent is needed for storing information on a device (such as cookies or local storage) or accessing existing information on the device. Our server-side event collection that does not access or store information on your device is allowed without consent.

10. SECURITY MEASURES

We have implemented reasonable administrative, technical, and physical security measures to protect your personal information against unauthorized access, destruction, or alteration. For example, we limit access to this information to authorized employees and contractors who need to know that information in order to operate, develop, or improve our Services. However, although we strive to provide reasonable security for the information we process and maintain, no security system can ever be 100% secure. Our security program includes:

Technical Measures.

- Encryption of personal data in transit using TLS 1.2 or higher

- Encryption of personal data at rest
- Secure authentication mechanisms with password hashing
- Regular security testing and vulnerability assessments
- Intrusion detection and prevention systems

Organizational Measures.

- Access controls limiting employee access on a need-to-know basis
- Confidentiality agreements with employees and contractors
- Security awareness training
- Incident response and business continuity plans
- Vendor management ensuring third-party processors implement appropriate security

Physical Measures.

- Secure data center facilities with restricted access
- Environmental controls and redundancy

You are responsible for maintaining the confidentiality of your account credentials and for any activity conducted under your account.

11. CHILDREN'S PRIVACY

Our services are intended for a general audience and are not designed for or meant to be used by children. We do not knowingly collect information from children under 13 without parental permission. If a parent or guardian learns that their child has provided us with information without their consent, they should contact us at contact@landng.com as soon as possible. We will delete such information from our records within a reasonable time. For users in the EU/UK, our services are not intended for children under 16. We comply with the Children's Online Privacy Protection Act (COPPA) and do not knowingly collect personal information from children under the applicable age.

12. THIRD-PARTY LINKS AND SERVICES

Users can follow Landng on Facebook, Instagram, X (formerly Twitter), LinkedIn, and other social media platforms as they become available. Users should review the privacy policies for each platform to understand what information is collected. We may provide links to third-party websites, apps, and services. This Privacy Policy does not cover the activities of third parties when they collect or use data for their own purposes. We are not responsible for the privacy practices or content of third-party services. We recommend reviewing their privacy policies before sharing your information.

13. DATA BREACH NOTIFICATION

In the event of a personal data breach, we will:

- Notify Affected Individuals. If a breach is reasonably likely to result in a risk to your rights and freedoms (GDPR/UK GDPR) or requires notification under applicable law (e.g., California Civil Code § 1798.82), we will notify affected individuals without undue delay, and where feasible, within 72 hours of becoming aware of the breach.
- Notify Supervisory Authorities. For GDPR/UK GDPR compliance, we will notify the relevant supervisory authority within 72 hours of becoming aware of a breach that poses a risk to individuals' rights and freedoms, unless the breach is unlikely to result in such risk.

- Notify California Attorney General. For breaches affecting more than 500 California residents, we will notify the California Attorney General as required by California Civil Code § 1798.82.

14. CHANGES TO THIS PRIVACY POLICY

If Landng makes material changes to its Privacy Policy, it will notify you by: (i) updating the Last Updated Date at the top of the Privacy Policy, (ii) sending an email to its users, and/or (iii) adding a notice to the Site or the applicable Services. Material changes include new categories of personal information collected, new purposes for processing, new categories of third parties with whom we share information, or substantial changes to your rights. Your continued use of the Services after notice indicates acceptance of the updated policy.

15. CONTACT INFORMATION

If you have any questions regarding privacy while using our Services, or have questions about our practices, please contact us via email at contact@landng.com.

- **For General Inquiries.**

Email: contact@landng.com

- **Mailing Address.**

Landng Inc.
2241 Hoonanea Street
Honolulu Hawaii, 96822
United States

- **Data Protection Officer (GDPR/UK GDPR Inquiries).**

Email: dpo@landng.com

- **EU Representative (Article 27 GDPR).**

VeraSafe has been appointed as Landng's representative in the European Union for data protection matters pursuant to Article 27 of the General Data Protection Regulation. If you are located in the European Economic Area, VeraSafe may be contacted in addition to dpo@landng.com, but only on matters related to the processing of personal data.

To make an inquiry, please contact VeraSafe using its contact form at <https://verasafe.com/public-resources/contact-data-protection-representative> or by telephone at +420 228 881 031.

Alternatively, VeraSafe may be contacted at:

VeraSafe Ireland Ltd.
Unit 3D North Point House
North Point Business Park
New Mallow Road
Cork T23AT2P
Ireland

- **UK Representative (Article 27 UK GDPR).**

VeraSafe has been appointed as Landng's representative in the United Kingdom for data protection matters pursuant to Article 27 of the United Kingdom General Data Protection Regulation. If you are located in the United Kingdom, VeraSafe may be

contacted in addition to or instead of dpo@landng.com, but only on matters related to the processing of personal data.

To make an inquiry, please contact VeraSafe using its contact form at <https://verasafe.com/public-resources/contact-data-protection-representative> or by telephone at +44 (20) 4532 2003.

Alternatively, VeraSafe may be contacted at:

VeraSafe United Kingdom Ltd.

37 Albert Embankment

London SE1 7TL

United Kingdom