

Privacy Policy

Vizbl Systems, Inc. | Websites, Apps, AR/3D Viewers, AI Tools, Hardware, APIs, SDKs and Integrations

Effective Date: August 4, 2026

Last Updated: August 4, 2026

Operator and Controller: Vizbl Systems, Inc.

155 S. Fair Oaks Ave, Suite 1005, Pasadena, CA 91105, USA

Privacy Contact: privacy@vizbl.com

Plain-language summary

This Policy explains what personal information Vizbl collects, why we use it, when we disclose it, how long we keep it, and the rights available to individuals. It also explains the different privacy roles that apply when Vizbl processes information for its own purposes and when Vizbl processes information for a business customer.

This Privacy Policy is incorporated into and should be read together with the Vizbl Terms of Use, Cookie Policy, Professional Use Policy, Acceptable Use Policy, Data Processing Addendum (“DPA”), and any applicable Order Form or other written agreement.

1. Scope and Who We Are

This Privacy Policy applies to personal information processed by Vizbl Systems, Inc. (“Vizbl,” “we,” “us,” or “our”) in connection with:

- vizbl.com, connect.vizbl.com, go.vizbl.com, developer.vizbl.com, samples.vizbl.com, core-ar.vizbl.com, wallart.vizbl.com, ai-tryon.vizbl.com, rugs.vizbl.com, flooring.vizbl.com, our hosted dashboard, help center, legal pages, share pages, public catalog pages and other Vizbl websites or subdomains that link to this Policy;
- Vizbl 3D Viewer, AR Viewer, Web AR, Multi-AR, Core AR, AR Rugs, AR Flooring, AR Wall Art and Posters, Vizbl Showroom AR, Construction AR, AutoFit AI, AI Photo Try-On, AR Public Catalog and related product experiences;
- Vizbl mobile catalog applications, iOS App Clips, native iOS and Android software, custom-branded iPad applications, preconfigured iPad hardware, APIs, SDKs, plugins, widgets, embeds, webhooks, QR codes, print links, share links and ecommerce integrations;
- 3D-modeling, asset-conversion, AI-assisted content-generation, implementation, support, professional and enterprise services;
- business communications, sales, demonstrations, events, marketing, recruiting and vendor relationships.

This Policy does not govern a third party’s independent privacy practices, including a Customer’s website, store, app, checkout, payment system or marketing program. Those parties are responsible for their own privacy notices and legal obligations.

2. Our Privacy Roles

Vizbl acts in different legal roles depending on the context:

Context	Vizbl role	What this means
Vizbl websites, account administration, billing, support, security, direct marketing and business operations	Controller / Business	Vizbl determines why and how personal information is processed.
Customer product content, Customer user accounts and End-User information processed to provide contracted services	Processor / Service Provider / Contractor	Vizbl processes information on the Customer's documented instructions, subject to the DPA and applicable agreement.
Public Catalog, community features, public profiles, reviews or user-submitted public content, where enabled	Controller, joint controller, or separate controller depending on the feature	The applicable interface, terms or supplemental notice will describe the role and choices available.

Where Vizbl acts as a processor or service provider, the Customer is responsible for providing required notices, establishing a lawful basis, obtaining required consent, responding to data-subject requests, and configuring the service lawfully. Requests concerning Customer-controlled information should ordinarily be directed to that Customer. We will assist the Customer as required by applicable law and the DPA.

3. Personal Information We Collect

The information we collect depends on the features used, the device, the Customer configuration and the choices made by the individual.

3.1 Information You Provide

- Account and identity data: name, business email, telephone number, organization, job title, role, username, password hash, authentication method and account preferences.
- Business and profile data: company details, product categories, website, store information, professional credentials, licenses, association memberships and team-member information.
- Billing and transaction data: billing address, tax information, subscription, invoices, payment status and payment-method tokens. Payment processors generally receive payment-card details; Vizbl does not intend to store complete card numbers or card security codes.
- Customer Content: product data, SKU identifiers, dimensions, materials, finishes, pricing or availability data, images, videos, 3D models, CAD files, GLB/USDZ files, floor or wall images, artwork, logos, trademarks, metadata and configuration choices.
- Communications: messages, support tickets, call notes, recordings where notice or consent is required, meeting information, survey responses and feedback.
- AI and visualization inputs: photos, selfies, full-body images, hand, face, ear, wrist, room, wall, floor, vehicle or product images submitted to use AI try-on, AR placement, AutoFit, segmentation, model-generation or related tools.
- Event, promotion and recruiting data: registration details, contest or promotion entries, resumes, employment history, portfolio materials and interview information.

3.2 Information Collected Automatically

- Device and network data: IP address, device type, operating system, browser, language, mobile carrier, device or advertising identifiers, time zone, approximate location and referring URL.
- Usage and analytics data: pages and features used, search activity, viewer loads, 3D interactions, AR launches, dwell time, clicks, errors, diagnostic events, conversion events configured by a Customer, timestamps and session information.
- Cookie and similar-technology data: cookies, pixels, local storage, SDK events and related identifiers, as described in the Cookie Policy and the Cookie Settings interface.
- Security data: login history, authentication events, audit logs, suspected-fraud indicators, rate-limit events and information used to detect misuse or unauthorized access.
- Camera and sensor data: permissions and device signals needed for AR, including camera access, motion, orientation, surface detection, depth information or similar signals where supported.

Camera frames and local AR processing

For ordinary Vizbl AR Viewer placement, camera frames are intended to remain on the End User's device and are not transmitted to Vizbl servers. This does not apply when a person affirmatively uploads a photo, selfie, room image, floor image, vehicle image or other media for an AI, try-on, support, model-generation or content-submission feature. Uploaded media is transmitted and processed as described in this Policy and the applicable interface.

3.3 Information From Other Sources

- Customers, authorized users, agencies, resellers, implementation partners and product suppliers;
- ecommerce, identity, login, analytics, CRM, payment, app-store and integration providers when authorized;
- public websites, business directories, industry associations, dealer networks and professional sources;
- advertising, measurement, event and lead-generation partners, subject to applicable consent and opt-out rules;
- fraud-prevention, sanctions-screening, security and data-validation providers;
- other users who submit content that contains information about you.

3.4 Product- and Application-Specific Processing

Different Vizbl products use different information. The following summary describes the principal data flows visible from our current product and application offerings. Actual processing may vary by Customer configuration, device capabilities, permissions and integrations.

Product or technology	Information processed	Principal purpose
Core AR, 3D Viewer and AR Viewer	Product models, GLB/USDZ assets, textures, PBR materials, dimensions, variants, hotspots, viewer events, device/browser information and camera permission. Ordinary live camera frames are intended to remain on-device.	Render, rotate, zoom and place products at true scale; deliver variants, dimensions, snapshots and AR links.

Multi-AR	Selected product identifiers, scene composition, object positions, object-on-object anchoring, layout state and interaction events.	Allow multiple products to be arranged, compared and retained within an AR scene.
AR Rugs, Flooring and Wall Art	Top-down product images, artwork, textures, room/floor/wall camera input, segmentation or surface-detection data, size, orientation, pattern, frame and composition selections.	Generate or render category-specific AR without a separate 3D model for every SKU.
AI Photo Try-On	A user-uploaded selfie or body-area image, product image or model, face/body/hand/wrist/ear landmarks, pose, segmentation, geometry and generated output.	Place jewelry, watches, eyewear, hats, clothing or accessories on an uploaded image.
AutoFit AI	Vehicle photograph or camera input, detected wheel area, vehicle and product selections, wheel/rim dimensions, finish choices and generated output.	Visualize wheels, rims or accessories on the actual vehicle.
Showroom AR and Construction AR	Customer catalog, sales-associate or authorized-user account, device and app telemetry, project or session selections, site/room camera input and saved layouts where enabled.	Operate custom-branded iPad workflows for showrooms, construction sites and on-site product selection.
AR Public Catalog and mobile catalog	Public product content, creator or business profile data, likes, saves, reviews, follows, searches, shares, click-throughs and purchase-link interactions where enabled.	Provide product discovery, community interaction, sharing and traffic to Customer destinations.
App Clips, native apps, QR and share links	App/device identifiers, invocation URL, QR or campaign parameters, permissions, session events and destination information.	Open the correct product experience and measure delivery, performance and attribution.
APIs, SDKs, embeds and commerce integrations	API credentials, Customer identifiers, SKU mappings, webhook payloads, integration configuration, request logs, errors and End-User events selected by the Customer.	Connect Vizbl to Shopify, WooCommerce, WordPress, Wix, BigCommerce, Squarespace, Webflow, custom storefronts and native applications.
3D production, conversion and edge delivery	Product photographs, CAD, GLB/USDZ, materials, measurements, metadata, optimization diagnostics, compressed assets, delivery logs and quality-review records.	Create, normalize, compress, store and deliver reusable 3D assets through Vizbl infrastructure and content-delivery networks.

Feature names and availability may change. When a feature collects materially different information, Vizbl or the applicable Customer will provide additional notice in the relevant interface, application, Order Form or supplemental privacy notice.

4. Sensitive Information, Images and Biometric-Related Data

Certain features may process information that some laws classify as sensitive personal information, biometric information, biometric identifiers, precise geolocation, health-related information or data concerning children. The classification depends on the information, technology, purpose and jurisdiction.

- AI Photo Try-On and image-based features may process face, body, hand, wrist, ear or other images

and may derive landmarks, geometry, pose, angle, segmentation masks or similar technical attributes to position or render clothing, jewelry, watches, eyewear, hats, hair accessories or other products.

- Vizbl does not use these image-derived attributes to identify or authenticate a person, create a general-purpose identity profile, or determine identity, unless a separate feature expressly states otherwise and all legally required notices and consents are provided.
- Vizbl does not sell biometric identifiers. We do not use face or body images for unrelated advertising profiling unless separately disclosed and permitted by law.
- Precise geolocation is collected only when the feature requires it, the device supplies it, and any required permission has been granted. Approximate location may be inferred from IP address.
- Customers may not use Vizbl to collect or infer sensitive information in a manner prohibited by the Terms, AUP, Professional Use Policy, DPA or applicable law.

Where written consent, a biometric notice, a retention schedule or destruction procedure is required, Vizbl or the applicable Customer will provide the required supplemental disclosure before collection. Customers deploying image, try-on or biometric-related features are responsible for confirming which party must obtain consent in each jurisdiction.

5. How and Why We Use Personal Information

Purpose	Examples	Typical legal basis where GDPR/UK GDPR applies
Provide and administer the Platform	Create accounts, authenticate users, host and render content, deliver 3D/AR experiences, operate apps, APIs, SDKs and integrations, process orders and provide support.	Contract; legitimate interests; legal obligation where applicable.
Process images and generate outputs	Run AI try-on, segmentation, AutoFit, model generation, optimization, conversion, rendering and quality review.	Contract; consent where required; legitimate interests for service improvement where permitted.
Secure and protect	Prevent fraud, abuse, unauthorized access, malware, scraping and attacks; maintain audit logs; enforce agreements.	Legitimate interests; legal obligation; establishment, exercise or defense of legal claims.
Improve and develop	Measure performance, troubleshoot, test, research, train and improve features using data permitted by contract and law.	Legitimate interests; consent where required; de-identified or aggregated data where feasible.
Communicate	Send service notices, invoices, support replies, product updates, event messages and marketing communications.	Contract; legitimate interests; consent where required.
Advertising and measurement	Measure campaigns, build audiences and deliver relevant advertising where enabled.	Consent or opt-out framework, depending on jurisdiction and technology.
Comply and defend	Meet legal, tax, accounting, regulatory and law-enforcement obligations and handle disputes.	Legal obligation; legitimate interests; legal claims.

We do not use personal information for materially different purposes without providing additional notice and, where required, obtaining consent. We may use de-identified or aggregated information for lawful

business purposes and will not attempt to re-identify information that is legally treated as de-identified, except to test whether de-identification controls work or as otherwise permitted by law.

6. Artificial Intelligence and Automated Processing

Vizbl uses automated systems, computer vision, machine learning and generative technologies to provide and improve product visualization, including image segmentation, product placement, try-on, 3D asset generation, compression, quality checks, recommendations, fraud detection and analytics.

- Inputs and outputs may be reviewed by authorized personnel or service providers for support, safety, quality control, rights management and improvement, subject to contractual and legal limits.
- Customer Content or End-User data processed on behalf of a Customer is used for model training or generalized product improvement only when permitted by the applicable agreement, Customer instruction and law. Where required, Vizbl will use de-identified, aggregated, licensed or consented data.
- Vizbl does not make decisions producing legal or similarly significant effects about an individual solely through AI Photo Try-On, AutoFit AI, AR placement, product recommendations or product visualization.
- Where a legally regulated automated-decision process is introduced, Vizbl will provide any required pre-use notice, access, explanation, correction, human-review or opt-out rights.

7. How We Disclose Personal Information

We may disclose personal information to the following categories of recipients, subject to appropriate contractual, technical and legal safeguards:

- Service providers and subprocessors: cloud hosting, content delivery, storage, databases, security, authentication, customer support, communications, analytics, AI/ML processing, model generation, payment processing and professional advisers.
- Customers and authorized users: account administrators, team members and the business operating the website, store, app or viewer through which an End User interacts.
- Integration and commerce partners: platforms, plugins, app stores, ecommerce systems and other services selected or enabled by a Customer or user.
- Advertising and measurement partners: only as described in the Cookie Policy, Cookie Settings and applicable state privacy disclosures.
- Business transaction parties: actual or prospective buyers, investors, lenders, auditors, insurers and advisers in connection with financing, reorganization, merger, acquisition, sale or bankruptcy, subject to confidentiality where appropriate.
- Authorities and legal recipients: courts, regulators, law enforcement, rights holders or other parties when required or permitted by law, to protect rights and safety, investigate fraud or enforce agreements.
- At your direction: recipients you choose, authorize or direct us to use.

We require service providers handling personal information on our behalf to use it only for authorized purposes and to protect it appropriately. A current list of material subprocessors may be made available

through the Platform, DPA or upon reasonable request, subject to confidentiality and security considerations.

8. Sale, Sharing and Targeted Advertising

Vizbl does not sell personal information for money. However, certain privacy laws define “sale,” “sharing,” “targeted advertising” or “cross-context behavioral advertising” broadly. Use of advertising cookies, pixels, audience tools or measurement technologies may fall within those definitions even when no money is exchanged.

- Where required, Vizbl provides a “Do Not Sell or Share My Personal Information” or comparable opt-out mechanism through Cookie Settings or another clearly identified control.
- Vizbl honors legally recognized universal opt-out signals, including Global Privacy Control, where required and technically applicable.
- We do not knowingly sell or share personal information of individuals under 16 without legally required affirmative authorization.
- Opting out of targeted advertising does not stop all advertising or all analytics. It limits use of information for covered cross-context or targeted advertising purposes.

9. Retention and Deletion

We retain personal information only for as long as reasonably necessary for the purposes described in this Policy, including to provide the Platform, comply with law, resolve disputes, enforce agreements, prevent fraud and maintain security. Retention varies by category and context.

Category	Typical retention approach
Account and subscription records	For the account term and a reasonable period afterward; certain billing, tax and contractual records may be retained longer as required by law.
Customer Content	During the Customer term. Following termination, account-level content is ordinarily retained for up to 30 days before deletion from active systems unless a different agreement, Customer instruction, legal hold or backup cycle applies.
Uploaded photos, selfies, vehicle images and AI inputs	For the period stated in the applicable feature or Customer configuration; otherwise only as long as needed to generate the requested output, provide support, maintain security and meet contractual or legal obligations. Generated outputs may be retained longer when the user saves, shares or publishes them.
Viewer and analytics events	For periods appropriate to reporting, security, product improvement and contractual commitments; data may be aggregated or de-identified sooner.
Support and communications	For as long as needed to handle the request, maintain business records, train staff where permitted and resolve disputes.
Backups	Deleted according to standard backup-rotation and disaster-recovery cycles, unless preservation is required by law or security needs.

Deletion may not be immediate where information is retained in backups, logs, fraud-prevention records, legal holds, de-identified datasets or records that must be kept by law. Retained information remains

protected and is not used for unrelated purposes.

10. Security

We use reasonable administrative, technical and physical safeguards designed to protect personal information, taking into account the nature of the information and the risks of processing. Measures may include encryption in transit, access controls, least-privilege permissions, logging, monitoring, vulnerability management, incident-response procedures, secure development practices, vendor review and workforce confidentiality obligations.

No method of transmission or storage is completely secure. Users and Customers are responsible for protecting credentials, using appropriate authentication, limiting access, maintaining secure integrations and promptly reporting suspected compromise to security@vizbl.com.

11. International Transfers

Vizbl is headquartered in the United States and works with service providers and personnel in multiple countries. Personal information may be transferred to, stored in or accessed from the United States and other jurisdictions whose laws may differ from those where the individual resides.

Where required for transfers from the EEA, United Kingdom or Switzerland, we use an approved transfer mechanism, such as an adequacy decision, the European Commission Standard Contractual Clauses, the UK International Data Transfer Agreement or UK Addendum, the Swiss addendum or another lawful safeguard. We may conduct transfer assessments and implement supplementary measures where appropriate. Copies of relevant safeguards may be requested at privacy@vizbl.com, subject to redaction of confidential and security-sensitive information.

12. Your Choices and Privacy Rights

Depending on your location and the applicable law, you may have some or all of the following rights:

- access or confirmation of whether we process your personal information;
- correction of inaccurate personal information;
- deletion, subject to legal and contractual exceptions;
- portability or a copy in a usable format;
- restriction of processing;
- objection to processing based on legitimate interests or to direct marketing;
- withdrawal of consent without affecting earlier lawful processing;
- opt out of sale, sharing, targeted advertising or certain profiling;
- limit use or disclosure of sensitive personal information where required;
- appeal a denial of a request where provided by law;
- not receive unlawful discriminatory treatment for exercising privacy rights;
- complain to a competent data-protection authority or regulator.

To submit a request, email privacy@vizbl.com or use an available privacy-request or account tool.

Describe the request, the relevant product or Customer, and the email address associated with the account or interaction. We may verify identity and authority using reasonable methods appropriate to the request. Authorized agents may submit requests where permitted, but we may require proof of authorization and direct identity verification.

When Vizbl processes information solely for a Customer, we may direct the request to that Customer and assist as required. We will respond within the period required by applicable law. Some information may be exempt from a request, including information needed for security, fraud prevention, legal claims, tax, accounting, contractual records or the rights of others.

13. Communications and Marketing

- Service and transactional communications: account, security, billing, privacy, support and operational messages are necessary to provide the Platform and generally cannot be opted out of while the account remains active.
- Email marketing: use the unsubscribe link or contact privacy@vizbl.com. We may retain a suppression record to honor the opt-out.
- Text messages: reply STOP where supported. Message and data rates may apply.
- Push notifications: change settings in the device or application.
- Cookies and advertising: use Cookie Settings, device controls and legally recognized opt-out signals as described in the Cookie Policy.
- Sales calls: tell the caller or email us to be placed on the applicable internal do-not-call list, subject to lawful business-contact exceptions.

14. Children and Minors

The Platform is primarily a business and commerce service and is not directed to children under 16. We do not knowingly collect personal information from children under 16 through consumer-directed features without the authorization, notice, consent and controls required by applicable law. Customers may not configure or market the Platform to children in violation of law.

If a parent, guardian or other person believes that a child provided personal information improperly, contact privacy@vizbl.com. We will investigate and delete or otherwise handle the information as required. Age thresholds and parental-consent requirements may vary by jurisdiction.

15. Customer Websites, Embedded Viewers and End Users

Customers may embed Vizbl viewers or deploy Vizbl APIs, SDKs, apps, QR codes, hardware or AI features in their own properties. In those cases:

- The Customer determines what product content is published, what optional events are enabled, which integrations are connected and what notices or consent mechanisms are presented.
- The Customer must disclose Vizbl and relevant subprocessors in its privacy materials where required and must obtain consent before activating non-essential cookies, advertising technologies, precise-location access, image uploads or sensitive-data processing when required.
- The Customer must provide a lawful method for End Users to exercise rights and must communicate

applicable deletion, restriction or opt-out instructions to Vizbl through approved channels.

- Vizbl may receive pseudonymous viewer identifiers, device and usage events, referrer information, product or SKU identifiers, AR-launch events and other data configured by the Customer. Vizbl does not need an End User's name or email to render ordinary 3D/AR content unless the Customer or End User submits it through another feature.
- The Customer is responsible for its independent collection, checkout, payment, CRM, email, advertising, analytics and fulfillment activities.

16. Supplemental Notice for California Residents

This section supplements the Policy for California residents and uses terms defined by the California Consumer Privacy Act, as amended ("CCPA"). It applies only to the extent Vizbl is subject to the CCPA for the relevant processing.

CCPA category	Examples collected	Business or commercial purposes	Categories disclosed to
Identifiers	Name, email, account ID, IP address, device identifiers, business contact details.	Provide services, security, support, billing, communications, analytics.	Service providers, Customers, integrations, authorities as required.
Customer records	Contact, billing, account and transaction records.	Account management, invoicing, support, compliance.	Payment, accounting, CRM and support providers.
Commercial information	Subscriptions, products viewed, SKUs, usage and purchase-related events supplied by Customers.	Provide services, reporting, personalization and analytics.	Customers and service providers.
Internet or electronic activity	Browsing, viewer events, AR launches, clicks, device and diagnostic data.	Operations, security, analytics, product improvement and advertising where enabled.	Analytics, security, Customer and advertising partners as applicable.
Geolocation	Approximate IP-derived location; precise location only where enabled and permitted.	Localize service, security, requested features.	Service providers and Customers as configured.
Audio, electronic or visual information	Uploaded product images, room photos, selfies, body or face images, support recordings where permitted.	AI/AR features, support, model generation, quality and security.	Service providers, Customers and authorized personnel.
Professional information	Organization, role, business profile, recruiting information.	Business operations, account administration, recruiting.	Service providers and business transaction parties.
Inferences	Product preferences, likely interests, fraud indicators, technical landmarks or segmentation outputs.	Personalization, visualization, safety, analytics and advertising where enabled.	Customers and service providers; advertising partners where applicable.

Sensitive personal information	Account credentials, precise geolocation if enabled, content of certain communications, and biometric-related data where legally classified as sensitive.	Provide requested features, authentication, security and compliance.	Service providers and Customers, subject to restrictions.
--------------------------------	---	--	---

California residents may request to know, access, correct or delete personal information; receive portability information; opt out of sale or sharing; limit certain uses of sensitive personal information; and receive equal service and price as required by law. We do not sell personal information for money. Our use of advertising and measurement technologies may constitute sale or sharing under the CCPA. Use Cookie Settings, the applicable “Do Not Sell or Share” link, Global Privacy Control, or email privacy@vizbl.com.

We do not knowingly sell or share personal information of consumers under 16 without the legally required opt-in. We may deny or limit requests where permitted and provide an explanation and appeal or complaint information where required.

17. Supplemental Information for the EEA, United Kingdom and Switzerland

Where GDPR, UK GDPR or Swiss data-protection law applies, Vizbl relies on the legal bases described in Section 5. Individuals may have rights of access, rectification, erasure, restriction, portability, objection, withdrawal of consent and complaint to a supervisory authority.

- Controller: Vizbl Systems, Inc., 155 S. Fair Oaks Ave, Suite 1005, Pasadena, CA 91105, USA.
- Contact for privacy matters and representative inquiries: privacy@vizbl.com. If Vizbl appoints a formal EU or UK representative or data protection officer for a particular activity, the applicable notice or customer documentation will identify that representative.
- Legitimate interests include operating and securing the Platform, preventing fraud, supporting Customers, improving services, maintaining business records and marketing to relevant business contacts, balanced against individual rights.
- International transfers are handled as described in Section 11.
- Complaints may be submitted to the supervisory authority in the individual's habitual residence, place of work or place of the alleged infringement.

18. Other U.S. State Privacy Rights

Residents of certain U.S. states may have rights similar to those described above, including access, correction, deletion, portability, opt-out of targeted advertising, sale or certain profiling, and appeal of a denied request. Vizbl will honor applicable rights and recognized opt-out signals as required. Submit requests to privacy@vizbl.com. State-specific rights apply only where the relevant law covers Vizbl and the processing at issue.

19. Third-Party Services and Links

The Platform may link to or interoperate with third-party websites, stores, social networks, payment processors, app stores, analytics providers and integrations. Their privacy practices are governed by their own notices. Enabling an integration or following a link may cause information to be sent to or received

from that third party. Review the third party's terms and privacy notice before use.

20. Changes to This Policy

We may update this Policy to reflect changes in law, technology, products, data practices or business operations. The "Last Updated" date identifies the current version. Where required, we will provide additional notice and obtain consent before a material change takes effect. Previous versions may be archived or made available upon request. Continued use after the effective date of an update is subject to applicable law and contractual terms.

21. Contact Us

Privacy requests and questions: privacy@vizbl.com

Security reports: security@vizbl.com

Legal notices: legal@vizbl.com

Postal address: Vizbl Systems, Inc., 155 S. Fair Oaks Ave, Suite 1005, Pasadena, CA 91105, USA

Please do not send passwords, full payment-card numbers, government identification documents or other highly sensitive information by ordinary email unless we specifically request it through a secure channel.