

PROTO Privacy Policy

Privacy is one of PROTO's core values. Your device is important to many aspects of your business. Our aim is to keep your business your business.

Collection and Use of Data

Data covered by this Policy may identify or be used to contact a user of a PROTO Device. You may be asked to provide information when you interact with PROTO or a PROTO-affiliated company. PROTO and its affiliates may share this information with each other and use it consistent with this Privacy Policy. They may also combine it with other information to provide and improve our products, services, and content. You are not required to provide information we request, but if you choose not to do so, in many cases we will not be able to provide products or services or respond to your questions. The following are examples of information PROTO may collect and how we may use it:

What information we collect

- When you download a software update, connect to our services, contact us or participate in an online survey, we may collect a variety of information, including your organization's name, mailing address, phone number, email address, contact preferences, device identifiers, IP address, location information, and credit card information, if applicable.

How we use your information

We may process your information for the purposes described in this Privacy Policy, with your consent, to comply with a legal obligation to which PROTO is subject, to perform a contract to which you are a party, to protect your vital interests, or when we have determined that processing is necessary for the legitimate interests pursued by PROTO or a third party to whom information may need to be disclosed. If you have questions about the applicable legal basis, contact PROTO Data Privacy at privacy@protohologram.com.

- The personal information we collect allows us to keep you informed about PROTO's latest product announcements, software updates, and upcoming events. If you do not want to be on our mailing list, you may opt out at any time by updating your preferences.
- We also use personal information to help us create, develop, operate, deliver, and improve our products, services, and content. We may use your information for account and network security purposes, including protecting our services for the benefit of users and pre-screening or scanning uploaded content for potentially illegal content.
- From time to time, we may use your personal information to send important notices, such as communications about changes to our terms, conditions, and policies. Because this information is important to your interaction with PROTO, you may not opt out of receiving these communications.
- We may also use personal information for internal purposes such as auditing, data analysis, and research to improve PROTO's products, services, and customer communications.

Source of your information where they are not collected from you

We may validate the information provided by you when creating a PROTO ID when applicable with a third party for security and fraud prevention purposes.

Collection and Use of Information

We also collect information in a form that does not, on its own, permit direct association with a specific organization or individual. We may collect, use, transfer, and disclose this information for the purposes described in this Privacy Policy. The following are examples of information we collect and how we may use it:

- We may collect information such as industry, zip code, area code, unique device identifier, referrer URL, location, and the time zone where a PROTO product is used so that we can better understand customer behavior and improve our products and services.
- We may collect limited information about customer interactions with our websites, cloud services, products, and services through operational, security, and diagnostic logs. We use this information to provide requested functionality, maintain security, troubleshoot issues, and improve reliability. We do not use this information for advertising, cross-site tracking, or website analytics or performance measurement.
- We may collect limited details about use of our services, such as requested features or services, search queries submitted to a requested service, timestamps, status information, and error data. We use this information to provide and troubleshoot the service and improve its reliability and the relevance of requested results. We associate this information with an IP address only where reasonably necessary to deliver, secure, or troubleshoot the service.
- With your explicit consent, we may collect data about how you use your device and applications in order to help app developers improve their apps.

AI Avatars and Personas

If you or your organization use PROTO's AI Avatars, Personas, or related AI features, we may collect or process avatar footage, images, video, voice samples, voice and likeness materials, consent videos, avatar and voice identifiers, persona names, descriptions, thumbnails, prompts, system prompts and context you enter, model and provider selections, device identifiers, account identifiers, playback records, credit records, session metadata, provider usage counts, error logs, support records, and other usage metadata.

Live Persona interactions. When a Persona is active during a live session, microphone audio or other input may be captured and processed to recognize speech, generate a response, and synthesize spoken output through the selected avatar, in always-listening or push-to-talk mode as configured by the customer operating the device. For current Persona interactions, PROTO does not record or persist raw microphone audio, live conversation transcripts, generated Persona responses, or live conversation history in PROTO-controlled storage. Live audio, transient transcripts, generated text, generated audio, and related session data may nonetheless be temporarily created, transmitted, transformed, cached, buffered, or processed as necessary to operate the feature and route data among PROTO systems and third-party AI providers.

Voice and likeness materials. Avatar creation uses video footage and voice samples, and may involve a consent video. Depending on the jurisdiction and how it is processed, this material may constitute biometric information or sensitive personal information. Where we collect it, we do so to create, verify, host, license, and operate avatars and personas at the direction of the customer that submits the material, and we retain it as an avatar, license, and consent record.

Third-party AI providers. Depending on the feature and customer configuration, PROTO may use third-party providers for avatar creation and hosting, real-time communications, speech-to-text processing, large language model processing, text-to-speech processing, and cloud hosting and infrastructure. Data disclosed to a provider is limited to information reasonably necessary for the applicable function and configuration. Applicable AI providers may also apply their own safety, abuse-prevention, or moderation controls as part of their services. Current core providers are identified in the PROTO AI Provider and Subprocessor Notice. Third-party AI providers process information under the applicable provider agreements, data-processing terms, service terms, privacy policies, account settings, and service configurations. Provider practices

concerning retention, human review, moderation, service improvement, and model training may vary by provider and configuration. PROTO will make a provider-specific no-training, zero-retention, or similar commitment only where that commitment is supported by the applicable provider terms and service configuration and is expressly stated in an order form or other written agreement signed by PROTO.

PROTO model training. PROTO does not use live Persona conversation audio, live transcripts, generated Persona responses, or live conversation history to train PROTO-owned models.

Customer-directed AI services. Where a customer connects its own model, API endpoint, or other external service using its own credentials, PROTO stores those credentials in encrypted form and logs only metadata, such as provider name, endpoint identifier, timestamps, usage counts, latency, error codes, and session identifiers. PROTO does not intentionally log full request or response payloads for those integrations. The customer-selected provider is not a PROTO service provider, and the customer is responsible for that provider's data practices.

Public and customer-controlled deployments. Customers may deploy PROTO devices and Personas in public, semi-public, workplace, event, retail, educational, healthcare, government, financial-services, and other customer-controlled environments where visitors interact with a Persona without signing in to PROTO Cloud. In those settings, the customer deploying the Persona is responsible for providing the notices and obtaining the consents required for that deployment, including any notice that a person is interacting with an AI system and that audio or other input may be processed. PROTO may not have a direct relationship with individuals who interact with a Persona in a customer-controlled environment. If you interacted with a PROTO device in such a setting and have a question or request about your information, contact the organization operating the device, or contact us and we will direct your request to that organization where we are able to identify it.

Cookies and Other Technologies

As of October 7, 2025, PROTO has disabled all non-essential cookies and tracking technologies on its websites and online services. PROTO uses only strictly necessary cookies that are required to provide website functionality, maintain security, manage sessions, remember essential settings, and operate requested services. PROTO does not use cookies, pixels, web beacons, or similar technologies for advertising, cross-context behavioral advertising, marketing, personalization, analytics, or performance measurement. PROTO does not use these technologies to track individuals across third-party websites or services.

PROTO may collect limited technical information through server and security logs, such as IP address, browser type and language, operating system, timestamps, requested pages, and security events. We use this information to operate, secure, troubleshoot, and maintain our websites and services, not for advertising or cross-site tracking.

Transfer of Personal Data Between Countries

PROTO products and offerings connect you to the world. To make that possible, your personal data may be transferred to or accessed by entities around the world. PROTO complies with laws on the transfer of personal data between countries to help ensure your data is protected, wherever it may be.

If you do not reside in the U.S., your personal data may be processed by PROTO. For example, imagery and associated data may be collected by PROTO around the world to improve video latency and to support PROTO's video capture features. Third-party AI providers used to deliver AI Avatar and Persona features may process data in the United States and in other jurisdictions in which they or their sub-processors operate.

When required, PROTO uses legally recognized safeguards for international transfers of personal data, which may include the European Commission's Standard Contractual Clauses and applicable transfer safeguards for the European Economic Area, the United Kingdom, and Switzerland. For questions about international transfers, contact PROTO Data Privacy at privacy@protohologram.com.

Others

It may be necessary – by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence – for PROTO to disclose your information. We may also disclose information about you if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate. We may also disclose information about you, but only where there is a lawful basis for doing so, if we determine that disclosure is reasonably necessary to enforce our terms and conditions or protect our operations or users. This could include providing information to public or governmental authorities. Additionally, in the event of a reorganization, merger, or sale we may transfer any and all information we collect to the relevant third party.

Protection of Information

PROTO takes the security of your information very seriously. PROTO online services protect your information during transit using encryption. When your data is stored by PROTO, we use computer systems with limited access housed in facilities using security measures. Cloud data is stored in encrypted form including when we utilize third-party storage.

Retention of Information

PROTO retains personal information only for as long as reasonably necessary to provide the Services, fulfill the purposes described in this Privacy Policy, comply with customer instructions, maintain security, satisfy legal and accounting obligations, and establish or defend legal claims. When a customer requests deletion of its PROTO Cloud account, customer content and other customer data designated for deletion are removed from PROTO Cloud within thirty (30) days after the request. Content stored on an active PROTO device associated with the deleted cloud account is also removed within that period if the device is connected to the Internet and able to receive the deletion instruction. If the device is offline, the deletion instruction cannot be delivered until the device reconnects to the Internet; the applicable content will be removed after the device reconnects and receives that instruction. For current AI Avatar and Persona interactions, PROTO does not record or persist raw microphone audio, live transcripts, generated Persona responses, or live conversation history in PROTO-controlled storage. PROTO may retain persona configuration, prompts and context saved in PROTO Cloud, avatar and license records, consent records, device and account identifiers, usage metadata, billing and credit records, security records, support records, and logs as described in this Policy and the applicable agreements. Certain billing, transaction, security, audit, legal, and backup records may be retained for longer periods where reasonably necessary or legally required. Third-party providers may retain information according to their applicable agreements, service configurations, and legal obligations.

Location-Based Services

To provide location-based services on PROTO products, PROTO and our partners and licensees, such as maps data providers, may collect, use, and share precise location data, including the real-time geographic location of your PROTO device. Where available, location-based services may use GPS, Bluetooth, and your IP Address, along with crowd-sourced Wi-Fi hotspot and cell tower locations, and other technologies to determine your devices' approximate location. Unless you provide consent, this location data is collected anonymously in a form that does not uniquely identify you and is used by PROTO and our partners and licensees to provide and improve location-based products and services. For example, your device may share its geographic location with application providers when you opt in to their location services.

Third-Party Sites and Services

PROTO websites, products, applications, and services may contain links to third-party websites, products, and services. Our products and services may also use or offer products or services from third parties – for example, a third-party app.

Information collected by third parties, which may include such things as location data or contact details, is governed by their privacy practices. We encourage you to learn about the privacy practices of those third parties. If you purchase a subscription in a third party app, we may offer the ability to create a Subscriber ID that is unique to you and the developer or publisher which we use to provide reports to the developer or publisher that include information about the subscription you purchased, and your country of domicile.

California Privacy Disclosures

The California Consumer Privacy Act, as amended by the California Privacy Rights Act (together, the “CCPA”), provides California residents with specific rights regarding their personal information. PROTO provides the following disclosures for California residents and reviews the CCPA’s applicability to its business periodically. Where the CCPA applies, these rights may include the rights to know, access, delete, and correct personal information; to opt out of its sale or sharing; to limit certain uses or disclosures of sensitive personal information; and to receive nondiscriminatory treatment for exercising those rights. Requests may be submitted to PROTO Data Privacy at privacy@protohologram.com.

The following is not applicable to de-identified or aggregated personal information or data publicly available.

Information we collect

In the execution of our services and when visiting our website we collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably linked, directly or indirectly, with a particular consumer or device. In particular, we may collect and disclose for a business purpose the following categories of data from our users:

Category	Examples	Collection and disclosure
A. Identifiers	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address	COLLECT: YES DISCLOSE: YES, to affiliates, service providers, and other vendors, if any, mentioned in our Privacy Policy.

Category	Examples	Collection and disclosure
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e))	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information Some personal information included in this category may overlap with other categories.	COLLECT: YES DISCLOSE: YES, to affiliates, service providers, and other vendors mentioned in this Privacy Policy.
C. Protected classification characteristics under California or federal law	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	COLLECT: NO DISCLOSE: NO
D. Commercial information	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	COLLECT: YES DISCLOSE: YES, to affiliates, service providers, and other vendors mentioned in this Privacy Policy.
E. Biometric information	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	COLLECT: YES DISCLOSE: YES, to affiliates, service providers, and other vendors mentioned in this Privacy Policy and in the PROTO AI Provider and Subprocessor Notice.

Category	Examples	Collection and disclosure
F. Internet or other similar network activity	Browsing history, search history, and information about a user's interaction with a website, application, or other content.	COLLECT: YES DISCLOSE: YES, to affiliates, service providers, and other vendors mentioned in this Privacy Policy.
G. Geolocation data	Physical location or movements, or the location of your device.	COLLECT: YES DISCLOSE: YES, to affiliates, service providers, and other vendors mentioned in this Privacy Policy.
H. Sensory data	Audio, electronic, visual, thermal, olfactory, or similar information	COLLECT: YES DISCLOSE: YES, to affiliates, service providers, and other vendors mentioned in this Privacy Policy and in the PROTO AI Provider and Subprocessor Notice.
I. Professional or employment-related information	Current or past job history or performance evaluations	COLLECT: NO DISCLOSE: NO
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g, 34 C.F.R. Part 99))	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	COLLECT: NO DISCLOSE: NO

We disclose your data for a business purpose to the following categories of third parties:

- Service providers
- Third parties to whom we disclose your personal information in connection with products or services we provide to you, and to accomplish our business purposes and objectives as set forth in the Privacy Policy.

Sensitive personal information

Some information processed in connection with AI Avatars and Personas may be “sensitive personal information” under the CCPA, including biometric information processed for the purpose of uniquely identifying a consumer. PROTO collects and uses such information only to perform the services requested, to create, verify, host, license, and operate avatars and personas, to maintain security and prevent fraud and abuse, and for other purposes permitted without a right to limit under Cal. Civ. Code § 1798.121 and its implementing regulations. PROTO does not use or disclose sensitive personal information to infer characteristics about a consumer. PROTO does not sell or share personal information as those terms are defined in the CCPA.

Data from children?

We do not intentionally collect information from children under the age of eighteen (18) years as we do not offer services to them. Parents who set up a profile holding information about children under the age of eighteen (18) years can only do so by granting parental consent which consent choices can be changed by the adults in the family. We do not direct services to children under the age of eighteen (18) years old. As a result, we do not knowingly process data or information from children under eighteen (18) years old. Customers may deploy PROTO devices and Personas in public or other customer-controlled environments that children may be able to access. In those settings, the customer deploying the device is responsible for determining whether its deployment is directed to children, for any parental consent required, and for the notices and consents required by applicable law. Customers may not create avatars or personas based on minors without explicit lawful permission.

Sale or Sharing of Personal Information

PROTO does not sell personal information or share personal information for cross-context behavioral advertising. PROTO does not use strictly necessary cookies to track individuals across third-party websites or services. Questions or requests concerning PROTO’s privacy practices may be submitted to PROTO Data Privacy at privacy@protohologram.com.

Our Companywide Commitment to Your Privacy

To make sure your information is secure, we communicate our privacy and security guidelines to PROTO employees and strictly enforce privacy safeguards within the company. PROTO is committed to the protection, security, availability, and confidentiality of customer data within the PROTO Cloud application.

SMS Messaging Terms of Service

PROTO uses SMS only for manual, one-to-one customer support and troubleshooting. Support requests originate by phone or support ticket. Before texting begins, the customer and a PROTO support representative mutually agree to exchange phone numbers and communicate by SMS.

By agreeing to communicate by SMS and providing your mobile number for that purpose, you consent to receive support texts from PROTO about your support request. SMS is optional; you may continue to use our established phone or support-ticket channels. We do not use this SMS service for automated messages or marketing.

Message frequency varies depending on your support needs and the troubleshooting conversation. Message and data rates may apply under your mobile carrier plan.

You may withdraw your consent at any time by replying STOP to opt out of SMS support messages. Reply HELP for help, or contact PROTO through the established support phone number or support-ticket channel used to open your request. You may continue receiving support through those channels after opting out of SMS.

PROTO does not sell or share SMS opt-in data or consent information with third parties or affiliates for marketing or promotional purposes. Our collection, use, disclosure, protection, and retention of information associated with SMS support are governed by this Privacy Policy, including its Protection of Information and Retention of Information sections.

Message delivery depends on your mobile carrier and network availability and is not guaranteed. Carriers are not liable for delayed or undelivered messages.

Privacy Questions

To ask a privacy question, submit a request concerning your personal information, or make a complaint about a possible violation of applicable privacy law, contact PROTO Data Privacy at privacy@protohologram.com. You may also contact us by phone using the relevant PROTO support number for your country or region.

When we receive a privacy question or a question about information provided in response to an access or download request, our team triages the request and responds as appropriate. We may request additional information when necessary. Wherever possible, we acknowledge substantive contacts within seven (7) days by responding to the issue raised, requesting additional information, or indicating that additional time will be required.

Where your complaint indicates an improvement could be made in our handling of privacy issues we will take steps to make such an update at the next reasonable opportunity. In the event that a privacy issue has resulted in a negative impact on your organization then we will take steps to address that with you.

PROTO may update its Privacy Policy from time to time. When we change the policy in a material way, a notice will be posted on our website along with the updated Privacy Policy. We will also contact you via your contact information on file, for example by email, notification or some other equivalent method.