PRIVACY POLICY

MX12 LLC

Effective Date: May 19, 2026
Company: MX12 LLC, Delaware Limited Liability Company
Website: mirrax12.world
Governing Law: State of Delaware, USA + regional laws at the location of the data subject

> **IMPORTANT.** By using MX12 services — including the AI widget powered by Google Gemini — the Client and end users agree to this Policy. Electronic acceptance has full legal force pursuant to the Delaware Electronic Transactions Act (6 Del. C. § 12A-101 et seq.).

1. WHO WE ARE AND OUR ROLES

1.1 MX12 LLC is a company incorporated in the State of Delaware, USA, providing managed support services through Live chat, Email, VoIP/SIP, AI widget, messengers, and social media. Services may be processed in the USA and other jurisdictions depending on the location of the infrastructure and subprocessors involved.

1.2 Role Definitions by Scenario:

Scenario	MX12 Role	Client Role
mirrax12.world website visitor data	Controller	—
MX12 client data (contractual)	Controller	Data subject
Client's end user data	Processor	Controller
Joint analytics	By separate written agreement	By separate written agreement

In limited cases the Parties may act as independent or joint controllers — exclusively to the extent and in the cases expressly agreed in writing. In the absence of a separate written Joint Controller Agreement, the Parties are not deemed joint controllers within the meaning of GDPR Art. 26.

1.3 The Client is the Controller with respect to its end users' data and bears full responsibility for having a lawful basis for transmitting such data to MX12.

1.4 In the event of conflict between the base section and a regional section — the regional section takes precedence on data protection matters.

1.5 Privacy by Design. MX12 applies the principles of privacy by design and by default (GDPR Art. 25) in developing and updating its Services: minimization of data collected, restriction of access, application of protective technical measures by default.

2. WHAT DATA WE COLLECT

2.1 Client Data: name, email, phone, job title; company data; transaction history; communications for quality control purposes; Service usage data. MX12 does not store payment card data — processing is carried out through secure payment systems (Stripe and others).

2.2 End User Data (on Client's instructions): name and contact details; content of inquiries (tickets, chats, calls); interaction history through Zendesk, Intercom, Freshdesk, Gorgias, AI widget; CRM data (HubSpot and others); VoIP/SIP call recordings where consent exists.

2.3 AI Widget Data. Processing path: end user message → MX12 AI widget → Google Gemini API → response to user. Upon operator request: widget → ticket → live operator. Text of messages, dialogue context, and session metadata are processed. Data is transmitted to Google pursuant to the Google Cloud Data Processing Addendum and Google Cloud Platform terms of use.

2.4 Website Visitor Data: IP address, browser, device, pages visited, session duration, referral URL, cookies.

2.5 Anonymized and Aggregated Data. Truly anonymized data no longer constitutes personal data under applicable law and is processed outside the scope of this Policy. MX12 uses such data to improve Service quality and for operational analytics.

2.6 What We Do NOT Collect: special categories of data (health, biometric, political views, and others under GDPR Art. 9) — without explicit consent; data of persons below the applicable age of consent in the user's jurisdiction.

3. PURPOSES AND LEGAL BASES

Purpose	GDPR / UK GDPR	CCPA / Delaware DPDPA	PIPEDA	Australia
Contract performance and Services	Art. 6(1)(b)	Business necessity	Principle 4.2	APP 3.3
AI widget (Google data transmission)	Art. 6(1)(a) — consent*	Consent	Principle 4.3	APP 3.3
Billing	Art. 6(1)(b)	Business necessity	Principle 4.2	APP 3.3
Quality control	Art. 6(1)(f)**	Legitimate interest	Principle 4.2	APP 3.3
Legal obligations	Art. 6(1)(c)	Legal obligation	Principle 4.2	APP 3.3
Marketing	Art. 6(1)(a)	Opt-in	Explicit consent	Explicit consent
Security	Art. 6(1)(f)**	Legitimate interest	Principle 4.7	APP 11
Anonymized analytics	Art. 6(1)(f)**	Legitimate interest	Principle 4.2	APP 3.3
Profiling / automated decisions	Art. 6(1)(a)	Consent***	Explicit consent	APP 3.3
Sanctions screening and compliance	Art. 6(1)(c)	Legal obligation	Principle 4.2	APP 3.3

*Transmission of data through the AI widget to Google servers may go beyond what is strictly necessary for performance of the support agreement depending on the specific deployment, Client instructions, and applicable law. MX12 establishes consent as the standard contractual requirement for this processing. The applicable legal basis is ultimately determined by the Client as controller taking into account its specific use case and applicable jurisdictions.

**For processing based on legitimate interest, MX12 conducts a Legitimate Interests Assessment (LIA). Results are available upon request by data subjects from the EU and UK.

***To the extent applicable under CCPA/CPRA and implementing regulations as currently in effect.

4. ARTIFICIAL INTELLIGENCE

4.1 Google Gemini — Primary AI Provider. Google acts as a subprocessor pursuant to Standard Contractual Clauses (SCC) and the Google Cloud Data Processing Addendum (GDPR Art. 28). MX12 configures the integration such that: data is not used to train Google's public models without separate permission; only the minimum necessary volume of data is transmitted (data minimization); connections are made through secure encrypted channels.

Limitation of Control Disclaimer. Google processes data in accordance with its own service terms, security measures, and applicable legal obligations, some of which are outside MX12's direct control. MX12 is responsible for data it transmits to Google under the agreed processing terms and is not liable for Google's processing of data beyond those terms. The Client is responsible for informing end users about the use of Google Gemini pursuant to GDPR Art. 13–14 and applicable law.

Procedure for Google Breach. Upon detection of a Google breach of data processing terms, MX12 will: notify the Client within twenty-four (24) hours; consider temporary suspension of data transmission to Google pending resolution; assist the Client in notifying regulators if the breach resulted in a personal data breach.

4.2 AI Use Principles: data minimization (GDPR Art. 5(1)(c)); prohibition on using data to train public models without the Client's explicit written consent; human control — switchover to a live operator is available upon request at any time; transparency — the widget does not deny its AI nature when directly asked by the user.

4.3 Profiling and Automated Decisions.

AI Widget. The AI widget may form a contextual dialogue profile to improve response quality. Such profiling: does not result in automated decisions with legal or significant consequences for the user; may be contested by the user (GDPR Art. 22); is not used to deny service or discriminate.

Automated Decisions Regarding MX12 Client Accounts. MX12 uses automated monitoring tools that may result in automatic suspension of a Client's account upon triggering of AUP violation conditions. Such decisions may have legal consequences. The Client may request human review of such decisions within five (5) business days of the suspension.

4.4 Change of Subprocessors. MX12 notifies the Client of planned changes to or additions of subprocessors no less than thirty (30) days in advance. The Client may object in writing within the stated period. The current subprocessor list is available upon request at **[DPA email].**

4.5 Data Subject Rights in AI Context: right to information about automated processing; right to object to profiling (GDPR Art. 21–22); right to live operator participation instead of AI; right to opt out of profiling; right to portability of dialogue data in machine-readable format (GDPR Art. 20).

5. TRANSFER OF DATA TO THIRD PARTIES

5.1 Data Recipients: operational platforms — Zendesk, Intercom, Freshdesk, Gorgias, HubSpot, SIP/VoIP providers, payment systems (Stripe and others); AI providers — Google Cloud Platform / Google Gemini under SCC and Google Cloud Data Processing Addendum; messenger platforms — Meta (WhatsApp), Telegram, Viber within agreed channels; service providers — IT infrastructure, analytics, cybersecurity; regulatory and law enforcement authorities where there is a lawful requirement.

5.2 What We Do Not Do: do not sell personal data; do not transfer data to third parties for their own marketing purposes without consent; do not use Client end user data for MX12's marketing purposes.

5.3 International Data Transfers:

Direction	Protection Mechanism
EU → USA	SCC (EC Decision 2021/914) + EU-US Data Privacy Framework
EU → USA (Google Gemini)	SCC + Google Cloud Data Processing Addendum
UK → USA	UK International Data Transfer Agreement (IDTA)
Canada → USA	PIPEDA Principle 4.1.3 (contractual protection)
Australia → USA	APP 8 (reasonable protective measures)

DPF Fallback Mechanism. In the event the EU-US Data Privacy Framework is invalidated, MX12 will transition to data transmission based solely on SCC as the fallback mechanism within a reasonable timeframe taking into account operational requirements. Clients from the EU and UK will be notified within five (5) business days of such decision.

5.4 OFAC Sanctions Compliance Disclosure. MX12 may disclose personal data to regulatory authorities including OFAC to the extent required by applicable law or reasonably necessary for sanctions compliance. Such disclosure is made on the basis of a legal obligation (GDPR Art. 6(1)(c)) and does not require data subject consent.

5.5 Transfer Upon Change of Ownership. In the event of merger, acquisition, or sale of MX12 assets, personal data may be transferred to the successor exclusively to the extent necessary for continuity of Services and provided the successor assumes the obligations of this Policy. Clients and data subjects from the EU and UK will be notified no less than thirty (30) days in advance. EU data subjects retain the right to object to the transfer.

6. DATA RETENTION AND PROTECTION

6.1 Retention Periods:

Category	Period	Basis
Client data (contractual)	Contract + 3 years	10 Del. C. § 8106 (statute of limitations for service contracts in Delaware)
Financial and payment records	7 years	US Tax Law / IRS requirements
Tickets and chats	Contract + 2 years	Legitimate interest
AI widget dialogues	Contract + 1 year	Contract performance
VoIP/SIP call recordings	90 days (or per SOW)	Legitimate interest
Website visitor data	12 months	Delaware Online Privacy Act
Marketing communications	Until consent withdrawal + 1 year	GDPR Art. 6(1)(a)

Upon expiration of periods, data is permanently deleted or anonymized. Periods are extended in the presence of ongoing judicial or regulatory proceedings, law enforcement requirements, or other mandatory legal grounds.

6.2 Data Retention Upon Contract Termination. After termination of the agreement with the Client, MX12 as processor: upon the Client's written request — returns or deletes Client end user data within thirty (30) days; in the absence of Client instructions within fifteen (15) business days of termination — deletes end

user data in accordance with the periods in Section 6.1; provides the Client with written confirmation of deletion upon request. This provision implements the requirement of GDPR Art. 28(3)(g).

6.3 Security Measures: encryption of data at rest and in transit using industry standards; role-based access control; two-factor authentication; personnel activity audit; regular security testing; personnel training; secure API connections with subprocessors.

Security Disclaimer. Despite the measures applied, no internet data transmission system can be guaranteed to be free from all risks. MX12 is not liable for security breaches arising from circumstances outside its reasonable control.

6.4 Breach Notification:

Jurisdiction	Timeline	Regulator
Delaware	Without unreasonable delay, no later than 60 days after determination of breach	Delaware Identity Theft Prevention Act (6 Del. C. § 12B-101)
EU	72 hours after determination	Supervisory authority of country of residence (GDPR Art. 33)
UK	72 hours after determination	ICO (UK GDPR Art. 33)
Canada	Shortest reasonable time	OPC (PIPEDA Breach Regulations)
Australia	30 days after determination	OAIC (Privacy Act, NDB scheme)

6.5 Internal Breach Response Procedure. Upon detection or suspicion of a breach, MX12 will: immediately isolate affected systems; conduct a preliminary assessment of scope within twenty-four (24) hours; notify regulators within the established timelines (Section 6.4); notify affected data subjects if the breach creates a high risk to their rights (GDPR Art. 34); document the incident pursuant to GDPR Art. 33(5).

6.6 Breach Due to Client Fault. If a breach of end user data occurred as a result of Client actions or omissions — transmission of data without consent, configuration errors, compromise of Client credentials, or actions of Client's third-party integrations — MX12 bears no liability for such breach. The Client must

immediately notify MX12 of any security incident on its side affecting data processed by MX12. The Client independently bears all costs associated with notification of regulators and data subjects upon a breach due to its fault.

7. YOUR RIGHTS BY JURISDICTION

7.1 EU / EEA — GDPR: access (Art. 15); rectification (Art. 16); erasure (Art. 17); restriction of processing (Art. 18); portability in machine-readable format including AI dialogue data (Art. 20); objection (Art. 21); opt-out from automated decisions with legal consequences (Art. 22); withdrawal of consent (Art. 7(3)). Complaints — supervisory authority of country of residence: edpb.europa.eu.

7.2 UK — UK GDPR + DPA 2018: Equivalent rights under UK GDPR. Data transfers — under UK IDTA. Complaints — ICO: ico.org.uk.

7.3 USA — Delaware DPDPA + California CCPA/CPRA:

Delaware — Delaware Personal Data Privacy Act (DPDPA, 6 Del. C. § 12D-101 et seq., effective January 1, 2025): right of access; rectification; erasure; portability; opt-out from sale of personal data; opt-out from targeted advertising; opt-out from profiling with legally significant consequences. Complaints — Attorney General of Delaware: ago.delaware.gov.

California — CCPA/CPRA: right to know what data is collected; right to deletion; right to rectification; right to portability; right to opt out of sale and sharing of data (MX12 does not sell personal data). Right to opt out of targeting and profiling — to the extent applicable under CCPA/CPRA and implementing regulations as currently in effect. Complaints — CPPA: cppa.ca.gov.

7.4 Canada — PIPEDA + Quebec Law 25: PIPEDA: access, rectification, withdrawal of consent. Complaints — OPC: priv.gc.ca. Quebec (Law 25): erasure, portability, mandatory Privacy Impact Assessment (PIA) for AI processing including Google Gemini. Complaints — CAI: cai.quebec.ca.

7.5 Australia — Privacy Act 1988: APP 12 (access); APP 13 (rectification); APP 5 (notification of collection purposes). Complaints — OAIC: oaic.gov.au.

7.6 UAE (DIFC) — Data Protection Law 2020: access, rectification, erasure, portability, objection. Complaints — DIFC Commissioner of Data Protection: difc.ae.

7.7 Global Baseline Standard: right to know what is collected and for what purposes; access to data; rectification of inaccurate data; withdrawal of consent for marketing communications. Requests — **[data requests email].**

7.8 Grounds for Lawful Refusal. MX12 may decline to fulfill a data subject right request where: fulfilling the request conflicts with mandatory law (for example, a request to delete financial data that MX12 is required to retain for 7 years under US tax law); the request is manifestly unfounded or excessively repetitive (GDPR Art. 12(5)); fulfilling the request would harm the rights and freedoms of third parties. Upon refusal, MX12 notifies the data subject within the established timelines with the specific grounds for refusal and information about the right to contact a supervisory authority.

8. HOW TO EXERCISE RIGHTS

Single contact for all jurisdictions: **[data requests email]**

Jurisdiction	Response Period	Extension
EU / UK	30 days	+ 60 days with notice
Delaware / California	45 days	+ 45 days with notice
Canada / PIPEDA	30 days	up to 30 days for complexity
Australia	30 days	reasonable period
Global	30 days	+ 30 days with notice

MX12 may request identity verification before processing a request. Requests are processed free of charge except for manifestly unfounded or excessively repetitive requests (GDPR Art. 12(5)).

9. COOKIES

9.1 Categories: strictly necessary — technically required, no consent needed; analytical, functional, marketing — require user consent.

9.2 Consent Management. Upon first visit a cookie banner is displayed implemented through a Consent Management Platform (CMP) compatible with IAB TCF 2.2 where implemented. For California — "Do Not Sell or Share My Personal Information" button. For Quebec — explicit consent before setting non-essential cookies.

9.3 Withdrawal of Consent. The user may at any time modify or withdraw cookie consent through the cookie banner settings at mirrax12.world. Withdrawal of consent is as simple as providing it (GDPR Art. 7(3)).

9.4 Retention Periods: strictly necessary — session or up to 12 months; analytical — up to 24 months; marketing — up to 12 months or until consent withdrawal. Full cookie list with name, provider, purpose, and retention period is available in the Cookie Policy at mirrax12.world.

MX12 does not create detailed behavioral profiles without explicit consent (Delaware Online Privacy and Protection Act, 6 Del. C. § 1201C; Delaware Personal Data Privacy Act, 6 Del. C. § 12D-101 et seq.).

10. CHILDREN

MX12 does not provide Services to persons below the applicable age of consent. Upon discovery of such persons' data — immediate deletion. The Client must ensure its end users meet the age requirements of applicable jurisdictions.

Jurisdiction	Regime	Law
EU / UK	Under 16 (min. 13 per national law) requires parental consent	GDPR Art. 8; UK GDPR
USA — under 13	Data collection requires parental consent	COPPA (15 U.S.C. § 6501 et seq.)
USA — 13–16	Sale and sharing of data requires opt-in consent	CCPA/CPRA
Canada	Under 13 — parental consent	PIPEDA
Australia	Assessed individually based on the person's maturity and capacity to understand what they are consenting to; no fixed statutory age threshold	Privacy Act 1988; OAIC guidance
Global baseline	16 years as the recommended standard absent other applicable law indications	—

11. DPA

For Clients from regulated jurisdictions, MX12 provides a modular DPA:

Module 1 — EU GDPR
Module 2 — UK GDPR
Module 3 — CCPA
Module 4 — PIPEDA / Quebec Law 25
Module 5 — Australia Privacy Act.

MX12's subprocessor list with name, country, and processing purpose is provided together with the DPA or upon separate request.

DPA and subprocessor list requests: **[DPA email]**

12. CONTACT DETAILS

MX12 LLC · **[Legal Address]** · **[email]** · mirrax12.world

Jurisdiction	Regulator	Website
EU	Supervisory authority of country of residence	edpb.europa.eu
UK	Information Commissioner's Office	ico.org.uk
Delaware	Attorney General	ago.delaware.gov
California	CPPA	cppa.ca.gov
Canada	OPC	priv.gc.ca
Quebec	CAI	cai.quebec.ca
Australia	OAIC	oaic.gov.au
UAE (DIFC)	DIFC Data Protection	difc.ae

13. POLICY AMENDMENTS

MX12 may update this Policy upon changes in law of any jurisdiction, platform policies, or operational processes. Material changes take effect **thirty (30) days** after publication at mirrax12.world. Clients from the EU, UK, Quebec, and Australia receive direct email notification of material changes.

14. GOVERNING LAW

Base governing law — Delaware Code Title 6 without regard to conflict of laws rules. Regional data protection law applies additionally with respect to data subject rights and mandatory requirements of the relevant jurisdictions. All disputes related to this Policy are resolved pursuant to the procedure provided in the MX12 MSA. This provision does not limit mandatory data subject rights including the right to contact a supervisory authority regardless of any contractual arbitration clause.