Privacy Policy

Effective Date: 22 Feb 2025
Last Updated: 22 Feb 2025

1. Introduction

Halo Digital FZ LLC ("Company," "we," "us," or "our") values your privacy and is committed to protecting your personal data. This Privacy Policy outlines how we collect, process, store, and share your data when you use our services, including our website, AI-powered solutions, and related digital platforms. It also explains your rights and how you can manage your data preferences.

We recognize the importance of privacy and data protection and comply with international data privacy laws, including:

1.1 General Data Protection Regulation (GDPR)

The GDPR (Regulation (EU) 2016/679) is a comprehensive data protection law that applies to individuals located in the European Economic Area (EEA), including the European Union (EU), Norway, Iceland, and Liechtenstein. Under GDPR, we are classified as a Data Controller, meaning we determine how and why your personal data is processed.

GDPR grants individuals several rights over their personal data, including:

- The right to access their data.
- The right to rectification (correct inaccuracies).
- The right to erasure (commonly known as the "right to be forgotten").
- The right to data portability (transfer data to another service).

This Privacy Policy explains how we comply with GDPR when handling data of users in the EEA.

1.2 United Arab Emirates Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (UAE PDPL)

The UAE PDPL is the primary data protection law in the United Arab Emirates, setting out strict guidelines on data collection, processing, and transfer.

Key provisions include:

- Personal data must be processed lawfully, fairly, and transparently.

- Explicit consent is required before processing personal data unless there is a legal exemption.
- Restrictions on transferring personal data outside the UAE unless the receiving country provides adequate protection.
- Individuals have rights similar to GDPR, including the right to access, correct, and delete their data.

As a company operating in the UAE, we adhere to UAE PDPL by ensuring compliance with consent requirements, data protection measures, and legal processing conditions.

1.3 California Consumer Privacy Act (CCPA)

The CCPA (enacted in 2018, amended by CPRA in 2023) provides privacy rights to residents of California, USA. It focuses on giving consumers greater control over their personal data and applies to businesses that process data of California residents.

Under the CCPA, California consumers have the right to:

- Know what personal data is being collected and how it is used.
- Request deletion of their personal data (with some exceptions).
- Opt-out of the sale or sharing of their personal data.
- Receive equal service and pricing even if they exercise their privacy rights.

Unlike GDPR and UAE PDPL, which require businesses to obtain consent for data collection, CCPA follows an opt-out model, meaning that businesses can collect data but must allow users to opt out of certain processing activities, particularly data sharing for targeted advertising.

1.4 Scope of This Privacy Policy

This Privacy Policy applies to:

- Visitors and users of our website and AI-powered solutions.
- Customers who purchase or subscribe to our services.
- Individuals who interact with our marketing campaigns or customer support.
- Business contacts and representatives of organizations that engage with us.

This policy does not cover:

- Data processing activities by third-party services integrated into our platform (see Section 5 on Third-Party Data Sharing).
- Data collected by external websites linked from our platform.

1.5 Your Acknowledgment & Acceptance

By using our services, you confirm that you have read, understood, and agreed to this Privacy Policy. If you do not agree, you should stop using our services immediately and contact us if you have any concerns.

2. Data We Collect

We collect different types of personal data depending on how you interact with our website, services, and AI-powered solutions. This section outlines the categories of data we collect, how it is gathered, and its intended use.

2.1 Personal Data

Personal data refers to any information that directly or indirectly identifies you as an individual. We collect personal data through various interactions with our services, including account registration, customer support, business communications, and marketing activities.

We may collect the following types of personal data:

Account Registration & Service Subscription

When you create an account or subscribe to our services, we collect:

- Name, email address, and phone number – To create and manage your account.
- Login credentials – To provide secure access to our platform.

Payments & Billing Information

When you purchase a paid service or subscription, we collect:

- Billing details and payment information – Including credit/debit card details, billing address, and transaction history.
- Invoice records – To process payments and comply with financial regulations.

Customer Support & Service Interactions

When you contact customer support or engage with our team, we collect:

- Contact information – Such as email, phone number, or company name.
- Support inquiries and correspondence – Including messages, attachments, and chat logs.
- Technical details – Device and software information relevant to troubleshooting.

Business Communication & Lead Qualification

As a business-to-business (B2B) AI-driven lead qualification service, we may process business communications that contain personal data, including:

- Messages exchanged via our platform – Such as emails, chatbot interactions, and CRM-integrated conversations.
- Lead qualification data – Responses submitted through forms, chatbots, or AI-driven assessments.
- Communication logs and transcripts – Used for analytics, sales optimization, and improving service efficiency.

If business communications include personal data (such as names, contact details, or opinions expressed in messages), we process such data in compliance with GDPR, UAE PDPL, and CCPA regulations. Users may request access, correction, or deletion of their communication records where legally applicable.

Surveys, Promotions & Marketing Activities

When you engage with our marketing campaigns, promotions, or events, we may collect:

- Survey responses & feedback – For product and service improvement.
- Preferences & interests – To personalize marketing materials.
- Participation details – Including webinar attendance and promotional redemptions.

Corporate Clients & Business Representatives

For corporate accounts and business partnerships, we collect:

- Company name, job title, and business contact details – For contractual and communication purposes.
- Professional profiles from public sources – Such as LinkedIn, industry directories, or business websites.

We do not knowingly collect sensitive personal data (such as race, religion, health information) unless required by law or explicitly provided by you for a specific purpose.

2.2 Technical Data

We collect technical information automatically when you visit our website:

- IP address, device type, browser version.
- Cookies and tracking technologies (see Section 8).
- Log data (such as access timestamps and interaction history).

2.3 Behavioral Data

To improve our services, we may collect data on how you interact with our platform:

- Pages visited, time spent on pages.
- Clicks, navigation, and engagement metrics.

2.4 Third-Party Data Sources

We may collect data from third-party sources, including:

- Social media integrations (LinkedIn, Facebook).
- Advertising and analytics platforms (Google Ads, Meta Pixel, LinkedIn Insight Tag).

3. How We Use Your Data

We process personal data to operate, improve, and secure our services while ensuring compliance with applicable privacy regulations. Below is a detailed explanation of how we use your data.

3.1 Service Delivery & Personalization

We process your data to provide and enhance our AI-driven lead qualification solutions and ensure a seamless user experience. This includes:

- Account setup and management – Creating and maintaining user accounts, processing login credentials, and verifying identities.
- Lead qualification and sales automation – Analyzing business inquiries, processing lead responses, and integrating with CRM systems.
- Customizing AI interactions – Improving chatbot responses and AI recommendations based on previous user interactions.
- Providing platform functionality – Storing preferences, enabling real-time messaging, and delivering relevant insights.

Processing is based on contractual necessity (to provide our services) and legitimate interests (to improve functionality).

3.2 Customer Support & Issue Resolution

We use personal data to respond to support inquiries, troubleshoot technical issues, and provide assistance. This includes:

- Processing support requests – Using emails, chat messages, or calls to resolve user concerns.
- Accessing communication logs – Reviewing past interactions to provide better assistance.
- Technical debugging – Using log data and device information to identify errors.
- Sending service updates – Notifying users of maintenance, security alerts, or changes in our services.

Processing is based on contractual necessity (to fulfill support obligations) and legitimate interests (to ensure service reliability).

3.3 Analytics & Performance Optimization

We collect behavioral and technical data to analyze website and platform performance, which helps us:

- Measure user engagement – Tracking how users interact with our AI-driven solutions.
- Optimize website functionality – Identifying navigation issues and improving interface design.
- Improve AI accuracy – Analyzing lead qualification effectiveness and adjusting AI models.
- Detect and prevent fraud – Identifying suspicious activity to protect users.

* *Processing is based on legitimate interests (to enhance services) and user consent (for optional analytics tracking).*

3.4 Marketing, Retargeting & Advertising

We use personal data to personalize marketing campaigns and improve ad relevance. This includes:

- Email marketing & newsletters – Sending updates, promotions, and service-related information (with opt-out options).
- Targeted advertising – Delivering relevant ads via Google Ads, Facebook Pixel, LinkedIn Insight Tag, and similar platforms.
- Retargeting campaigns – Showing ads to users who previously interacted with our website.
- Webinar & event invitations – Notifying users about upcoming business-related events.
- Lead nurturing & sales outreach – Following up with potential clients based on business inquiries.

Processing is based on user consent (for email subscriptions and online tracking) and legitimate interests (for B2B outreach and CRM interactions).

3.5 Legal, Security & Compliance

To comply with global privacy regulations and ensure a secure environment, we:

- Fulfill legal obligations – Adhering to GDPR, UAE PDPL, and CCPA data protection laws.
- Process data subject requests – Handling user requests for data access, correction, or deletion.
- Prevent fraud & abuse – Monitoring for fraudulent signups, spam, and unauthorized system access.
- Comply with financial & tax regulations – Retaining transaction records where legally required.

- Respond to law enforcement – Providing legally required disclosures in response to government or regulatory requests.

Processing is based on legal obligations and legitimate interests (to maintain security and prevent misuse).

3.6 Internal Research & AI Model Training

We may use aggregated, anonymized data to improve our AI technology, ensuring better accuracy in lead qualification and customer interactions. This includes:

- Enhancing AI-driven responses – Training models to understand customer intent more effectively.
- Developing new features – Using user feedback to refine automation and CRM integrations.
- Benchmarking AI accuracy – Comparing AI performance across industries and use cases.

Processing is based on legitimate interests (to improve AI models) and user consent (if AI training involves personal data).

3.7 AI & Automated Decision-Making

Our AI-powered lead qualification tools analyze business inquiries, process customer interactions, and generate insights to improve sales and customer engagement.

How AI Analyzes Lead Responses

- AI processes user inquiries, responses, and behavioral data to determine lead quality.
- The system assigns lead scores based on predefined business logic, customer intent, and interaction patterns.
- AI integrates with CRM systems to provide automated insights to sales teams.

Automated Decision-Making & Human Oversight

- AI processing is based on legitimate business interests and does not make legally binding decisions.
- Certain AI-driven actions (e.g., lead scoring, engagement predictions) are fully automated but subject to human review where necessary.
- Users can request a review of AI-based assessments if they believe a decision was incorrect or unfair.

Storage of AI-Processed Data

- AI models may store historical lead interaction data for up to 36 months to improve accuracy and predictive analysis.

- Personal data used for AI training is either anonymized or pseudonymized where possible.
- AI does not process sensitive personal data without explicit user consent.

User Rights & Risk Mitigation

- Users have the right to access AI-generated data related to their interactions.
- If AI-based lead scoring impacts user engagement, they can contest AI-driven decisions.
- We implement bias detection and fairness testing to prevent discriminatory AI outcomes.

4. Legal Basis for Processing

We process personal data based on the applicable legal frameworks, including the General Data Protection Regulation (GDPR) for users in the European Economic Area (EEA), the United Arab Emirates Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (UAE PDPL) for users in the UAE, and the California Consumer Privacy Act (CCPA) for users in California, USA. This section outlines the legal bases on which we process personal data under these regulations.

4.1 GDPR (EEA Users)

Under the GDPR (Regulation (EU) 2016/679), we must have a valid legal basis for processing personal data. We rely on the following lawful bases:

Consent (Article 6(1)(a) GDPR)

We process personal data based on explicit user consent in the following situations:

- When users accept cookies for analytics, advertising, and personalization.
- When users opt in to receive marketing emails, newsletters, or promotional offers.
- When we use personal data for AI training or data enrichment (if applicable).
- When processing sensitive personal data (only when required and explicitly agreed to).

Users can withdraw their consent at any time through their account settings or by contacting us at support@halodigitalai.com

Contractual Necessity (Article 6(1)(b) GDPR)

Processing is necessary for the performance of a contract when:

- Users create an account and subscribe to our AI-driven lead qualification services.
- We process payment details for billing purposes.
- We provide customer support and fulfill contractual obligations.

Without this processing, we would be unable to provide our services to users.

Legitimate Interests (Article 6(1)(f) GDPR)

We process data when it is necessary for our legitimate business interests, provided it does not override user rights. Examples include:

- Monitoring website performance and improving AI accuracy.
- Detecting fraudulent activities and securing our platform.
- Conducting business communications, sales outreach, and lead qualification.
- Processing CRM interactions to improve customer engagement.

Users can object to processing based on legitimate interests by contacting us.

Legal Compliance (Article 6(1)(c) GDPR)

We process data to comply with legal and regulatory obligations, such as:

- Retaining payment and tax records as required by financial regulations.
- Responding to data access and deletion requests under GDPR.
- Preventing fraudulent activity and ensuring cybersecurity compliance.

4.2 UAE PDPL (UAE Users)

The **UAE PDPL** applies to the collection, storage, and transfer of personal data within the United Arab Emirates. We process personal data based on the following legal justifications:

User Consent (Mandatory for Marketing & Data Transfers)

Under UAE PDPL, explicit consent is required for:

- Marketing communications, such as promotional emails and remarketing campaigns.
- International data transfers, unless the receiving country has an adequate data protection framework.

Users can withdraw their consent at any time through their privacy settings.

Contractual Obligations

We process personal data without requiring additional consent when it is necessary for:

- Providing our services, including AI-driven lead qualification.
- Processing payments and handling invoices.
- Maintaining business communications with clients and prospects.

Legal Compliance & Public Interest

Certain types of data processing are permitted without consent when required by:

- Regulatory authorities in cases of fraud prevention or security threats.
- Financial regulations for record-keeping of transactions and billing data.
- Law enforcement requests related to cybersecurity risks or investigations.

We ensure that all international data transfers comply with UAE PDPL by implementing safeguards, such as Standard Contractual Clauses (SCCs) or obtaining user consent where necessary.

4.3 CCPA (California Users)

Under the **California Consumer Privacy Act (CCPA)**, California residents have specific rights regarding their personal data.

Right to Opt-Out of Data "Sales" or "Sharing"

The CCPA defines "selling" personal data as disclosing or sharing it for monetary or other valuable consideration. While we do not sell personal data, we may:

- Share data with third-party advertising networks for marketing and retargeting purposes.
- Use tracking technologies (such as Facebook Pixel or Google Ads) to optimize ad performance.

California users can opt out of data sharing for advertising purposes via our Cookie Settings or by submitting a "Do Not Sell or Share My Personal Information" request.

Right to Know & Right to Delete

Under the CCPA, California users can:

- Request a copy of the personal data we have collected about them.
- Request deletion of their personal data unless retention is required for legal or operational reasons.

Deletion requests can be submitted through our privacy portal or by contacting support@halodigitalai.com

Right to Non-Discrimination

Users exercising their CCPA rights will not:

- Be denied services.
- Be charged higher fees.
- Receive a lower quality of service.

We treat all users fairly, regardless of their privacy preferences.

5. Data Sharing and Third Parties

We do not sell personal data. However, to provide our services efficiently, we share data with trusted third-party providers that support our operations, ensuring compliance with GDPR, UAE PDPL, and CCPA. This section details the types of third parties with whom we share data, the purpose of such sharing, and how we safeguard international data transfers.

5.1 Categories of Third Parties We Share Data With

We may share personal data with the following categories of third parties:

Cloud Hosting & Infrastructure Providers

To store and process data securely, we rely on cloud computing and infrastructure providers that enable us to host, manage, and scale our services. These providers may include:

- Amazon Web Services (AWS), Google Cloud, Microsoft Azure, Digital Ocean and other providers – Cloud hosting and data storage solutions.
- CDN (Content Delivery Networks) – Providers that optimize website performance and load speed.

These providers operate under strict security and compliance frameworks, ensuring data is encrypted and protected against unauthorized access.

Payment Processors & Financial Institutions

If you purchase a subscription or make a payment, your payment details are processed by third-party payment service providers, including:

- Stripe, MamoPay or other payment gateways – For secure online transactions.
- Banks & financial institutions – For fraud prevention and compliance with financial regulations.

We do not store or process payment card details directly; instead, we rely on PCI DSS-compliant third-party providers.

Analytics & Marketing Platforms

We use third-party analytics and advertising platforms to improve our services, measure user engagement, and deliver personalized marketing campaigns. These may include:

- Google Analytics, Hotjar, Microsoft Clarity – To track user interactions and optimize website performance.
- Google Ads, Facebook Pixel, LinkedIn Insight Tag – For advertising and retargeting campaigns.

- Email marketing services (e.g., Mailchimp, HubSpot, SendGrid) – To send newsletters and promotional emails.

Users can manage their cookie preferences or opt out of targeted advertising through our Cookie Policy settings.

CRM & Sales Automation Tools

To manage business relationships and streamline sales processes, we may share data with:

- Customer Relationship Management (CRM) software – To track leads, manage sales pipelines, and improve communication.
- AI-driven automation tools – To enhance lead qualification and customer engagement.

These tools store and process data in accordance with international privacy laws.

Customer Support & Communication Services

We use third-party communication platforms to provide customer support and ensure efficient service delivery. These may include:

- Live chat providers (e.g., Intercom, Zendesk, Freshdesk and other) – For real-time customer assistance.
- Help desk ticketing systems – To manage user inquiries and support cases.
- Voice & video call providers (e.g., Zoom, Twilio, WhatsApp Business API and other) – For customer interactions.

Support interactions may be recorded for quality assurance and training purposes, as permitted by law.

Regulatory & Law Enforcement Authorities

We may disclose personal data when required by applicable laws, court orders, or regulatory authorities in the following situations:

- To comply with financial and tax regulations.
- To respond to legal processes, subpoenas, or government requests.
- To investigate fraud, cyber threats, or illegal activities.

Such disclosures will only occur where legally necessary, and we will notify users unless prohibited by law.

5.2 International Data Transfers

Since we operate globally, personal data may be transferred to and processed in jurisdictions outside of the European Economic Area (EEA), the United Arab Emirates (UAE), and the United States (US). When transferring data internationally, we implement the following safeguards:

Standard Contractual Clauses (SCCs) – GDPR Compliance

For data transfers outside the EEA, we rely on Standard Contractual Clauses (SCCs) approved by the European Commission, ensuring that third parties provide an adequate level of protection.

UAE PDPL Compliance – Data Transfer Restrictions

Under **UAE PDPL**, data transfers outside the UAE require:

- Adequacy assessment – Ensuring that the recipient country has a comparable level of data protection.
- User consent – If an adequacy decision is not in place.
- Contractual safeguards – Similar to SCCs, ensuring lawful processing.

Data Privacy Framework (DPF) – US Compliance

For data transfers to the United States, we comply with the Data Privacy Framework (DPF) where applicable or ensure contractual safeguards.

Additional Security Measures

Regardless of jurisdiction, we implement:

- End-to-end encryption for data in transit and at rest.
- Restricted access controls to limit data exposure.
- Anonymization and pseudonymization where possible to enhance privacy.

Users may contact us to inquire about specific data transfer mechanisms applicable to their region.

5.3 How We Ensure Data Security with Third Parties

We require all third-party service providers to:

- Comply with GDPR, UAE PDPL, and CCPA regulations.
- Use encryption and industry-standard security measures to protect user data.
- Sign Data Processing Agreements (DPAs) to ensure data protection obligations.
- Limit data retention periods to only what is necessary for business purposes.

We conduct regular audits and risk assessments to verify compliance with these security standards.

5.4 User Control & Opt-Out Options

Users can control how their data is shared with third parties:

- Manage cookie preferences – Adjust settings for analytics and advertising cookies in our Cookie Policy.
- Opt out of marketing emails – Unsubscribe using the link in any marketing email.
- Request data deletion – Users can submit a request to delete personal data where legally applicable.

6. Data Retention & Security

We are committed to ensuring that personal data is retained only for as long as necessary to fulfill its intended purpose, comply with legal obligations, or meet business requirements. This section details how long we retain different categories of data and the measures we take to protect it.

6.1 Retention Period

We store personal data based on the type of data and the purpose for which it is collected. Below is an overview of our data retention periods:

User Account Data

- Retention Period: As long as the account remains active.
- Purpose: To provide continuous access to our services, maintain user preferences, and ensure account security.
- Deletion Policy: When a user requests account deletion or has been inactive for more than 36 months, their personal data is deleted or anonymized unless retention is required by law.

Payment & Transaction Records

- Retention Period: Retained for a minimum of 5 years (or as required by financial regulations).
- Purpose: To comply with accounting, tax, and anti-fraud regulations.
- Deletion Policy: After the legal retention period, records are securely deleted unless required for legal disputes.

Customer Support & Communication Logs

- Retention Period: Stored for 12 months from the last interaction.
- Purpose: To resolve disputes, improve customer support, and enhance service quality.

- Deletion Policy: Deleted automatically after 12 months unless required for regulatory compliance or internal audits.

Analytics & Website Interaction Data

- Retention Period: Stored for up to 24 months.
- Purpose: To measure website performance, analyze trends, and improve user experience.
- Deletion Policy: Automatically purged after 24 months, unless retained in an aggregated, anonymized format.

Marketing & Advertising Data

- Retention Period: Retained until the user opts out of marketing communications.
- Purpose: To send promotional emails, retargeting campaigns, and personalized recommendations.
- Deletion Policy: Users can unsubscribe from emails or request data deletion at any time.

CRM & Sales Data (Lead Qualification)

- Retention Period: Stored for up to 36 months from the last interaction.
- Purpose: To track business relationships, sales opportunities, and lead engagement.
- Deletion Policy: Automatically deleted after 36 months unless the lead converts into a paying customer.

Regulatory & Compliance Data

- Retention Period: As required by applicable laws and regulations.
- Purpose: To comply with GDPR, UAE PDPL, and CCPA requirements, financial reporting, and fraud investigations.
- Deletion Policy: Removed after the legal requirement expires, unless required for pending legal matters.

6.2 Security Measures

We implement stringent security measures to protect personal data from unauthorized access, alteration, disclosure, or destruction. These measures include:

Data Encryption

- In Transit: All data transmitted between users and our servers is encrypted using TLS (Transport Layer Security) 1.2 or higher.
- At Rest: Stored data is encrypted using AES-256 encryption to prevent unauthorized access.

Access Controls & Authentication

- Role-Based Access (RBAC): Only authorized personnel have access to sensitive data.
- Multi-Factor Authentication (MFA): Required for internal systems handling personal data.
- Regular Access Reviews: We periodically audit access logs to prevent unauthorized usage.

Network & Infrastructure Security

- Firewall & Intrusion Detection Systems (IDS): To monitor and block unauthorized access attempts.
- DDoS Protection: Implemented to safeguard against distributed denial-of-service attacks.
- Regular Security Audits: We conduct penetration testing and vulnerability assessments.

Data Anonymization & Minimization

- Anonymization: Where possible, personal data is anonymized for analytics and research.
- Data Minimization: We only collect the data necessary for the intended purpose.

Incident Response & Breach Notification

- 24/7 Monitoring: Our security team continuously monitors for potential threats.
- Breach Notification Protocol: In case of a data breach, affected users will be notified within 72 hours in compliance with GDPR and UAE PDPL regulations.

6.3 User Control Over Data Retention

Users have the following rights regarding data retention:

- Request Deletion: Users may request their data be deleted unless required for legal or regulatory purposes.
- Update or Correct Data: Users can modify their personal details through their account settings.
- Withdraw Consent: Marketing preferences and cookie tracking can be managed via account settings or the Cookie Policy.

6.4 Data Breach Notification

We implement strict security measures to protect personal data; however, in the event of a data breach, we follow legal requirements to notify affected users and regulators.

GDPR Compliance (EEA Users)

- In accordance with Article 33 of the GDPR, we will notify the relevant Data Protection Authority (DPA) within 72 hours of becoming aware of a breach, unless it is unlikely to result in a risk to individuals' rights and freedoms.

- If the breach poses a high risk to users, we will also notify affected individuals without undue delay.

UAE PDPL Compliance (UAE Users)

- Under the UAE PDPL, organizations are required to notify the UAE Data Office or other designated regulators if a data breach occurs that may cause harm to individuals.
- The law does not specify a strict 72-hour deadline as in GDPR, but best practices recommend following similar response times.
- If personal data of UAE residents is affected, we will assess the risks and take appropriate actions, including informing users and authorities when required.

CCPA Compliance (California Users)

- The CCPA does not have a strict data breach notification deadline, but businesses are required to inform affected users and take remedial actions in case of unauthorized access to personal data.
- If a breach meets the criteria of the California Data Breach Notification Law, we will notify the California Attorney General and affected individuals in a timely manner.

Notification Process & User Rights

- If required, notifications will be sent via email, website announcements, or direct communication.
- Users have the right to request details on the nature of the breach and the measures taken to mitigate risks.

7. User Rights

Users have specific rights regarding the collection, processing, and storage of their personal data, which vary based on their location. This section outlines the rights granted under the General Data Protection Regulation (GDPR) for users in the European Economic Area (EEA), the United Arab Emirates Personal Data Protection Law (UAE PDPL) for users in the UAE, and the California Consumer Privacy Act (CCPA) for users in California, USA.

7.1 GDPR Rights (EEA Users)

Under the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), individuals in the EEA (European Economic Area) have the following rights regarding their personal data:

Right to Access (Article 15 GDPR)

Users can request confirmation of whether we process their personal data and obtain:

- A copy of the personal data we hold about them.

- Information about the purposes of data processing.
- Details on third parties with whom their data has been shared.

Right to Rectification (Article 16 GDPR)

If personal data is inaccurate or incomplete, users can request corrections or updates.

Right to Erasure ("Right to be Forgotten") (Article 17 GDPR)

Users may request the deletion of their personal data under certain conditions, such as:

- The data is no longer necessary for the purpose it was collected.
- The user withdraws consent (where processing was based on consent).
- The data was unlawfully processed.

Exceptions apply where retention is legally required (e.g., tax records, fraud prevention).

Right to Restrict Processing (Article 18 GDPR)

Users can request limited processing of their data if:

- The accuracy of the data is contested.
- Processing is unlawful, but the user does not want it deleted.
- The data is needed for legal claims.

Right to Object (Article 21 GDPR)

Users can object to the processing of their personal data when processing is based on:

- Legitimate interests (e.g., business analytics, AI improvement).
- Direct marketing (users can opt out at any time).

Right to Data Portability (Article 20 GDPR)

Users can request a structured, machine-readable copy of their data and transfer it to another service provider.

Right to Withdraw Consent

Where processing is based on user consent (e.g., marketing emails, cookies), users can withdraw consent at any time.

7.2 UAE PDPL Rights (UAE Users)

Under the United Arab Emirates Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (UAE PDPL), users in the UAE have rights similar to those under GDPR but with additional restrictions on international data transfers.

Right to Access

Users have the right to:

- Request confirmation of whether their personal data is being processed.
- Obtain a copy of their personal data.

Right to Rectification

Users can request corrections if their personal data is inaccurate or incomplete.

Right to Erasure ("Right to be Forgotten")

Users can request deletion of their data unless retention is legally required or necessary for ongoing business operations.

Right to Restrict Processing

Users can request restrictions on how their data is processed in cases where:

- The accuracy of the data is contested.
- The processing is unlawful but the user does not want data deleted.
- The data is no longer needed but required for legal claims.

Right to Object to Processing

Users may object to data processing if it is used for:

- Direct marketing.
- Automated decision-making that affects their rights.

Right to Data Portability

Users can request a copy of their data in a structured, commonly used format for transfer to another entity.

Right to Withdraw Consent

Users can withdraw consent for data processing where consent was the legal basis (e.g., marketing emails, international data transfers).

Restrictions on International Data Transfers

Unlike GDPR, UAE PDPL imposes strict rules on cross-border data transfers, requiring:

- User consent for transfers to countries without adequate data protection laws.
- Regulatory approval for transfers outside the UAE in certain circumstances.

7.3 CCPA Rights (California Users)

Under the California Consumer Privacy Act (CCPA) (as amended by CPRA in 2023), California residents have the following rights:

Right to Know (Access to Information)

Users can request:

- The categories of personal data we collect.
- The purpose of data collection and whether data is shared with third parties.
- The categories of third parties with whom we share personal data.

Right to Delete

Users can request the deletion of their personal data, subject to exceptions where retention is required for:

- Completing a transaction or providing a service.
- Security and fraud prevention.
- Legal and regulatory compliance.

Right to Opt-Out of Data Sharing ("Do Not Sell or Share My Personal Information")

CCPA defines "selling" personal data as sharing it for monetary or valuable consideration. We do not sell personal data, but users can opt out of:

- Targeted advertising using cookies and tracking technologies.
- Sharing of behavioral data with third-party marketing platforms.

Users can opt out via:

- Our Cookie Consent Tool (to disable tracking technologies).
- "Do Not Sell or Share My Personal Information" request form (available in our Privacy Settings).

Right to Correct Inaccurate Information

Users can request updates or corrections to their personal data.

Right to Limit Use of Sensitive Personal Data

Users can restrict how certain types of sensitive data (e.g., financial, biometric) are used.

Right to Non-Discrimination

We will not:

- Deny services to users who exercise their privacy rights.
- Charge different prices or offer lower service quality based on privacy choices.

7.4 Exercising Your Rights

Users can submit requests regarding their data by contacting:

Email: support@halodigital.ai

To verify identity, we may:

- Request additional information to confirm user identity.
- Require authentication via registered email or phone.

We will respond within:

- 30 days for GDPR and UAE PDPL requests (extendable under complex cases).
- 45 days for CCPA requests (extendable by an additional 45 days if necessary).

For opt-out requests related to cookies and targeted advertising, users can manage their preferences via our Cookie Settings page.

8. Cookies & Tracking Technologies

We use cookies and similar tracking technologies to enhance user experience, analyze website performance, and support advertising and marketing efforts. These technologies help us understand how users interact with our services and allow us to deliver relevant content. For a detailed breakdown of our cookie practices, please refer to our **Cookie Policy**.

8.1 What Are Cookies and Tracking Technologies?

Cookies are small text files stored on your device when you visit our website. Other tracking technologies, such as pixels, tags, and scripts, work similarly by collecting data about user interactions. These technologies allow us to:

- Improve website functionality and security.
- Track and analyze user behavior to enhance our services.
- Personalize content and marketing campaigns.

8.2 Types of Cookies We Use

We categorize cookies based on their function and necessity:

Essential Cookies (Strictly Necessary)

- Required for core website functions (e.g., authentication, security).
- Cannot be disabled as they are crucial for service operation.

Functional Cookies

- Store user preferences (e.g., language settings, session history).
- Improve navigation and enhance user experience.

Analytics & Performance Cookies

- Help us measure traffic, monitor errors, and optimize performance.
- Example: Google Analytics, Hotjar, Microsoft Clarity.

Advertising & Targeting Cookies

- Enable personalized ads and retargeting across platforms.
- Example: Google Ads, Facebook Pixel, LinkedIn Insight Tag, TikTok Pixel.
- Users can opt out of targeted advertising via their Ad Preferences Settings.

8.3 How Users Can Manage Cookies

Users can control cookie preferences in several ways:

- Browser Settings: Most browsers allow users to block or delete cookies.
- Cookie Consent Banner: Manage settings through our on-site consent tool.
- Ad Platform Opt-Outs: Users can disable personalized ads via:
    - Google Ad Settings
    - Facebook Ad Preferences
    - LinkedIn Ads Settings

For more information, including retention periods and opt-out procedures, please review our Cookie Policy.

9. Data Transfers Outside the EU, UAE, and US

Since we operate globally, we may transfer personal data to locations outside the European Economic Area (EEA), the United Arab Emirates (UAE), and the United States (US). When doing so, we ensure that adequate protections are in place to safeguard personal data in compliance with GDPR, UAE PDPL, and CCPA.

9.1 How We Ensure Secure Data Transfers

When transferring personal data internationally, we implement the following safeguards:

Standard Contractual Clauses (SCCs) – GDPR Compliance

For data transfers outside the EEA, we rely on Standard Contractual Clauses (SCCs) approved by the European Commission. These contractual agreements ensure that third-party recipients uphold EU-level data protection standards.

UAE PDPL Compliance – Data Transfer Restrictions

Under the UAE Personal Data Protection Law (UAE PDPL), data transfers outside the UAE require:

- Adequacy assessment – Ensuring that the destination country has an equivalent level of data protection.
- User consent – If an adequacy decision is not in place, explicit user consent may be required.
- Contractual safeguards – Agreements similar to SCCs must be in place with non-UAE recipients.

Data Privacy Framework (DPF) – US Compliance

For data transfers between the US and the EU or UAE, we comply with the EU-US Data Privacy Framework (DPF) where applicable, or ensure contractual safeguards equivalent to SCCs.

Binding Corporate Rules (BCRs) – Where Applicable

For intra-company transfers across multiple jurisdictions, we may implement Binding Corporate Rules (BCRs) approved by data protection authorities.

9.2 Additional Security Measures

Regardless of jurisdiction, we apply the following protections when transferring data internationally:

- Encryption – Data is encrypted both in transit and at rest.
- Access Controls – Restricted access to personal data based on necessity.
- Data Minimization – Only the necessary data is transferred.
- Ongoing Compliance Audits – Regular assessments of international data transfers.

9.3 Where We Transfer Data

We may transfer personal data to:

- Cloud hosting providers (e.g., AWS, Google Cloud, Microsoft Azure, Digital Ocean) with international data centers.
- Payment processors and financial institutions handling cross-border transactions.
- Analytics and marketing platforms operating in multiple jurisdictions.
- Customer support services with offshore or regional support teams.

9.4 User Rights Regarding International Transfers

Users can:

- Request details on how their data is transferred.
- Withdraw consent for international transfers where required by law.
- Object to transfers in certain cases where data protection adequacy is uncertain.

10. Updates to This Policy

We may update this Privacy Policy from time to time to reflect:

- Changes in applicable privacy laws and regulations – including but not limited to updates to the General Data Protection Regulation (GDPR), United Arab Emirates Personal Data Protection Law (UAE PDPL), California Consumer Privacy Act (CCPA), and other international data protection frameworks.
- Changes in regulatory guidance or enforcement requirements – to align with evolving interpretations and enforcement actions by data protection authorities.
- Changes in business operations – such as expansion into new markets, introduction of new services, or modifications to our data processing activities.
- Changes in partnerships and third-party service providers – if we engage new vendors or discontinue relationships with existing third parties that process personal data.
- Security and compliance improvements – to enhance data protection practices, mitigate emerging security threats, or implement industry best practices.
- User experience enhancements – including adjustments to our privacy practices based on feedback, usability improvements, or new features requiring updates to data handling procedures.

10.1 How We Notify Users of Updates

If we make material changes to this Privacy Policy that significantly affect how we process personal data, we will provide notice through one or more of the following methods:

- Email notification – Sent to registered users and subscribers.
- Website notification – Displayed on our homepage or privacy settings page.
- Account dashboard alerts – If applicable to account holders.

For non-material updates, we will update the "Last Updated" date at the top of this Privacy Policy and encourage users to review the latest version.

10.2 Continued Use After Updates

By continuing to use our services after the updated Privacy Policy takes effect, users acknowledge and accept the revised terms.

If users do not agree with the changes, they may:

- **Review their privacy settings** and adjust preferences accordingly.
- **Contact us** for further clarification regarding the updates.
- **Discontinue use of the services** if they disagree with the revised policy.

11. Contact Information

For privacy-related inquiries, please contact:
Email: support@halodigitalai.com
Website: http://halodigital.ai