LEGAL DOCUMENT

Data & InfoSec Policy

Security commitments, compliance roadmap, and data handling

Version 1.2 · May 2026 · 365Agents, Inc.

365 AGENTS, INC.

DATA & INFOSEC POLICY (v1.2)

Changes from v1.1: Added Section 1 (Compliance Roadmap) consolidating 365Agents' current and planned attestations and certifications (SOC 2, ISO/IEC 42001, PCI DSS, HIPAA, USDP). Renumbered subsequent sections accordingly. **Changes from v1.0 (carried forward):** Renumbered sections to fix the duplicate "Section 7" bug. Harmonized terminology with the MSA, Reseller Agreement, and SLA. Added incident-notification timing aligned with the agreements (72 hours from confirmation; ≤ 24 hours for active material risk). Aligned defined terms.

This Data & InfoSec Policy ("**Policy**") is incorporated into and governed by the terms of a customer's agreement with 365Agents, Inc. ("**365Agents**") for access to and use of the 365Agents Platform (the "**Agreement**"). Capitalized terms not defined here have the meanings given in the Agreement. "**Customer**" includes both direct customers under the MSA and Resellers under the Reseller / White-Label Agreement.

---

1. COMPLIANCE ROADMAP

365Agents pursues an aggressive compliance posture appropriate to a modern AI voice and text platform serving regulated and unregulated SMB markets. Status as of the date of this Policy:

Framework	Status	Detail
SOC 2 Type I	✅ Achieved	Independent attestation by [insert auditor name]; report dated [insert]. Renewed annually.
SOC 2 Type II	▯ Planned	Type II observation period commencing [insert date]; target attestation [insert quarter].
ISO/IEC 42001:2023 (AI Management System)	✅ Certified	Certificate issued by [insert accredited certification body]; certificate dated [insert]. The first ISO standard specifically for AI governance — covers risk management, lifecycle controls, transparency, and human oversight.
PCI DSS — Service Provider	✅ Attestation Level [2/3/4 — confirm]	Attestation of Compliance (AOC) dated [insert]; scope-minimization design — cardholder data is not stored on the Platform unless Customer enables PCI-compliant payment flows.
HIPAA	✅ BAA-ready	365Agents implements administrative, physical, and technical safeguards consistent with the HIPAA Security Rule and is prepared to execute a Business Associate Agreement (BAA) for

		Customer use cases involving PHI. PHI processing requires (a) an executed BAA and (b) PHI-mode enabled at the account level. *Note: HIPAA does not provide for a "certification"; "BAA-ready" is the operational status.*
U.S. Data Privacy (USDP)	▯ In Progress	365Agents is implementing a unified U.S. multi-state privacy program tracked in Vanta, harmonizing obligations under CCPA/CPRA (California), VCDPA (Virginia), CPA (Colorado), CTDPA (Connecticut), UCPA (Utah), and the rolling wave of similar state laws (TX TDPSA, OR OCPA, TN TIPA, FL FDBR, MD MODPA, MN MCDPA, NJ NJDPA, DE DPDPA, NH NHPA, IA ICDPA, IN ICDPA, MT MCDPA, RI, NE, KY, etc.). Target completion [insert quarter].
GDPR / UK GDPR / Swiss FADP	☑ DPA-ready	Data Processing Addendum incorporates EU Standard Contractual Clauses (SCCs) and UK Addendum; available on request prior to processing EU/UK personal data.
CCPA / CPRA	☑ Compliant	Consumer rights portal at https://365agents.com/privacy-requests; "Do Not Sell or Share" honored; 45-day response window with permitted 45-day extension.
TCPA / TSR / state telemarketing & AI-disclosure laws	☑ Customer-configurable controls	Platform provides consent capture, do-not-call list integration, AI-disclosure prompts, "click-to-cancel" mechanics, and time-window controls; Customer is responsible for configuration consistent with applicable jurisdictions.

Forward-looking statements. Items listed as "Planned" or "In Progress" are targets, not contractual commitments. Achieved attestations and certifications are subject to annual renewal and may lapse if not renewed; Customers will be notified through this Policy when material changes occur. Copies of attestation reports, AOCs, and certificates are available under NDA on written request to security@365agents.com.

---

2. SECURITY INFRASTRUCTURE AND COMMITMENTS

(a) Security standards. 365Agents maintains security measures designed to protect Customer Data, including:

- Encryption at rest using AES-256 encryption for all stored data
- Encryption in transit using TLS 1.3 or higher for all data transmissions
- Multi-factor authentication required for all administrative access
- Regular security audits conducted by independent third-party security firms

- SOC 2 Type I compliance with annual attestation updates (Type II in progress — see Section 1)
- ISO/IEC 42001:2023 AI-Management-System controls applied across the model lifecycle

(b) Access controls. 365Agents implements:

- Role-based access control with minimum-necessary permissions
- Regular access reviews and timely deprovisioning procedures
- Background checks for personnel with access to Customer Data
- Secure development practices, including code reviews and automated vulnerability scanning
- Annual security awareness training for all employees and contractors with system access

---

3. DATA BREACH RESPONSE PROCEDURES

(a) Incident detection and classification. 365Agents maintains 24×7 security monitoring to detect:

- Unauthorized access to Customer Data or systems
- Data exfiltration attempts or successful breaches
- System vulnerabilities that could compromise security
- Malware or ransomware incidents
- Insider threats or suspicious employee activity

(b) Immediate response (0–4 hours). Upon detecting a potential security incident:

- Incident response team activation within 1 hour of detection
- Preliminary assessment of scope and severity
- Containment measures to prevent further unauthorized access
- Evidence preservation for forensic analysis
- Initial documentation of incident timeline and affected systems

(c) Investigation phase (4–72 hours). Incident response includes:

- Forensic analysis to determine root cause and scope
- Assessment of data types and volume of information potentially compromised
- Identification of affected customers and data subjects
- Documentation of unauthorized access methods and duration
- Coordination with law enforcement if criminal activity is suspected

---

4. CUSTOMER NOTIFICATION PROCEDURES

(a) Notification timeline. 365Agents will notify affected Customers:

- **Without unreasonable delay and no later than 72 hours** after confirming a Personal Data breach (consistent with GDPR requirements)
- **Immediately**, by reasonable means available, if ongoing risk requires urgent customer action (target: within 24 hours of confirmation)
- As required by applicable law in Customer's jurisdiction

(b) Notification content. Breach notifications will include:

- Description of the incident, including date, time, and duration
- Types of data involved and estimated number of affected records
- Likely consequences of the breach for affected individuals
- Measures taken to address the breach and prevent recurrence
- Contact information for questions and additional details
- Recommendations for Customers to protect affected individuals

(c) Regulatory notifications. 365Agents will handle required notifications to:

- Data protection authorities within 72 hours when required
- Law enforcement agencies when criminal activity is involved
- Other regulatory bodies as required by applicable law
- Credit-monitoring services when financial data is involved

---

5. DATA RECOVERY AND BUSINESS CONTINUITY

(a) Backup and recovery. 365Agents maintains:

- Automated daily backups with geographically distributed storage
- Point-in-time recovery capabilities for database restoration
- Disaster recovery sites with maximum **4-hour Recovery Time Objective (RTO)** and **24-hour Recovery Point Objective (RPO)**
- Regular backup testing and restoration procedures
- Business continuity planning with defined escalation procedures

(b) Service restoration. Following a security incident:

- Secure service restoration only after confirming threat elimination

- Enhanced monitoring for related threats
- Security improvement implementation based on incident lessons learned
- Customer communication regarding service status and security enhancements

---

6. POST-INCIDENT PROCEDURES

(a) Incident analysis. After resolution, 365Agents conducts:

- Root cause analysis to identify failure points
- Security control assessment and enhancement recommendations
- Process improvement review for incident response procedures
- Documentation update for policies and procedures
- Staff training updates based on incident findings

(b) Ongoing monitoring. Enhanced security measures include:

- Increased monitoring of affected systems for 90 days
- Additional security controls implementation as appropriate
- Regular vulnerability assessments and penetration testing (annually at minimum)
- Third-party security reviews for affected components

---

7. COMPREHENSIVE GDPR COMPLIANCE

(a) Legal basis for processing. 365Agents processes Personal Data under the following legal bases:

- Contract performance for providing services requested by customers
- Legitimate interests for improving services and preventing fraud
- Consent where specifically obtained for marketing or optional features
- Legal obligations for compliance with applicable laws and regulations

(b) Data subject rights. Under GDPR, individuals have the right to:

- Access their Personal Data and obtain a copy
- Rectification of inaccurate or incomplete Personal Data
- Erasure (“right to be forgotten”) under specific circumstances
- Restriction of processing in certain situations
- Data portability in machine-readable format

- Object to processing based on legitimate interests
- Withdraw consent where processing is based on consent

(c) Data Protection Impact Assessments (DPIAs). 365Agents conducts DPIAs for:

- High-risk processing activities involving Personal Data
- New AI model training using customer voice data
- System changes that may affect data protection
- Cross-border data transfers to new jurisdictions

---

8. DATA RETENTION AND DELETION

(Renumbered in v1.1: was previously labeled "7" along with the CCPA section.)

(a) Retention periods by data type:

Data type	Retention
Voice recordings	Deleted within 30 days unless Customer requests longer retention via Order or admin setting
Voice models (synthetic voices)	Retained until Customer requests deletion or account termination
Usage logs and telemetry	12 months (for security, performance, and fraud monitoring)
Customer account data	Up to 7 years after account closure for legal and tax compliance
Billing and transaction records	7 years (as required by tax and financial regulations)
Customer Data (other than the above)	For the Subscription Term plus 30 days post-termination, then deleted; archive backups retained until expiry per backup rotation

(b) Automated deletion processes:

- Scheduled deletion jobs run daily to remove expired data
- Customer-initiated deletion processed within 30 days of verified request
- Backup purging on rotation to remove deleted data from all systems
- Verification procedures confirm complete data removal

---

9. RIGHTS UNDER CCPA AND SIMILAR LAWS

(Was previously labeled Section 7 alongside Data Retention. Renumbered to Section 8.)

(a) Consumer rights under CCPA. California residents have the right to:

- Know what Personal Information is collected and how it is used
- Delete Personal Information held by businesses
- Opt out of "sale" or "sharing" of Personal Information
- Non-discrimination for exercising CCPA rights
- Access specific pieces of Personal Information

(b) CCPA disclosures. 365Agents provides:

- Annual privacy policy updates with required CCPA disclosures
- A consumer request portal for exercising CCPA rights (https://365agents.com/privacy-requests)
- Verification procedures for identity confirmation
- Response timelines of 45 days, with possible 45-day extension as permitted

(c) State-law equivalents. 365Agents extends comparable rights to consumers in states with substantially similar privacy laws (including VCDPA, CPA, CTDPA, UCPA, and other applicable state laws), as required.

---

10. INTERNATIONAL DATA TRANSFER SAFEGUARDS

(Renumbered from Section 8 in v1.0.)

(a) Transfer mechanisms. For international data transfers, 365Agents uses:

- Standard Contractual Clauses approved by the European Commission
- Adequacy decisions where available for specific countries
- Binding Corporate Rules for intra-group transfers
- Certification schemes where recognized by data protection authorities

(b) Country-specific restrictions. Data transfers are restricted or prohibited to:

- Countries under sanctions by the U.S., EU, or other applicable jurisdictions
- Jurisdictions without adequate protection unless appropriate safeguards are in place
- High-risk countries identified by 365Agents' security assessments

---

11. UPDATES TO THIS POLICY

365Agents may update this Policy from time to time and will post the current version at https://365agents.com/legal/infosec. 365Agents will not materially diminish the protections set forth in this Policy as of a Customer's Effective Date during the then-current Subscription Term.

Document version: 1.1 · **Effective date:** [insert]
Owner: Information Security Officer, 365Agents, Inc.
Contact: security@365agents.com