Annex 4 - Security Measures

As from the Addendum Effective Date, Decagon will implement and maintain the Security Measures as set out in this Annex.

Technical and Organizational Security Measure	Details
Measures for compliance attestations, third-party audits, and certifications	Decagon undergoes annual SOC 2 Type II audits covering the Security and Confidentiality Trust Service Criteria, and maintains ISO 27001 certification. These reports and certificates are available to Customers upon request or via Decagon's trust portal. Decagon engages independent third parties to perform annual penetration testing of production systems and quarterly vulnerability scans of external-facing systems; executive summaries or attestation letters from the most recent penetration test are available to Customers upon request, subject to execution of a mutual non-disclosure agreement. For subprocessors and critical third-party vendors, Decagon reviews attestation reports (such as SOC 2 Type II and ISO 27001) and conducts security assessments at least annually to verify appropriate controls are maintained. Decagon supports Customer audit rights as set forth in the DPA, including through provision of the reports and summaries described in this Annex.
Measures of pseudonymisation and encryption of personal data	Decagon encrypts customer data at rest using AES-256 encryption and secures data in transit using TLS 1.2 or higher with strong cipher suites. We manage encryption keys in accordance with NIST SP 800-57 standards with controlled access and regular key rotation. We implement data minimization practices through our Privacy Compliance and Data Management Policy, retaining PII only for as long as there is a legitimate business purpose, and restrict access to personal data on a need-to-know basis using role-based access controls. PII redaction services in the product provide a flexible, customer-managed capability for pseudonymization of user-provided content.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Decagon implements comprehensive measures to ensure the ongoing protection and resilience of systems processing Customer Personal Data. To maintain confidentiality, our customer agreements contain strict confidentiality obligations, and Decagon requires every downstream Subprocessor to sign confidentiality provisions that are substantially similar to those contained in Decagon’s customer agreements. Decagon maintains independent third-party compliance attestations covering the security program, as described under Compliance Attestations in this Annex. Decagon maintains infrastructure monitoring tools that continuously monitor system performance and generate automated alerts when predefined thresholds are met, enabling rapid response to potential issues. To ensure resilience and business continuity, Decagon maintains a documented Business Continuity and Disaster Recovery plan that is tested at least annually and includes procedures for rapid recovery from business disruptions. Decagon also maintains an Incident Response Plan that is tested at least annually to guide response to security incidents and maintains cybersecurity insurance to mitigate the financial impact of business disruptions.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Decagon performs daily automated backups of production systems and databases, storing them separately from production with encryption. We conduct at least annual backup restore testing to validate recovery procedures. Decagon maintains documented Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for production systems processing Customer Personal Data, which are available to Customers upon request. We log data restoration activities involving PII and maintain a Business Continuity Plan with alternate locations and vendor contingency procedures.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Decagon performs vulnerability scanning on both internal and external-facing systems. Cloud infrastructure is continuously monitored for misconfigurations, known CVEs, and compliance violations via cloud security posture management tools. Static application security testing (SAST) runs automatically on every code change, with full codebase scans performed regularly. Dependency vulnerabilities are continuously monitored across repositories. External attack surface scanning is performed on at least a weekly basis. Decagon performs annual third-party penetration testing and annual network security assessments. Our Incident Response Plan undergoes annual review and testing through tabletop exercises. We conduct automated testing on system changes and implement continuous monitoring capabilities for quality assurance. Personnel receive annual security training, and quarterly access rights reviews verify appropriate permissions across systems. Identified vulnerabilities are tracked in a ticketing system, assigned to system owners, and remediated according to documented, risk-based timelines that are maintained separately and available to Customers upon request or via Decagon's trust portal.
Measures for user identification and authorization	Decagon implements role-based access control (RBAC) following the principle of least privilege, ensuring users receive only the access necessary for their job functions. Users are assigned unique identifiers, and access provisioning requires documented approval from system owners or authorized management. Decagon uses secure authentication protocols and processes and follows industry best practices for authentication, including Multi-factor Authentication and Single Sign-On (SSO). Production access requires the use of two-factor authentication, and network infrastructure is securely configured to vendor and industry best practices to block unnecessary ports, services, and unauthorized network traffic. Access rights are reviewed quarterly to verify appropriate permissions, and access is promptly revoked upon termination or role change. Privileged access to production systems requires additional management authorization and multi-factor authentication. Personnel with privileged access use separate accounts for non-privileged activities, and privileged access roles are segregated to prevent concentration of sensitive capabilities. Privileged access is reviewed at least quarterly.
Measures for the protection of data during transmission	Decagon requires TLS 1.2 or higher for data transmission over public networks, using only approved cipher suites consistent with industry best practices. Remote connections to production systems must be encrypted, and Decagon requires encrypted connections for remote access to production systems and confidential data. Multi-factor authentication secures remote access, and we review production network access rules annually. Firewalls and network access controls restrict traffic to and from the production environment. Decagon deploys intrusion detection and prevention capabilities and web application firewall

	(WAF) controls to protect production systems and applications from network-based threats.
Measures for the protection of data during storage	Decagon encrypts Customer Personal Data at rest using AES-256 encryption via the cloud infrastructure provider's managed database services. Encryption keys are managed in accordance with NIST SP 800-57 standards with access restricted to authorized personnel and regular key rotation. Employee endpoints (laptops and workstations) that may access or store Customer Personal Data are encrypted. Decagon's policy prohibits the storage of confidential data on removable media. Backups of production data are encrypted. Decagon's platform architecture enforces logical tenant isolation, ensuring that each Customer's data is segregated from that of other customers through application-level access controls, separate data partitions, and enforced tenant boundaries. No customer can access, query, or inadvertently receive another customer's data. Decagon deploys Data Loss Prevention (DLP) controls to detect and prevent unauthorized disclosure of Customer Personal Data, including monitoring of data egress across cloud environments, endpoints, email, and network boundaries.
Measures for ensuring events logging	Decagon configures systems to produce detailed logs recording user activities, security events, exceptions, system faults, and privileged administrator actions on systems containing Customer Personal Data. These logs are collected and analyzed using centralized log management tools with automated alerts for potential security threats. System clocks are synchronized to network time servers to ensure accurate timestamps across systems. Log information is protected from tampering and unauthorized access, with access restricted to authorized security and engineering personnel only. The security and engineering teams monitor, review, and investigate security events detected in logs, escalating findings according to Decagon's Incident Response procedures and security policies. Security and audit logs are retained for a minimum of twelve (12) months in a tamper-resistant, centralized log management system. Logs relevant to an active security investigation or legal matter are preserved for the duration of the investigation or as required by applicable law. Log retention periods are reviewed at least annually as part of Decagon's Data Management Policy review process.
Measures for ensuring system configuration, including default configuration	Decagon adheres to a change management process to administer changes to the production environment for the Services, including changes to its underlying software, applications, and systems. Production changes are automated through CI/CD tools where possible to ensure consistent configurations across the environment. Systems are provisioned and configured according to documented hardening standards based on industry best practices, which are reviewed at least annually. Default accounts are removed or disabled before deployment to production. In limited cases where a default account cannot be removed due to vendor requirements, compensating controls are applied, including renaming the account, restricting its access to the minimum necessary, and monitoring it for anomalous activity. Vendor default credentials are changed on systems before they are connected to the production network. Configuration changes are tested in non-production environments before deployment to production, and production network access configuration rules are reviewed annually to ensure appropriate security controls remain in place. Changes to the production environment are recorded in an auditable log that includes the change description, authorization, testing performed, and rollback procedures.

Measures for secure software development	Decagon follows a Secure Development Lifecycle (SDLC) in accordance with its Secure Development Policy. Developers receive training on secure coding practices. Code changes undergo peer review before merging. Decagon employs static application security testing (SAST) and dependency vulnerability scanning integrated into the CI/CD pipeline. Dynamic application security testing (DAST) is performed as part of regular security assessments. Third-party libraries and dependencies are monitored for known vulnerabilities using automated scanning tools, and vulnerable dependencies are remediated in accordance with Decagon's vulnerability management timelines. Decagon conducts annual third-party penetration testing of production systems and applications. Development, staging, and production environments are logically separated, and Customer Personal Data is not used in non-production environments. Developer access to production environments is restricted and controlled through documented approval processes; production deployments are performed through automated CI/CD pipelines.
Measures for the security of AI and machine learning processing	Decagon implements dedicated security controls for AI and machine learning components used in the delivery of Services. Decagon enforces prompt injection defenses, including a supervisor model that detects adversarial inputs, as well as automated monitoring for hallucination and bad actor behavior. Decagon maintains an AI System Governance Policy overseen by designated engineering leadership, which governs the full lifecycle of AI systems including approval, development, testing (including bias validation, adversarial testing, and security testing), monitoring, and termination. Customer data is never used to train or fine-tune any AI models. Decagon performs annual risk assessments of AI services and monitors for model drift, performance degradation, and emerging threats on an ongoing basis.
Measures for security incident notification	In the event Decagon becomes aware of a Personal Data Breach affecting Customer Personal Data, Decagon will notify the Customer without undue delay and in any event within forty-eight (48) hours of confirmation. The notification will include, to the extent reasonably available: the nature of the breach, the categories and approximate number of data subjects affected, the likely consequences, and the measures taken or proposed to mitigate the breach. Decagon will provide ongoing updates as material new information becomes available during the investigation. Decagon maintains a documented Incident Response Plan, tested at least annually through tabletop exercises, with defined severity levels (P1 through P4) and escalation procedures.
Measures for cross-border data transfers and data residency	When Customer Personal Data is transferred outside the European Economic Area (EEA), Decagon relies on the European Commission's Standard Contractual Clauses (Commission Implementing Decision 2021/914), using Module 2 (Controller to Processor) for customer relationships and Module 3 (Processor to Subprocessor) for downstream vendor relationships. Decagon maintains a Transfer Impact Assessment (TIA) that evaluates the legal environment of recipient countries, the effectiveness of supplementary measures, and residual risk, and reviews the TIA at least annually or upon material changes to applicable law. Supplementary technical measures include end-to-end encryption (TLS 1.2+ in transit, AES-256 at rest), prompt pseudonymization of user-generated content before processing outside the EEA where configured by the Customer, logical segmentation of EU and US environments, and regional access restrictions. Upon request, Decagon offers EU-only data residency, in which Customer Personal Data is processed and stored within EEA-located infrastructure. Decagon maintains a

	current list of subprocessors, including their locations and processing activities, which is available to Customers via Decagon's trust portal.
Measures for internal IT and IT security governance and management	Decagon's security program encompasses change management procedures, vendor risk management, asset inventory management, and incident response capabilities. Personnel receive annual security awareness training covering their data protection responsibilities. Security governance, policy review, risk assessments, and compliance attestations are described under the Security Oversight and Governance and Compliance Attestations sections of this Annex.
Measures for personnel security	Decagon personnel undergo background checks prior to commencing employment, in accordance with applicable law and commensurate with the sensitivity of data they will access. Personnel with access to Customer Personal Data are bound by written confidentiality obligations that survive termination of employment. Security responsibilities are defined in employment contracts, and personnel are required to acknowledge and comply with Decagon's information security policies upon hire and annually thereafter. Contractors and third-party personnel with access to production systems or Customer Personal Data are subject to security requirements no less protective than those applied to Decagon employees, including background verification, confidentiality agreements, and mandatory security awareness training.
Measures for physical and device security	Decagon's primary production infrastructure is hosted on Google Cloud Platform (GCP), which maintains SOC 2 Type II, ISO 27001, ISO 27017, and ISO 27018 certifications covering physical and environmental security controls for its data centers, including biometric access controls, 24/7 surveillance, environmental protections, and visitor management. Decagon does not operate its own data centers. Decagon enforces endpoint encryption on employee devices, deploys Mobile Device Management (MDM), Endpoint Detection and Response (EDR), and anti-malware solutions across employee endpoints, with malware signatures updated at least daily. Decagon scans inbound email attachments for malware and malicious content. Decagon requires multi-factor authentication for remote access to production systems, and maintains policies prohibiting the storage of Customer Personal Data on local devices or removable media. Decagon implements industry standard physical security controls, including access control, cameras, and guest check-in at Decagon offices. Decagon's Physical Security Policy is reviewed at least annually.
Measures for ensuring data minimization	Decagon collects and retains Customer Personal Data only for as long as there is a legitimate business purpose in accordance with documented data retention requirements. Personally identifiable information (PII) is deleted or de-identified as soon as it no longer serves a legitimate business purpose. Access to Customer Personal Data is restricted on a need-to-know basis using role-based access controls following the principle of least privilege. Where configured by the Customer, Decagon applies prompt pseudonymization of user-generated content following conversation completion, in accordance with Decagon's configured redaction schedules. Data collected for specific purposes, such as responding to data subject requests, is used only for that stated purpose and deleted after the request is fulfilled. Decagon reviews data retention requirements at least annually as part of the Data Management Policy review process.

Measures for ensuring data quality	Decagon implements multiple controls throughout the development lifecycle to ensure data quality. Data integrity is protected through encryption at rest and in transit, with access controls restricting data modification to authorized personnel. We require formal change management with documented approval before production deployment. Our automated testing framework validates system behavior when changes are deployed. Continuous monitoring validates that systems operate within expected parameters, and we log system activities for review and audit. Backup and restore capabilities are tested at least annually to validate data integrity and recoverability. These measures ensure the accuracy, completeness, and integrity of Customer Personal Data throughout its lifecycle. Customers can request correction of inaccurate personal data through data subject access request procedures in accordance with applicable data protection laws and contractual obligations.
Measures for ensuring limited data retention	Customers unilaterally determine what data they route through the Services. As such, Decagon operates on a shared responsibility model. During active service, where configured by the Customer, Decagon implements prompt pseudonymization of user-generated content following conversation completion. Personally identifiable information is deleted or de-identified as soon as it no longer serves a legitimate business purpose, in accordance with documented data retention requirements that are reviewed at least annually. Decagon will delete Customer Personal Data upon the Customer's written request, within the timeframe specified in this DPA and in accordance with Applicable Privacy Laws. Following service termination, Customer Personal Data is deleted in accordance with the timeframes and procedures set forth in the DPA. Deletion is performed using methods consistent with NIST SP 800-88 guidelines, rendering Customer Personal Data unrecoverable. For cloud-hosted infrastructure, Decagon relies on the cryptographic erasure and media sanitization controls provided by the cloud infrastructure provider, which are validated through the provider's independent compliance certifications.
Measures for ensuring accountability	Decagon has adopted comprehensive measures for ensuring accountability. Roles and responsibilities for information security and data privacy functions are formally assigned, with personnel receiving annual security awareness training on their data protection responsibilities. Decagon implements data protection and information security policies across the business that are reviewed at least annually. Personal Data Breaches are recorded and reported through documented incident response procedures. Decagon executes Data Processing Agreements with customers and subprocessors that document data protection obligations and accountability requirements. To verify compliance, Decagon conducts independent third-party audits and maintains audit logs of system activities to provide traceable records of data processing and security events. Details of compliance attestations and audit programs are described under Compliance Attestations in this Annex.
Measures for allowing data portability and ensuring erasure	Customer Personal Data submitted to the Services by Customer may be deleted or retrieved by the Customer using Decagon's publicly accessible APIs at the Customer's discretion. Decagon implements data minimization and privacy-by-design principles to limit collection and processing of Customer Personal Data. Customers can submit deletion requests through our documented data subject request process, which we handle within required timeframes per our Privacy Compliance Policy. We respond to consumer rights requests including access, rectification, deletion, and data portability in accordance with GDPR, CCPA/CPRA,

	and other applicable privacy regulations. Deletions are performed using methods that render Customer Personal Data unrecoverable, consistent with NIST SP 800-88 guidelines.
Technical and organizational measures of subprocessors	Decagon maintains a vendor management program that includes inventory, security and privacy requirements, and annual reviews of subprocessors. Prior to engaging any subprocessor, Decagon performs a risk assessment and executes written agreements that include confidentiality provisions and data protection obligations no less protective than those in Decagon's customer agreements. Decagon provides Customers with advance notification of new subprocessors in accordance with the DPA, including the opportunity to object. Subprocessors handling Customer Personal Data are required to maintain appropriate technical and organizational security measures. Decagon reviews attestation reports (such as SOC 2 Type II and ISO 27001) and conducts security assessments of subprocessors and high-risk vendors at least annually to verify they maintain appropriate technical and organizational measures.
Measures for security oversight and governance	Decagon maintains a formal information security governance framework with designated executive ownership, including the Chief Technology Officer (CTO) and dedicated security leadership. The Board of Directors is briefed at least annually on cybersecurity and privacy risks. Information security policies are reviewed at least annually and communicated to personnel. Personnel receive annual security awareness training covering data protection, incident reporting, social engineering awareness, and responsible use of AI systems. Decagon performs formal risk assessments at least annually, or upon material changes to the threat landscape, business operations, or regulatory requirements. Control self-assessments and ongoing monitoring activities verify the effectiveness of security controls between formal review cycles.

Decagon may update the Security Measures from time to time in accordance with Section 4 (**Security**) of the DPA and/or Section 2.3 (**Security Measures**) of the Agreement.