Control-C Data Processing Addendum

Last updated: March 20, 2025

1. Scope and Incorporation

This Data Processing Addendum ("DPA") forms part of the Terms & Conditions (./terms-and-conditions) or other written agreement between Control-C ("Processor") and the customer entering into that agreement ("Controller"). It applies to the extent Control-C processes Personal Data on behalf of Controller in providing the Service.

2. Roles and Responsibilities

Controller determines the purposes and means of processing Personal Data. Control-C will process Personal Data solely on documented instructions from Controller, which are set forth in the underlying agreement, this DPA, and Customer's administrative actions via the Service. Control-C will promptly notify Controller if an instruction violates applicable data protection laws.

3. Subject Matter and Duration

The subject matter, nature, and purpose of processing involve providing continuity orchestration, analytics, and related services. Categories of data subjects and Personal Data are described in Attachment A to this DPA. Processing continues for the subscription term and any transition period where Controller exports or deletes Personal Data.

4. Confidentiality

Control-C ensures that personnel authorized to process Personal Data are bound by confidentiality obligations and receive appropriate privacy and security training. Access is limited to personnel who require it to deliver the Service.

5. Security Measures

Control-C implements technical and organizational measures described in Attachment B and summarized in the Trust Center (/trust-center). Measures include encryption in transit and at rest, access controls, security logging, vulnerability management, incident response, and regular penetration testing by independent assessors.

6. Subprocessors

Controller authorizes Control-C to engage subprocessors listed in the Subprocessor Registry (./subprocessors). Control-C will impose data protection obligations on subprocessors equivalent to this DPA. Controller will receive notice of new subprocessors via email or the registry and may object within fifteen (15) days for reasonable, documented grounds. If Control-C cannot accommodate an objection, Controller may terminate the impacted services with a pro-rata refund.

7. Data Subject Rights

Taking into account the nature of processing, Control-C will assist Controller by appropriate technical and organizational measures, insofar as possible, to fulfill Controller's obligations to respond to data subject requests under applicable law. Assistance includes providing tooling for export, access, correction, deletion, and restriction of Personal Data processed within the Service.

8. Incident Notification

Upon becoming aware of a Personal Data Breach, Control-C will notify Controller without undue delay and provide information necessary for Controller to meet breach reporting obligations. Control-C will promptly investigate, mitigate, and document the incident, and cooperate with Controller and supervisory authorities as required.

9. Audits and Assessments

Control-C maintains independent security and compliance audits, including SMB1001 Cyber Security Framework certification at the Silver maturity level. Crosswalks to Essential Eight, UK Cyber Essentials, ISO 27001, CMMC, and Right Fit for Risk are available for customer due diligence. Control-C will provide summary reports and responses to reasonable security questionnaires. Controller may, at its expense, conduct an on-site audit no more than once per year with thirty (30) days' written notice, subject to reasonable scheduling and confidentiality restrictions. Remote assessments leveraging third-party attestations are preferred.

10. International Transfers

When transferring Personal Data from the European Economic Area, United Kingdom, or Switzerland to a country lacking an adequacy decision, the parties agree that the EU Standard Contractual Clauses (controller-to-processor) and the UK International Data Transfer Addendum apply by reference. Control-C will not transfer Personal Data to a jurisdiction subject to government access requests that conflict with Controller's documented instructions without safeguards described in Attachment C.

11. Return or Deletion

Upon termination or expiration of the Service, Controller may export Personal Data via available tooling. Control-C will delete or anonymize Personal Data within ninety (90) days of termination unless retention is required by law. Certifications of deletion are available upon written request.

12. Liability and Conflict

Liability arising out of this DPA is governed by the limitation and exclusion provisions in the underlying agreement. If there is a conflict between this DPA and other agreement terms, this DPA prevails with respect to data protection obligations.

13. Governing Law

This DPA is governed by the laws identified in the underlying agreement, unless otherwise required by applicable data protection laws.

Attachment A – Data Processing Details

- **Data subjects**: Customer employees, contractors, partners, clients, and other individuals whose information is entered into the Service.
- **Personal Data**: Identification data (name, email, phone), role-based access data, business continuity plan content, audit logs, incident metadata, device identifiers, and optional integrations (e.g., ticketing, HR systems). Controller may configure custom fields, which remain Controller's responsibility.
- **Special categories**: Control-C does not require special category data. Controller is responsible for ensuring such data is not uploaded unless expressly agreed in writing.

Attachment B – Security Measures

- **Governance**: Security policies reviewed annually, risk management program, dedicated security and privacy teams.
- **Access Controls**: Single sign-on, multi-factor authentication, role-based access, least privilege, quarterly access reviews.
- **Encryption**: TLS 1.2+ for data in transit, AES-256 or better for data at rest, managed key services.
- **Monitoring**: Centralized logging, intrusion detection, anomaly detection, and 24/7 security operations monitoring.
- **Resilience**: Redundant infrastructure across multiple availability zones, tested disaster recovery plans, quarterly backup restores.
- **Development**: Secure SDLC, code reviews, dependency scanning, and annual third-party penetration tests.

Attachment C – Transfer Impact Safeguards

- Evaluate government access requests under applicable legal standards and challenge unlawful or disproportionate requests.
- Notify Controller, where legally permitted, before disclosing Personal Data to law enforcement.
- Maintain transparency reporting in the Trust Center (/trust-center).