C2 All-in-One HRIS Platform

Data Processing Agreement

Between the Controller (Customer) and Agile Futurist (Processor)

Version	1.4
Effective Date	As of the date the Customer accepts the C2 Terms of Service or executes this Agreement, whichever is earlier.
Processor	Agile Futurist, a sole proprietorship registered under the laws of the Netherlands, with registered address at De Nieuwe Erven 3, Unit 14784, 5431 NV Cuijk, The Netherlands (trading as C2 All-in-One HRIS Platform at cognitis.cloud)
Controller	The Customer entity identified in the associated C2 Subscription Agreement or Order Form.
Governing Law	Laws of the Netherlands (Dutch law), subject to mandatory local data protection law where the Controller is established.

IMPORTANT LEGAL NOTICE: This Data Processing Agreement is provided as a standard template by Agile Futurist in accordance with Article 28 of Regulation (EU) 2016/679 (GDPR). It should be reviewed by the Customer's legal counsel or Data Protection Officer before execution. Agile Futurist recommends all Customers maintain their own legal review process. This document does not constitute legal advice.

Recitals

This Data Processing Agreement ("Agreement" or "DPA") is entered into between the Controller and Agile Futurist, a sole proprietorship registered under the laws of the Netherlands with its registered address at De Nieuwe Erven 3, Unit 14784, 5431 NV Cuijk, The Netherlands, trading as C2 All-in-One HRIS Platform ("the Processor"), and forms part of, and is incorporated into, the C2 Subscription Agreement or Terms of Service (the "Principal Agreement") between the Parties.

WHEREAS:

(A) The Processor provides the C2 All-in-One HRIS Platform, a cloud-based human resources information system, to the Controller pursuant to the Principal Agreement.

(B) In providing the Platform, the Processor will process Personal Data on behalf of the Controller, who acts as the Data Controller in respect of such Personal Data.

(C) Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR") requires that Processing by a Processor shall be governed by a binding contract setting out the subject matter, duration, nature, and purpose of the Processing, the type of Personal Data and categories of Data Subjects, and the obligations and rights of the Controller.

(D) The Parties wish to record their agreement on the terms governing such Processing in this DPA.

NOW THEREFORE, the Parties agree as follows:

Clause 1: Definitions

In this Agreement, the following terms shall have the meanings set out below. Capitalised terms not defined herein shall have the meanings given to them in the Principal Agreement or, where applicable, in the GDPR.

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this Agreement, the Customer.

"Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

"Data Protection Laws" means all applicable laws and regulations relating to the processing of Personal Data and privacy, including without limitation: (i) the GDPR; (ii) national implementing legislation in the Member State(s) where the Controller is established; (iii) the EU ePrivacy Directive (2002/58/EC) and any implementing or successor legislation; and (iv) any guidance, codes of practice, or binding decisions issued by a competent Supervisory Authority.

"Data Subject" means an identified or identifiable natural person whose Personal Data is processed by the Processor under this Agreement.

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

"Personal Data" means any information relating to an identified or identifiable natural person as defined in Article 4(1) GDPR.

"Platform" means the C2 All-in-One HRIS software-as-a-service platform operated by the Processor at cognitis.cloud, as described in the Principal Agreement.

"Principal Agreement" means the Subscription Agreement, Terms of Service, Order Form, or equivalent master agreement governing the Controller's use of the Platform.

"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination, restriction, erasure, or destruction.

"Processor" means Agile Futurist, a sole proprietorship registered under the laws of the Netherlands, with registered address at De Nieuwe Erven 3, Unit 14784, 5431 NV Cuijk, The Netherlands, trading as C2 All-in-One HRIS Platform, which processes Personal Data on behalf of the Controller pursuant to this Agreement.

"Restricted Transfer" means a transfer of Personal Data to a third country or international organisation outside the European Economic Area (EEA) that is not subject to an adequacy decision under Article 45 GDPR.

"Special Category Data" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, as defined in Article 9 GDPR.

"Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679, as adopted by the European Commission Decision of 4 June 2021 (Commission Implementing Decision (EU) 2021/914), as may be updated or replaced from time to time.

"Sub-processor" means any third party appointed by or on behalf of the Processor to process Personal Data on behalf of the Controller.

"Supervisory Authority" means the independent public authority responsible for monitoring the application of the GDPR, as referred to in Article 51 GDPR.

Clause 2: Subject Matter, Nature, Purpose and Duration

2.1 Subject matter. The Processor shall process Personal Data on behalf of the Controller for the purpose of providing the Platform and related support services pursuant to the Principal Agreement.

2.2 Nature of processing. The processing activities to be carried out by the Processor on behalf of the Controller are described in Schedule 1 (Details of Processing) to this Agreement.

2.3 Purpose. The Processor shall process Personal Data solely for the purpose of delivering the Platform functionality subscribed to by the Controller, including: hosting and storing employee, candidate, and user data entered by the Controller; providing access to Platform features (recruitment, onboarding, leave management, performance management, learning management, reporting, and AI-assisted HR functions); and providing technical support, maintenance, and security operations in relation to the Platform.

2.4 Duration. This Agreement shall remain in force for as long as the Processor processes Personal Data on behalf of the Controller under the Principal Agreement. Upon termination or expiry of the Principal Agreement, the provisions of Clause 9 (Return and Deletion of Personal Data) shall apply.

Clause 3: Obligations of the Processor

The Processor shall, in relation to any Personal Data processed in connection with the performance of its obligations under this Agreement:

3.1 Instructions. Process the Personal Data only on the documented instructions of the Controller, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The Controller's instructions are set out in this Agreement and the Principal Agreement. The Controller may issue further documented

instructions during the term of this Agreement, and the Processor shall comply with such instructions to the extent technically feasible and commercially reasonable.

3.2 Confidentiality. Ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that access to Personal Data is restricted to those personnel who require such access for the purposes of performing the Principal Agreement.

3.3 Security. Implement and maintain the technical and organisational security measures described in Schedule 2 (Technical and Organisational Measures) to this Agreement, in accordance with Article 32 GDPR, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

3.4 Processor's obligation to notify of conflicting instructions. Notify the Controller promptly if, in the Processor's reasonable opinion, an instruction given by the Controller infringes Data Protection Laws. In such circumstances, the Processor shall be entitled to refuse to carry out the instruction pending resolution.

3.5 Assistance with Data Subject Rights. Taking into account the nature of the Processing, assist the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, in fulfilling the Controller's obligation to respond to requests from Data Subjects exercising their rights under Chapter III of the GDPR (including rights of access, rectification, erasure, restriction, portability, and objection). The Processor shall promptly forward any Data Subject request received directly to the Controller and shall not respond to any such request on the Controller's behalf except as expressly instructed by the Controller.

3.6 Assistance with Controller's obligations. Assist the Controller in ensuring compliance with its obligations under Articles 32 to 36 GDPR (security, breach notification, DPIAs, and prior consultation), taking into account the nature of the Processing and the information available to the Processor. Such assistance may include: (a) providing the Controller with information about the security measures described in Schedule 2; (b) notifying the Controller of Data Breaches as set out in Clause 8; (c) providing reasonable assistance in the completion of Data Protection Impact Assessments where required under Article 35 GDPR.

3.7 EU Data Residency. The Processor shall store and process all Personal Data exclusively within the European Economic Area (EEA), unless the Controller has given prior written consent to processing outside the EEA and appropriate safeguards are in place as described in Clause 7 (International Transfers).

3.8 Records. Maintain all records required under Article 30(2) GDPR in relation to processing activities carried out on behalf of the Controller, and make such records available to the Controller or a relevant Supervisory Authority on request.

Clause 4: Obligations of the Controller

4.1 Lawful basis. The Controller shall ensure that it has a valid lawful basis for processing Personal Data under Data Protection Laws, and that it has provided Data Subjects with all required information (including privacy notices) before or at the time Personal Data is collected and uploaded to the Platform.

4.2 Accuracy and minimisation. The Controller is responsible for the accuracy, completeness, and appropriateness of the Personal Data it uploads to the Platform and for ensuring that Personal Data is not excessive or unnecessary for the purposes for which it is processed.

4.3 Instructions. The Controller shall ensure that its instructions to the Processor are lawful and comply with Data Protection Laws. The Controller acknowledges that the Processor's ability to deliver the Platform is dependent on receiving lawful and technically feasible instructions.

4.4 Special Category Data. The Controller is responsible for having a valid legal basis under Article 9 GDPR for any Special Category Data it processes through the Platform, such as health data in sickness absence records. The Processor may impose reasonable additional security requirements in respect of Special Category Data.

4.5 Access management. The Controller is responsible for managing user access credentials, roles, and permissions within the Platform, and for ensuring that access is granted only to authorised personnel.

Clause 5: Sub-processors

5.1 General authorisation. The Controller hereby grants the Processor a general written authorisation to engage the Sub-processors listed in Schedule 3 (Sub-processor Register) for the purposes of providing the Platform. The Processor shall update Schedule 3 as Sub-processors are added or replaced.

5.2 Notification of changes. The Processor shall notify the Controller of any intended addition or replacement of Sub-processors by updating the Sub-processor Register published at cognitis.cloud/trust-center/#tc-subprocessors and providing at least thirty (30) calendar days' advance notice by email to the Controller's registered email address or via in-platform notification.

5.3 Controller's right to object. The Controller may object to the addition or replacement of a Sub-processor within ten (10) calendar days of receiving notification under Clause 5.2, by sending written notice to dpo@agilefuturist.com stating the reasonable grounds for objection. The Parties shall discuss such objection in good faith. If the Parties are unable to resolve the objection within thirty (30) days, either Party may terminate the Principal Agreement on sixty (60) days' written notice without liability for termination fees in respect of affected services.

5.4 Sub-processor obligations. The Processor shall impose on each Sub-processor, by way of written contract, data protection obligations equivalent to those set out in this Agreement, including the obligation to implement appropriate technical and organisational security measures. The Processor shall remain fully liable to the Controller for the performance of any Sub-processor's obligations to the extent the Sub-processor fails to fulfil its data protection obligations.

5.5 EU data residency for Sub-processors. The Processor shall ensure that any Sub-processor it engages processes Personal Data exclusively within the EEA, unless the requirements of Clause 7 are satisfied in respect of the relevant Sub-processor.

Clause 6: Audit Rights and Inspections

6.1 Information and audit. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller.

6.2 Notice and scope. The Controller shall provide the Processor with at least thirty (30) days' prior written notice of any audit or inspection, except where a Supervisory Authority requires the audit to be conducted on shorter notice. Audits shall be conducted during normal business hours, shall not unreasonably disrupt the Processor's operations, and shall be limited in scope to the Processor's processing of Personal Data under this Agreement.

6.3 Frequency. Unless required by a Supervisory Authority, the Controller may conduct no more than one (1) audit per calendar year at its own expense. Additional audits may be conducted where there are reasonable grounds to believe a Data Breach has occurred or the Processor has breached this Agreement.

6.4 Certification as substitute. The Processor may satisfy its obligations under Clause 6.1 in whole or in part by providing the Controller with up-to-date copies of relevant third-party certifications (including ISO 27001, ISO 27701, penetration test reports, SOC 2 reports, or equivalent), subject to appropriate confidentiality undertakings. The Controller may nonetheless request a direct audit if not satisfied with the documentary evidence provided.

6.5 Audit costs. The Controller shall bear all costs of any audit, including the Processor's reasonable out-of-pocket costs of facilitating the audit. Where an audit reveals a material breach by the Processor of this Agreement, the Processor shall bear the reasonable costs of the audit.

Clause 7: International Transfers

7.1 EEA processing. The Processor shall by default process all Personal Data within the EEA. The Processor's primary hosting infrastructure is located in the European Union, as specified in Schedule 1.

7.2 Transfers outside the EEA. Where Personal Data is transferred outside the EEA in connection with the use of a Sub-processor or for other operational reasons, the Processor shall ensure that an appropriate transfer mechanism is in place in accordance with Chapter V GDPR. Such mechanisms may include: (a) an adequacy decision under Article 45 GDPR in respect of the destination country; (b) appropriate safeguards under Article 46 GDPR, including Standard Contractual Clauses (Module 2: Controller to Processor, or Module 3: Processor to Processor as applicable); or (c) binding corporate rules approved under Article 47 GDPR.

7.3 SCCs. Where SCCs are used to legitimise a Restricted Transfer, they are hereby incorporated into this Agreement by reference. In the event of any conflict between the body of this Agreement and the SCCs, the SCCs shall prevail in respect of the Restricted Transfer to which they apply. The relevant module, clauses, and options selected shall be as specified in the applicable Sub-processor entry in Schedule 3.

7.4 Transfer impact assessments. Where required by applicable Data Protection Laws or Supervisory Authority guidance, the Processor shall cooperate with the Controller in conducting a transfer impact assessment (TIA) in relation to any Restricted Transfer made under this Agreement.

Clause 8: Personal Data Breach Notification

8.1 Processor notification obligation. The Processor shall notify the Controller without undue delay, and in any event within twenty-four (24) hours of becoming aware of a Data Breach affecting Personal Data processed under this Agreement, so that the Controller can meet its own obligations under Articles 33 and 34 GDPR. Notification shall be sent to the email address designated by the Controller in Schedule 1 or, where no such address is designated, to the Controller's primary account email address.

8.2 Content of notification. The initial notification shall include, to the extent then known: (a) a description of the nature of the Data Breach, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (b) the name and contact details of the Processor's data protection contact; (c) a description of the likely consequences of the Data Breach; and (d) a description of the measures taken or proposed to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

8.3 Staged notification. Where it is not possible to provide all information referred to in Clause 8.2 at the time of initial notification, the information may be provided in phases as it becomes available, without undue further delay.

8.4 Controller's notification obligations. The Controller is responsible for assessing whether the Data Breach requires notification to the relevant Supervisory Authority under Article 33 GDPR and/or to affected Data Subjects under Article 34 GDPR. The Processor shall provide reasonable assistance to the Controller in making such assessment and in preparing any required notifications.

8.5 Mitigation. The Processor shall take reasonable steps to contain and mitigate the Data Breach and shall keep the Controller informed of progress. The Processor shall cooperate fully with the Controller and any relevant Supervisory Authority in the investigation and remediation of the Data Breach.

8.6 Record keeping. The Processor shall maintain an internal record of all Data Breaches, including those not notified to the Controller or a Supervisory Authority, in accordance with Article 33(5) GDPR, and shall make this record available to the Controller and any relevant Supervisory Authority on request.

Clause 9: Return and Deletion of Personal Data

9.1 Upon termination. Upon the expiry or termination of the Principal Agreement, the Processor shall, at the choice of the Controller and as notified in writing: (a) return all Personal Data to the Controller in a machine-readable format (CSV or JSON) within ninety (90) days of termination; or (b) securely delete or destroy all Personal Data and existing copies thereof within ninety (90) days of termination, unless Union or Member State law requires storage of the Personal Data.

9.2 Confirmation. Following completion of the return or deletion described in Clause 9.1, the Processor shall provide the Controller with written confirmation that all Personal Data has been returned or deleted, specifying the deletion method used and the date of completion.

9.3 Backup systems. The Processor shall ensure that Personal Data is deleted from all backup systems within a commercially reasonable timeframe, consistent with the Processor's standard backup rotation schedule (not to exceed ninety (90) days), following the deletion of live data under Clause 9.1, unless Union or Member State law requires storage of the Personal Data.

9.4 Export window. The Controller shall have a sixty (60) day window following termination or expiry of the Principal Agreement to request a data export. The Processor may charge a reasonable fee for data export requests made after this window.

9.5 Aggregate data. Notwithstanding the above, the Processor may retain anonymised or aggregated data derived from Personal Data (from which no individual Data Subject can be identified, directly or indirectly) for product improvement, analytics, and benchmarking purposes.

Clause 10: Confidentiality and Personnel

10.1 Confidentiality obligations. The Processor shall treat all Personal Data processed under this Agreement as confidential and shall not disclose it to any third party except: (a) to Sub-processors in accordance with Clause 5; (b) as required by Union or Member State law, in which case the Processor shall, to the extent permitted by law, provide the Controller with prior notice; (c) as instructed in writing by the Controller.

10.2 Personnel access. The Processor shall ensure that access to Personal Data is limited to those of its personnel and Sub-processor personnel who need access to perform the services under the Principal Agreement. The Processor shall ensure that all such personnel are subject to binding confidentiality obligations.

10.3 Training. The Processor shall ensure that all personnel with access to Personal Data receive appropriate and regular training on data protection obligations under this Agreement and applicable Data Protection Laws.

Clause 11: Liability

11.1 Each Party shall be liable to the other for damages caused by any breach of this Agreement in accordance with the liability provisions of the Principal Agreement.

11.2 Where both the Controller and the Processor are responsible for any damage caused by processing in breach of this Agreement or applicable Data Protection Laws, they shall be held liable in accordance with Article 82 GDPR. Each Party shall inform the other promptly of any claim, complaint, or enforcement action by a Supervisory Authority or Data Subject that relates to the processing of Personal Data under this Agreement.

11.3 Nothing in this Agreement shall limit or exclude either Party's liability for: (a) death or personal injury caused by negligence; (b) fraud or fraudulent misrepresentation; (c) any liability that cannot be lawfully excluded or limited; or (d) any liability to Data Subjects under Article 82 GDPR.

Clause 12: Term, Amendments and Governing Law

12.1 Term. This Agreement shall enter into force on the Effective Date and shall continue in full force and effect until the termination or expiry of the Principal Agreement, subject to the survival provisions of Clause 12.4.

12.2 Amendments by Processor. The Processor may amend this Agreement from time to time to reflect changes in Data Protection Laws, regulatory guidance, or Sub-processor arrangements. The Processor shall provide the Controller with at least thirty (30) days' written notice of any material amendment. Continued use of the Platform following the notice period shall constitute acceptance of the amended Agreement. Where an amendment materially and adversely affects the Controller's data protection obligations, the Controller may terminate the Principal Agreement within the notice period without liability for termination fees.

12.3 Governing law and jurisdiction. This Agreement is governed by the laws of the Netherlands (Dutch law), without regard to its conflict of law provisions. Any dispute arising out of or in connection with this Agreement that cannot be resolved by good-faith negotiation within thirty (30) days shall be submitted to binding arbitration in Amsterdam, the Netherlands, in accordance with the rules of the Netherlands Arbitration Institute (NAI). The language of the proceedings shall be English. Nothing in this clause prevents either Party from seeking urgent injunctive or other interim relief from a court of competent jurisdiction. This clause is subject to any mandatory jurisdiction requirements applicable to the Controller in its country of establishment.

12.4 Survival. Clauses 1 (Definitions), 6 (Audit Rights), 9 (Return and Deletion), 10 (Confidentiality), 11 (Liability), and 12 (Term and Governing Law) shall survive the termination or expiry of this Agreement.

12.5 Precedence. In the event of any conflict or inconsistency between this Agreement and the Principal Agreement, the provisions of this Agreement shall prevail in respect of the processing of Personal Data. In the event of any conflict between this Agreement and the SCCs incorporated under Clause 7.3, the SCCs shall prevail to the extent required by applicable Data Protection Laws.

12.6 Entire agreement. This Agreement, together with its Schedules and the Principal Agreement, constitutes the entire agreement between the Parties with respect to the processing of Personal Data and supersedes all prior agreements, understandings, and representations, whether oral or written, relating to the same subject matter.

Execution

The Parties have executed this Data Processing Agreement as of the Effective Date. This Agreement may be executed electronically, including by acceptance of the C2 Terms of Service which incorporates this DPA by reference, or by wet ink signature below.

THE CONTROLLER	**The Controller (Customer)**
Authorised Signatory	Signature: _____
Name & Title	Name: _____
Date	Date: _____
Note: Where the Controller accepts this DPA as part of the C2 online Terms of Service acceptance flow, a separate wet-ink signature is not required. The electronic acceptance record constitutes valid execution.	

THE PROCESSOR	**Agile Futurist (acting as the Processor for the C2 Platform)**
Authorised Signatory	Signature: _____

Name & Title	Name: _____
Date	Date: _____

Schedule 1: Details of Processing

This Schedule sets out the details of the processing carried out by the Processor on behalf of the Controller pursuant to Clause 2 and Article 28(3) GDPR.

Subject matter of processing	Provision of the C2 All-in-One HRIS Platform, including all modules subscribed to by the Controller: Applicant Tracking System, Onboarding, Employee Records Management, Leave & Absence Management, Performance Management, Learning Management System, AI HR Assistant, Reporting & Analytics, and any additional modules enabled under the Controller's subscription tier.
Duration of processing	For the duration of the Principal Agreement and for such further period as required under Clause 9 (Return and Deletion).
Nature of processing	Collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, and deletion of Personal Data; automated processing for the purpose of Platform functionality including AI-assisted HR queries (where the AI module is enabled).
Purpose of processing	Delivery of the Platform services described in the Principal Agreement; technical support, maintenance, and security operations; backup and disaster recovery; platform analytics and performance monitoring (using anonymised/aggregated data only).
Types of Personal Data processed	Identification data (name, employee ID, date of birth); contact data (email address, telephone number, work address, home address where provided); employment data (job title, department, employment start/end dates, contract type, salary grade); payroll data where integrated (salary, tax information, bank account details); absence and leave data (dates, reason categories); performance data (appraisal records, feedback, goals, disciplinary records); recruitment data (CV, application form, interview notes, assessment results); learning data (training completions, certification records); access and authentication data (username, login timestamps, system audit logs); Special Category Data only where explicitly entered by the Controller (health/medical absence data, disability information where provided).
Categories of Data Subjects	Current employees of the Controller; former employees (during applicable retention periods); job applicants and candidates; contractors and temporary workers; Platform users (managers, HR administrators) of the Controller.
Processing location	Primary: European Union (EU). All data is stored and processed within EU-based infrastructure. Processor shall not transfer Personal Data outside the EEA without compliance with Clause 7.
Controller's designated contact for Data Breach notifications	As specified in the Controller's account settings, or the primary account administrator email address if no separate contact is designated.

Schedule 2: Technical and Organisational Measures (TOMs)

This Schedule describes the technical and organisational measures implemented by the Processor to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR. These measures are subject to ongoing review and improvement by the Processor.

2.1 Access Control and Authentication

- Role-based access control (RBAC) enforced at application and infrastructure level; access rights granted on principle of least privilege.
- Multi-factor authentication (MFA) required for every employee and administrator at every sign-in, with a one-time code sent by email; also enforced for Processor's own personnel accessing production systems.
- Unique user credentials for each user; shared accounts prohibited.
- Automatic session timeout after a configurable period of inactivity.
- Access logs retained for ninety (90) days; alerts on anomalous activity reviewed daily.
- Privileged access management (PAM) controls for infrastructure-level access by Processor personnel.

2.2 Encryption

- All Personal Data encrypted in transit using TLS 1.2 or higher (TLS 1.3 preferred).
- All Personal Data encrypted at rest with AES-256, using keys held in AWS Key Management Service (AWS KMS).
- Each Controller environment is encrypted under keys created for that tenancy alone: one for its databases, one for its uploaded content, and two for the Platform's own secrets and logs.
- Platform custody (default on all plans): the Processor manages the tenancy's keys in AWS KMS on the Controller's behalf. Keys are rotated at least annually.
- Tenant custody (available on request on all plans): the Controller generates the key material for the database and content keys on its own systems, wraps it so that only AWS KMS can unwrap it, and retains its own copy. The Processor passes the wrapped material to AWS KMS and never has access to the unwrapped key material.
- Under tenant custody the Controller may at any time withdraw the key material held by AWS KMS: itself, without the Processor's cooperation, through a cloud account it has nominated for that purpose, or otherwise by instructing the Processor to withdraw it. All stored copies of the Controller's data then become unreadable to every party, including the Processor and AWS. Running services stop no later than their next restart, normally within hours.
- Access is restored when the Controller re-imports the key material it retained. On Startup and SME plans restoration is complete. On Enterprise plans, a database instance left inaccessible for more than seven (7) days cannot be restored as an instance and is restored from backup instead.
- While the key material is in place, the Platform decrypts Personal Data as needed to provide the services. Tenant custody gives the Controller the ability to end that access; it does not prevent processing during normal operation.
- The Processor's tooling refuses to schedule deletion of a tenant-custody key, and no Processor operator identity holds a standing right to decrypt Controller data. Any call against a tenancy's keys by an identity other than that tenancy's own is recorded in an audit trail and raises an alert. Permanent deletion of key material is a separate step, governed by the Principal Agreement.
- Export copies: every backup and long-term archive is also written as an export copy encrypted to a key held only by the Controller, in both custody modes, once the Controller has supplied the public half of its export key. Export copies can be opened by the Controller without the Processor, and are not affected by a withdrawal of key material.

- Under tenant custody the Controller holds two secrets, its key material and its export key, and each is the recovery path for the other. If the Controller loses both, the Personal Data cannot be recovered, and the Processor cannot recreate either secret.
- Backup data encrypted using the same or equivalent standards as live data.

2.3 Tenant Isolation and Data Separation

- Each Controller is provisioned with a dedicated single-tenant environment: its own databases and storage, not shared with any other customer.
- Each environment is encrypted under keys created for that tenancy alone (see section 2.2).
- Access to an environment is limited to the Platform's own service identities for that tenancy and to authorised Processor personnel, in accordance with section 2.1.

2.4 Infrastructure Security

- All infrastructure hosted in EU-based data centres with ISO 27001 certification.
- Network segmentation with defined security zones; web-facing services separated from internal processing and data layers by firewall controls.
- Web Application Firewall (WAF) deployed in front of all publicly accessible endpoints.
- DDoS mitigation controls in place.

2.5 Vulnerability and Patch Management

- Internal security audits against OWASP ASVS Level 2; findings remediated and tracked. An independent penetration test by a qualified third party is planned.
- Automated vulnerability scanning of application code and dependencies as part of the CI/CD pipeline.
- Security updates to the operating system and components are taken in on every release, and portal software is updated weekly.
- Dependency management tooling in place to identify and remediate known CVEs.

2.6 Availability, Backup and Disaster Recovery

- On Enterprise plans, the Platform runs with redundant infrastructure components across multiple availability zones.
- Daily automated backups of all tenant data; backups retained for thirty (30) days.
- Restores are rehearsed every quarter for every component, against a recovery time objective (RTO) of at most one (1) hour and a recovery point objective (RPO) of at most twenty-four (24) hours.
- Documented Disaster Recovery Plan reviewed annually.

2.7 Incident Response and Breach Management

- Documented Security Incident Response Plan defining roles, escalation paths, and response timelines.
- Security events logged and monitored with CloudWatch alarms; alerts are read and acted on daily, weekends and holidays included, by the Processor's DevOps team.
- Data Breach register maintained in accordance with Article 33(5) GDPR.
- Personnel trained on incident identification and escalation procedures.

2.8 Personnel and Organisational Measures

- All personnel with access to Personal Data subject to contractual confidentiality obligations.

- Designated Data Protection Officer contact (dpo@agilefuturist.com) available to respond to Controller and Data Subject queries.

2.9 Privacy by Design

- Data minimisation principles applied in Platform development; only Personal Data necessary for each feature's stated purpose is collected.
- Retention periods set per data category; candidate, helpdesk, CRM and internal support data are erased or anonymised automatically when their period ends, and other categories are reported for review.

Schedule 3: Sub-processor Register

NOTE: The live and authoritative Sub-processor Register, including the most current additions and changes, is published and maintained at: cognitis.cloud/trust-center/#tc-subprocessors. The table below reflects approved Sub-processors as of the version date of this Agreement. The Processor will provide advance notice of changes in accordance with Clause 5.2.

Sub-processor	Purpose / Services Provided	Processing Location	Transfer Mechanism	DPA Status
Amazon Web Services, Inc. *Cloud Infrastructure and Storage (Amazon S3)*	Primary compute, object storage (Amazon S3), networking and databases underpinning the Platform.	EU (Ireland, eu-west-1)	N/A (EEA)	**Signed, Art. 28 compliant**
Amazon Web Services, Inc. (Amazon SES)	Transactional and notification emails: DSAR alerts, onboarding flows, system notifications.	EU (Ireland, eu-west-1)	N/A (EEA)	**Signed, Art. 28 compliant**
Mistral AI SAS	Default language model provider for the AI assistant on the Frontoffice and the Learning Portal. Receives the questions people type into the assistant and the knowledge-base excerpts it answers from. The assistant has no access to HR records, and users are asked not to type personal or health details. Knowledge retrieval uses a self-hosted Qdrant vector database on EU (Ireland) infrastructure. The Platform sends every request to Mistral's EU endpoint. Mistral does not use Controller data to train its models and keeps no copy of requests (Zero Data Retention). On request, SME and Enterprise customers can have the Frontoffice assistant answer from their own AI host instead.	EU (the Platform sends every request to Mistral's EU endpoint; Mistral AI SAS, Paris, France)	N/A (EEA)	**Mistral AI Data Processing Addendum (effective 27 July 2026), Art. 28**
Amazon Web Services, Inc. (Amazon CloudWatch) *Platform Monitoring and Observability*	Application performance monitoring, logging and alerting. Covered by the same AWS DPA as core infrastructure.	EU (Ireland, eu-west-1)	N/A (EEA)	**Signed, Art. 28 compliant**

LEGAL NOTE TO CONTROLLER: Before executing this DPA, the Controller should verify that the named Sub-processors and their processing locations are acceptable given the Controller's own data protection obligations and any applicable national restrictions. Sub-processor DPA documentation and ISO/SOC 2 certifications are available on request by contacting dpo@agilefuturist.com.

Data Protection Contact & Version History

Processor Data Protection Contact

Legal Entity	Agile Futurist, sole proprietorship, registered under Dutch law. Registered address: De Nieuwe Erven 3, Unit 14784, 5431 NV Cuijk, The Netherlands
Trading Name	C2 All-in-One HRIS Platform
Platform URL	www.cognitis.cloud
Data Protection Officer (DPO)	dpo@agilefuturist.com
DPA Questions & Objections	dpo@agilefuturist.com
Data Subject Rights Requests	dpo@agilefuturist.com
Sub-processor Change Notifications	Published at cognitis.cloud/trust-center/#tc-subprocessors
Security Incidents & Breach Notifications	security@agilefuturist.com
General & Legal Correspondence	c2.hris@cognitis.cloud
Customer Support	support@cognitis.cloud

Version History

Version	Date	Summary of Changes	Applicable To
1.0	April 2026	Initial release. Full Art. 28 GDPR compliance. Includes Schedules 1–3 and AI module provisions.	All new and existing C2 customers from April 2026.
1.1	July 2026	Schedule 3 updated: sub-processor vendor names added (Amazon Web Services eu-west-1 for infrastructure and email delivery, OpenAI for AI language model inference). Transfer mechanism for OpenAI confirmed as SCC Module 2 (Controller to Processor). AI data-flow note added: no personal employee data transmitted to OpenAI; knowledge retrieval is handled by a self-hosted Qdrant vector database on EU (Ireland) infrastructure. Customer support platform (Frappe HelpDesk) confirmed as self-hosted on EU	All C2 customers from July 2026.

		(Ireland, AWS eu-west-1) infrastructure; Frappe Ltd is not a sub-processor.	
1.2	October 2026	Schedule 2 updated: tenant isolation now described as a dedicated single-tenant environment per Controller; encryption key management expanded (per-tenancy AWS KMS keys, platform custody by default, tenant custody available on request, export copies encrypted to a Controller-held key, and the Controller's responsibility for its own key material). Schedule 3 updated: Mistral AI SAS (EU) replaces OpenAI as the AI language model provider; OpenAI removed as a Sub-processor. Address of the live Sub-processor Register corrected to cognitis.cloud/trust-center/#tc-subprocessors.	All C2 customers on the current platform from October 2026.
1.3	October 2026	Clause 8.1: Data Breach notice to the Controller within twenty-four (24) hours of becoming aware, instead of seventy-two (72); breach contact changed to security@cognitis.cloud. Clause 4.4 reworded. Clause 5.3: objection period ten (10) calendar days, instead of fourteen (14), to match the notice periods of the Processor's own sub-processors. Clause 9.3 aligned with the legal-retention exception in 9.1. Schedule 2 brought in line with how the Platform is run: withdrawal of key material by the Controller through a nominated cloud account or on instruction, MFA for every employee and administrator, access logs kept 90 days, internal security audits with an independent penetration test planned, patching on every release, multi-zone redundancy on Enterprise plans, quarterly restore rehearsals with stated RTO and RPO, daily review of monitoring alerts, retention as enforced, and no intrusion detection system listed. Schedule 3: Mistral and CloudWatch entries corrected; Frappe HelpDesk removed, as it is part of the Platform and not a sub-processor.	All C2 customers from October 2026.
1.4	October 2026	Processor contacts changed: the Data Protection Officer to dpo@agilefuturist.com (Clause	

		5.3, Schedule 2, Schedule 3 and the contact table), and security incidents and Data Breach notifications to security@agilefuturist.com. The Processor's legal form corrected to sole proprietorship (eenmanszaak). No change to the rights or obligations of either Party.	

FINAL LEGAL DISCLAIMER: This Data Processing Agreement template has been prepared by Agile Futurist for use with the C2 All-in-One HRIS Platform. It is provided for informational purposes and as a standard contractual baseline. Agile Futurist does not provide legal advice. The Controller is strongly advised to have this Agreement reviewed by qualified legal counsel or a Data Protection Officer before execution, particularly in relation to jurisdiction-specific requirements in Belgium, the Netherlands, Germany, Austria, and any other country where the Controller operates. Agile Futurist reserves the right to update this Agreement in accordance with Clause 12.2.