Data Processing Agreement — Core

Just Software ApS · Approved

Version	v1.21	**Approved on**	8 November 2026
Approval authority	CISO or CTO	**Next review due**	—
Last reviewed	—	**Review interval**	365 days
Relevant frameworks	GDPR		

Data Processing Agreement — Core

Standard Contractual Clauses pursuant to Article 28(3) of Regulation (EU) 2016/679 (GDPR)

Clauses 1–15 reproduce the standard contractual clauses adopted by the Danish Data Protection Agency (Datatilsynet), January 2020 version, approved by the European Data Protection Board (Opinion 14/2019), completed only where the template leaves a matter to the parties. Everything the parties have agreed beyond the template is in the Appendices.

Data controller	The customer identified in the Customer Schedule ("the data controller")
Data processor	Just Software ApS · CVR no. 43432117 · Automatikvej 1, 3., 2860 Søborg, Denmark ("the data processor")
Services covered	The services identified in the Customer Schedule, each described in its Product Annex
Composition	This Core DPA, the Product Annexes, the Residency Annexes, any Jurisdiction Annexes and the Customer Schedule — see Appendix D.9

each a "party"; together "the parties"

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble
3. The rights and obligations of the data controller
4. The data processor acts according to instructions
5. Confidentiality
6. Security of processing
7. Use of sub-processors
8. Transfer of data to third countries or international organisations
9. Assistance to the data controller
10. Notification of personal data breach
11. Erasure and return of data
12. Audit and inspection
13. The parties' agreement on other terms
14. Commencement and termination
15. Data controller and data processor contacts/contact points

Appendix A — Information about the processing
Appendix B — Authorised sub-processors
Appendix C — Instruction pertaining to the use of personal data
Appendix D — The parties' terms of agreement on other subjects
Form of Customer Schedule

2. Preamble

2.1 These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2.2 The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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 and repealing Directive 95/46/EC (General Data Protection Regulation).

2.3 In the context of the provision of the services identified in the Customer Schedule, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

2.4 The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

2.5 Four appendices are attached to the Clauses and form an integral part of the Clauses.

2.6 Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

2.7 Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

2.8 Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

2.9 Appendix D contains provisions for other activities which are not covered by the Clauses.

2.10 The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

2.11 The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

3.1 The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the Clauses.

3.2 The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3.3 The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

4.1 The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

4.2 The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

5.1 The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

5.2 The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

6.1 Article 32 GDPR stipulates that, 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, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

- (a) Pseudonymisation and encryption of personal data;
- (b) the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.2 According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

6.3 Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by inter alia providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

7.1 The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

7.2 The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

7.3 The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 (thirty) days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

7.4 Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

7.5 A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

7.6 If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not

affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

8.1 Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

8.2 In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

8.3 Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

- (a) transfer personal data to a data controller or a data processor in a third country or in an international organization;
- (b) transfer the processing of personal data to a sub-processor in a third country;
- (c) have the personal data processed in by the data processor in a third country.

8.4 The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

8.5 The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

9.1 Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

- (a) the right to be informed when collecting personal data from the data subject;
- (b) the right to be informed when personal data have not been obtained from the data subject;
- (c) the right of access by the data subject;
- (d) the right to rectification;
- (e) the right to erasure ('the right to be forgotten');
- (f) the right to restriction of processing;
- (g) notification obligation regarding rectification or erasure of personal data or restriction of processing;
- (h) the right to data portability;
- (i) the right to object;
- (j) the right not to be subject to a decision based solely on automated processing, including profiling.

9.2 In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

- (a) The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
- (b) the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;
- (c) the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);
- (d) the data controller's obligation to consult the competent supervisory authority prior to processing where

a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

9.3 The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

10.1 In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

10.2 The data processor's notification to the data controller shall, if possible, take place within 24 (twenty-four) hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

10.3 In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

- (a) The nature of the personal 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 likely consequences of the personal data breach;
- (c) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10.4 The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

11.1 On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

11.2 The data processor commits to exclusively process the personal data for the purposes and duration provided for by any such Union or Member State law requiring storage and under the strict applicable conditions.

12. Audit and inspection

12.1 The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

12.2 Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

12.3 The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

13.1 The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

14.1 The Clauses shall become effective on the date of both parties' signature.

14.2 Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

14.3 The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

14.4 If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

14.5 Signature: the Clauses are signed by way of the Customer Schedule, or accepted as set out in Appendix D.9.

15. Data controller and data processor contacts/contact points

15.1 The parties may contact each other using the contacts/contact points set out in Appendix D.7 and the Customer Schedule.

15.2 The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Appendix A — Information about the processing

A.1 The purpose of the data processor's processing of personal data on behalf of the data controller is: as set out, for each service, in the Product Annex for that service.

A.2 The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing): as set out, for each service, in the Product Annex for that service, together with the handling of support requests and online meetings described in Appendix C.2 and C.4.

A.3 The processing includes the following types of personal data about data subjects: as set out, for each service, in the Product Annex for that service. No special categories of personal data (Article 9 GDPR) and no data relating to criminal convictions and offences (Article 10 GDPR) are processed in the services, and the data controller shall not submit such data to the services.

A.4 Processing includes the following categories of data subject: as set out, for each service, in the Product Annex for that service.

A.5 The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration: the duration of the service agreement between the parties. Upon termination, personal data is deleted in accordance with Clause 11.1 and Appendix C.4.

Appendix B — Authorised sub-processors

B.1 Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors: those listed in (a), which are used in every data residency boundary; the AI provider selected by the data controller under (b), where AI-assisted diagnostics is enabled; and the sub-processors listed in the Residency Annex for the tenant's primary data residency boundary and in the applicable Product Annexes.

(a) Sub-processors used in every data residency boundary

Name	Registration no.	Address	Processing location	Description of processing
Microsoft Ireland Operations Limited (Microsoft Azure and Microsoft 365)	Irish company no. 256796	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	Microsoft Azure: Azure regions within the data residency boundaries selected in the Customer Schedule. Microsoft 365: EU (Microsoft EU Data Boundary), for every residency boundary	Microsoft Azure: cloud infrastructure hosting of the hosted services — compute, storage, networking, backup, logging and telemetry. Microsoft 365 (Exchange Online, Microsoft Teams): receipt of support requests sent by e-mail before their transfer to the ticketing system, and online meetings with the data controller's personnel. Customer meetings are not recorded or transcribed unless agreed with the data controller in advance
Herodesk ApS	CVR 44196972	Voldbækvej 1, 8220 Brabrand, Denmark	EU (Germany), for every residency boundary	Support ticketing: support requests and related contact details submitted by the data controller's personnel
Mistral AI SAS	Paris register no. 952 418 325	15 rue des Halles, 75001 Paris, France	EU, for every residency boundary	AI-assisted handling of support requests: classification of incoming support e-mail, drafting of anonymised knowledge-base content, and anonymisation under Appendix C.4. Processes the content of support requests and related contact details submitted by the data controller's personnel

(b) Optional AI providers for AI-assisted diagnostics

Where a Product Annex states that AI-assisted diagnostics is available and the data controller enables it, the data controller selects one of the following providers in the Customer Schedule. Only the selected provider processes the data controller's diagnostic data; a provider that has not been selected processes none. The selection does not depend on the data residency boundary.

Name	Registration no.	Address	Processing location	Description of processing	Retention	Transfer tool
Mistral AI SAS	Paris register no. 952 418 325	15 rue des Halles, 75001 Paris, France	EU	AI-assisted diagnostics, where selected (Appendix C.2)	Not retained: zero data retention applies to inputs and outputs, and troubleshooting and analytics data are not stored	None required (processing within the EU)

Name	Registration no.	Address	Processing location	Description of processing	Retention	Transfer tool
Anthropic PBC	Delaware public benefit corporation	500 Howard Street, San Francisco, CA 94105, USA	United States	AI-assisted diagnostics, where selected (Appendix C.2)	Zero data retention: inputs and outputs are not stored after the response; see below for flagged content	EU Standard Contractual Clauses, Module Three (processor to processor), incorporated in its data processing addendum, and the EU-U.S. Data Privacy Framework

The data processor has opted out of model training with Mistral AI SAS under section 2.3 of the provider's data processing addendum, and uses the provider's EU API endpoint.

Anthropic's processing for its own purposes. Anthropic PBC processes diagnostic data as a sub-processor, with one exception. Where Anthropic's automated systems flag inputs or outputs as potentially violating its usage policies, Anthropic may retain those inputs and outputs for up to two years to enforce those policies. For that limited processing Anthropic acts as an independent controller, not on the data processor's instruction. The data controller can avoid it entirely by selecting Mistral AI SAS or by leaving AI-assisted diagnostics disabled.

Sub-processors whose use depends on the data residency boundary — in particular transactional e-mail delivery — are listed, with their processing location and transfer tool, in the Residency Annex for that boundary. For each tenant, those of the Residency Annex for the tenant's primary boundary apply.

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. Save as provided in Clause 7.3 and Appendix B.2, the data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

For clarity: Google Analytics is not a sub-processor under the Clauses. It processes personal data solely in the data processor's capacity as an independent data controller (website analytics) and does not process personal data on behalf of the data controller within the services. Nor is Microsoft 365 a sub-processor where it is used for the data processor's ordinary business correspondence with the data controller — for example about contracts, invoicing or account management — which the data processor carries out as an independent data controller (Appendix D.8).

Published listing. The sub-processors currently authorised for each service and residency boundary, and the Azure regions currently used in each boundary, are also published at https://just-software.com/trust, or at such other address as the data processor notifies to the data controller. That publication is for information. In the event of any discrepancy, this Appendix B and the applicable annexes, as amended by notices given under Appendix B.2, prevail. Publication alone does not constitute notice under Clause 7.3.

B.2 Prior notice for the authorisation of sub-processors

In accordance with Clause 7.3, the data processor shall notify the data controller in writing, to the contact stated in the Customer Schedule, of any intended addition or replacement of sub-processors at least 30 (thirty) days before the change takes effect. Where the Customer Schedule records that the data controller has selected Extended Governance (Appendix D.12), the notice period is 90 (ninety) days.

A change takes effect for the data controller when the added or replacing sub-processor first processes the data controller's personal data. The data processor may apply the change to other customers earlier, provided the data controller's personal data is not processed by that sub-processor before the notice period has expired. Where the data controller itself enables a feature that uses a notified sub-processor before the notice period has expired, that is its documented instruction to engage the sub-processor from that time.

If the data controller objects on reasonable, data-protection-related grounds, the change does not take effect for it while the parties seek a solution in good faith; if no solution is found, the data controller may terminate the affected services without penalty before the change takes effect.

Appendix C — Instruction pertaining to the use of personal data

C.1 The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the processing described in the applicable Product Annexes, and the handling of support requests and online meetings described in Appendix C.2 and C.4, as necessary to provide, operate, secure, support and maintain the services in accordance with the service agreement, the service documentation (docs.just-software.com) and the Clauses. The service agreement, the configuration options exercised by the data controller (including selection of the primary and secondary data residency boundaries, of optional features and their AI provider, and of extended log retention) and the Clauses together constitute the complete documented instruction.

Persons authorised by the data controller, including its own service providers, may administer the services and give instructions on the data controller's behalf through the services or in writing. Instructions given and configuration made by such persons are instructions of the data controller.

C.2 Security of processing

This Appendix C.2, together with the service-specific measures in each applicable Product Annex, constitutes the description of technical and organisational measures for the purposes of Article 28(3)(c) and Article 32 GDPR.

The level of security shall reflect the nature of the personal data processed by each service and the role of that service in the data controller's organisation, as described in its Product Annex. No special categories of personal data are processed. Unless a Product Annex states otherwise, the parties agree that a high level of security is required.

Deployment model. Unless its Product Annex states otherwise, each service is a hosted service, operated by the data processor in Microsoft Azure. Where a Product Annex states that a service is a customer-deployed service, the personal data processed by that service is stored in the data controller's own environment, and the provisions on data residency boundaries, primary and secondary regions, backups, recovery objectives and retention in this Appendix C apply to it only to the extent that its Product Annex says so. The data processor's processing of personal data in connection with a customer-deployed service is limited to what its Product Annex describes, together with the handling of support requests.

The data processor operates an information security management system certified under the Danish D-mærket (D-Seal) scheme, with policies and controls mapped to ISO/IEC 27001:2022 Annex A. The current certificate and control status report form part of the documentation package in Appendix C.7.

The data processor is then entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security. The data processor shall however – in any event and at a minimum – implement the following measures, together with the service-specific measures in each applicable Product Annex:

- **Encryption:** personal data is encrypted in transit (TLS 1.2 or higher for web, API and administrative traffic) and at rest (platform-level encryption in Microsoft Azure and Microsoft 365), in accordance with a documented encryption standard.
- **Access control:** least-privilege and need-to-know access, role-based access control, multi-factor authentication for all administrative access, just-in-time activation of privileged access with no standing access to production key material, and dedicated protection of administrator accounts. Access rights are reviewed periodically and withdrawn on role change or departure under documented on- and offboarding procedures.
- **Segregation:** logical separation of customer tenants, and separation of production from development and test environments. Production data is not copied into test environments.
- **Data classification:** information assets are classified and handled under a documented classification scheme.
- **Availability and resilience:** unless its Product Annex states otherwise, each tenant of a hosted service is deployed in a primary Azure region and in a secondary Azure region, each within a data residency boundary selected by the data controller in the Customer Schedule. The data controller may select a secondary region within the same boundary as the primary region, or in a different boundary. Product data, including backups, is held in both the primary and the secondary region, and backup copies are logically separated from the source systems. Where a Product Annex states that a service runs in a single region, or a Residency Annex states that no secondary region is available within its boundary and

the data controller has not selected one in another boundary, the consequences for recovery objectives are stated in that annex. Point-in-time restore is enabled on the datastores supporting every service with a stated recovery point objective. Recovery objectives for each service are set out in its Product Annex and are measured from incident declaration within supported hours (Appendix D.4). Recovery objectives are validated by a yearly continuity test with recorded results. Backup integrity and restore capability are verified at least quarterly by automated restore tests covering a sample of services and datastores selected for each test.

- **Vulnerability and threat management:** continuous security monitoring, vulnerability management and threat intelligence; continuous automated security testing, with documented review of vulnerabilities in production systems at least quarterly; and penetration testing of the services by a qualified independent third party, the first to be completed no later than 31 March 2027 and thereafter at least once a year.
- **Secure development:** a documented secure software development lifecycle applying privacy and security by design, with code review and change management. Production infrastructure is defined as code and held under version control.
- **Optional AI-assisted diagnostics:** where a Product Annex states that the feature is available, it is disabled by default and enabled only on the data controller's recorded selection, which includes its choice of AI provider from those listed in Appendix B.1(b) and constitutes a documented instruction for the purposes of Clause 4. Submitted diagnostic data is processed only by the selected provider, at the location and on the transfer tool stated in Appendix B.1(b). Where the selected provider is located outside the tenant's data residency boundaries, the data controller can keep diagnostic processing within its boundaries by selecting a provider located within them, where one is listed, or by leaving the feature disabled.
- **AI-assisted support handling:** support requests submitted by the data controller's personnel are processed with the assistance of the AI provider listed for that purpose in Appendix B.1(a), which is located within the EU/EEA. This covers classification of incoming support e-mail, drafting of knowledge-base content and anonymisation under Appendix C.4. It applies to all support requests and does not depend on the data controller's selection of optional features.
- **AI providers generally:** the data processor does not permit data submitted to an AI provider to be used for model training, and user feedback submission to AI providers is disabled in the services.
- **Logging:** security-relevant events in the services and underlying infrastructure are logged, and logs are retained in accordance with Appendix C.4 and, where selected, Appendix D.11. Audit logs of access to the data processor's own infrastructure and key management systems are retained as described in Appendix D.8.
- **Organisational measures:** a top-level information security policy approved by management; named security responsibility; confidentiality undertakings for all personnel as part of documented onboarding; mandatory security awareness training under a documented training plan; a documented incident management procedure; internal audit; management review; and documented supplier security management covering the sub-processor chain.
- **Physical security:** physical security of the infrastructure of the hosted services is provided by Microsoft Azure data centres (ISO/IEC 27001 and SOC 2 attested). The data processor operates no production infrastructure on its own premises; endpoint and remote-work controls apply to its personnel's devices.

The data processor may modify these measures, provided that the modifications do not materially reduce the overall level of security of the services.

C.3 Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

- **Data subject requests:** upon written request, the data processor shall provide the information or perform the access, rectification, erasure, restriction or export operations available in the services, or otherwise assist the data controller, without undue delay and in time to enable the data controller to meet the time limits that apply to it under the GDPR.
- **Personal data breach:** the elements to be provided under Clause 10.4, and the notification procedure, are as set out in Appendix D.3.
- **DPIA and prior consultation:** the data processor shall make available the documentation package in Appendix C.7 and answer reasonable written questions to support the data controller's data protection impact assessments and any prior consultation of the supervisory authority.

Assistance under this Appendix C.3 is provided free of charge to the extent it is required by the GDPR and

proportionate to the nature of the services. Costs of assistance exceeding this may be charged at the data processor's then-current reasonable rates, agreed in advance in writing.

C.4 Storage period/erasure procedures

Prior to deletion, the data controller may export personal data from the services using the export functions available in the services, or request the data processor's assistance with the return of the data.

Personal data is stored with the data processor for the duration of the service agreement and is thereafter deleted according to the following schedule, together with the service-specific entries in each applicable Product Annex. The data processor certifies deletion as required by Clause 11.1; the certification may take the form of an automated written confirmation sent to the contact stated in the Customer Schedule.

Data type	Retention	Erasure procedure
Application data (accounts, configuration and service data not listed separately in a Product Annex)	Deleted from production within 30 days of termination of the services; purged from backups on backup rotation and no later than 90 days after termination	Automated deletion from production in both regions; removed from backups on expiry of the backup retention period
Support data (Herodesk)	365 days from ticket closure	Deleted, or anonymised as set out below, by the data processor and the sub-processor
Support e-mail in the support mailbox (Microsoft 365)	365 days from receipt	Automated deletion by a Microsoft 365 retention policy
Support requests processed by the AI provider (Mistral AI)	Not retained: zero data retention applies to inputs and outputs	No retained data to erase
Transactional e-mail logs	As stated in the Residency Annex for the tenant's primary boundary	Automated deletion by the sub-processor
AI diagnostic submissions	As stated for the selected provider in Appendix B.1(b)	No retained data to erase, save content retained by the provider for its own purposes as described in Appendix B.1(b)
Security and access logs containing product data (such as user and device identifiers and IP addresses)	90 days, or 13 months for a service for which the data controller has selected extended log retention (Appendix D.11)	Automated log rotation and deletion

Infrastructure audit logs. Audit logs of access to the data processor's own infrastructure and key management systems contain no product data and are not covered by this schedule. They are described in Appendix D.8.

Anonymisation of support requests and knowledge-base content. The data controller instructs the data processor, on expiry of the retention period for support data, either to delete each support request or to anonymise it irreversibly, so that neither the request nor any information derived from it relates to an identified or identifiable natural person or identifies the data controller's organisation. Anonymisation covers the content of the request — including user identifiers, device identifiers, IP addresses, certificate details and log excerpts — and not only the contact details attached to it, and is carried out under a documented procedure. The data processor may also derive knowledge-base content from support requests at any time, provided that the knowledge-base content is anonymised to the same standard before it is retained. Content anonymised in this way is no longer personal data, and the data processor may retain it for its support knowledge base. Content that cannot be reliably anonymised, or whose anonymisation an applicable Jurisdiction Annex does not permit, is deleted.

C.5 Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation: the processing locations stated for each sub-processor in Appendix B.1 (for an optional AI provider, only where the data controller has selected it), the locations set out in the Residency Annex for each data residency boundary selected by the data controller, and, for a customer-deployed service, the data controller's own environment.

C.6 Instruction on the transfer of personal data to third countries

The data controller's selection in the Customer Schedule of a primary data residency boundary and of the boundary of its secondary region constitutes its documented instruction to transfer personal data to the locations, and to the sub-processors, stated in the Residency Annex for each boundary selected, on the basis of the transfer tool stated there. The data controller's selection of an AI provider for AI-assisted diagnostics under Appendix B.1(b) constitutes its documented instruction to transfer the diagnostic data it submits to that provider's processing location, on the transfer tool stated there. If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7 Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data processor shall once a year, at its own expense, make available to the data controller an audit and documentation package consisting of: the current D-mærket (D-Seal) certificate and re-certification status; the current control status report, being a report of the implementation status of the controls in the data processor's D-mærket control framework; a summary of the approved information security policy set; the current description of technical and organisational measures (Appendix C.2 and the applicable Product Annexes); a summary of the results of the most recent yearly continuity test; and, once performed, a summary of the most recent independent penetration test. The parties agree that this package may be used as the primary means of demonstrating compliance.

In addition, the data controller or a representative of the data controller (who shall not be a competitor of the data processor) may carry out an audit, including an inspection of the data processor's compliance with the Clauses, once per calendar year, or additionally when required by a competent supervisory authority, following a personal data breach, or where the data controller has documented, reasonable grounds to believe that the data processor is not complying with the Clauses. Audits shall be announced with at least 30 (thirty) days' written notice, save where a supervisory authority or the circumstances of a personal data breach require a shorter period, be conducted during normal business hours, not unreasonably disrupt the data processor's operations, and be subject to appropriate confidentiality undertakings. Physical inspection of Microsoft Azure data centres is not possible; audit of the hosting layer is performed on the basis of Microsoft's third-party audit reports (ISO/IEC 27001, SOC 2), which the data processor shall make available. Each party bears its own costs of an audit; the data processor's reasonable assistance beyond one audit day per year may be charged as set out in Appendix C.3.

C.8 Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor shall review each sub-processor's compliance at least once a year on the basis of the sub-processor's third-party audit reports and certifications (for Microsoft: ISO/IEC 27001 and SOC 2 reports; for other sub-processors: their data processing agreements, certifications and audit documentation). Documentation of the review and the underlying reports shall be made available to the data controller on written request, subject to the sub-processor's confidentiality terms. Where such documentation is insufficient to demonstrate compliance, the data processor shall take reasonable steps to obtain additional assurance, which may include supplementary documentation, written responses, independent reports or, where contractually available and proportionate, an audit.

Appendix D — The parties' terms of agreement on other subjects

D.1 Relationship to the service agreement and transaction channels

The Clauses supplement the service agreement between the parties, regardless of the transaction channel, including subscriptions purchased through the Microsoft Azure Marketplace or through a reseller. Clause 2.4 applies to any terms accepted through such a channel.

D.2 The data controller acting as data processor for its customers

Where the data controller acts as data processor for its own customers, as indicated in the Customer Schedule, the following applies:

- (a) The data controller is responsible for obtaining the authorisation required under Article 28(2) GDPR from the relevant customer(s) to engage the data processor as a sub-processor, and for ensuring that its instructions under the Clauses are consistent with those customers' instructions.
- (b) The obligations of the data processor under the Clauses apply equally to personal data processed on behalf of the data controller's customers.
- (c) Where a data processing agreement between the data controller and a customer imposes data protection obligations on the data controller that are stricter than or additional to the Clauses, or a customer requires further instructions relating to the services, and the data controller notifies the data processor of them in writing, identifying the customer and tenant(s) concerned, those obligations and instructions apply to the data processor in respect of that customer's personal data and, where stricter, take precedence over the corresponding provisions of the Appendices and annexes.
- (d) Within 10 (ten) business days of a notification under (c), the data processor shall confirm that it can comply, or state which obligations or instructions it cannot meet within the standard services, or can meet only at additional cost. The notified obligations and instructions take effect on confirmation, or on expiry of that period if the data processor has not objected. If the data processor objects, the parties shall agree the necessary measures, including any price, or the services shall not be used for that customer.
- (e) References in the Clauses to "the data controller" shall be read as references to the data controller acting on behalf of the relevant customer(s). The Clauses do not determine or limit the content of the data controller's data processing agreements with its customers. The data controller is the data processor's contractual counterpart and point of contact for instructions under the Clauses.
- (f) This Appendix D.2 does not limit any rights which a customer has directly against the data processor under applicable law, or as a named third-party beneficiary of a document signed by the data processor, including rights of audit and inspection and, in the event of the data controller's insolvency, rights of access to and return of its personal data.
- (g) The selections recorded in the Customer Schedule — including data residency boundaries, optional AI-assisted diagnostics and its AI provider, and extended log retention — may be made separately for each tenant in the ordering record, which then forms part of the Customer Schedule for that tenant.

D.3 Personal data breach — elements and procedure (Clause 10.4 and Appendix C.3)

The data processor's notification under Clause 10 is sent by e-mail to the data controller's designated contact in the Customer Schedule, and is followed up in phases as information becomes available. The data processor shall provide the elements listed in Clause 10.3, together with: the time the breach was discovered and, where known, when it occurred; the services, tenants and residency boundaries affected; the contact point at the data processor from whom more information can be obtained; and, after closure, a written post-incident report.

D.4 Supported hours

"Supported hours" means Monday to Friday, 08:00–17:00 Central European Time (CET, or CEST when daylight saving time applies), excluding Danish public holidays, unless the service agreement states otherwise. Supported hours determine how recovery objectives are measured under Appendix C.2: a recovery time objective of 8 hours means 8 supported hours, not 8 elapsed hours. Supported hours do not limit the notification obligations in Clause 10.

D.5 Liability

Each party's liability arising out of or in connection with the Clauses is subject to the limitations and exclusions of liability set out in the service agreement between the parties.

Nothing in the Clauses or in the service agreement limits or excludes: (a) either party's liability to a data subject under Article 82 GDPR; (b) either party's liability for an administrative fine imposed on it in respect of its own infringement; or (c) any liability which cannot be limited or excluded under applicable law.

Where one party has paid compensation for damage for which the other party is also responsible, it may claim back from the other party that part of the compensation corresponding to the other party's part of the responsibility, in accordance with Article 82(5) GDPR.

D.6 Governing law and venue

The Clauses shall be governed by Danish law. Any dispute shall be settled by the ordinary Danish courts at the data processor's registered venue.

D.7 Contact points

The data controller's contact points for notices and breach notification are set out in the Customer Schedule. The data processor's contact points are security@just-software.com (data protection and breach notification) and mail@just-software.com (general).

D.8 Processing by the data processor as an independent controller

The data processor processes the following personal data relating to the data controller's personnel as an independent data controller, and not on behalf of the data controller: (a) account, administrator and billing records needed to establish, invoice and administer the service relationship, and ordinary business correspondence about it; (b) records of administrative access to the data processor's own management and support systems, kept to meet its own obligations under Article 32 GDPR; and (c) records the data processor must retain under Danish bookkeeping and tax legislation. The Clauses, including Clause 11.1, do not apply to that processing, which is governed by the data processor's privacy notice.

Infrastructure audit logs. Audit logs of access to the data processor's own infrastructure and key management systems, for example operations on cryptographic key material, record actions by the data processor's personnel and service identities. They contain no product data and are not processed on behalf of the data controller. The data processor keeps them to meet its own obligations under Article 32 GDPR and to evidence its security controls in audits. They are retained for 13 months in write-once storage, which prevents their alteration or deletion during that period, and are then deleted automatically. The Clauses, including Clause 11.1, do not apply to them.

The data processor shall not process personal data supplied to or generated within the services for its own purposes, including product development, model training, marketing or analytics. This does not prevent the use, for the data processor's support knowledge base, of support content and knowledge-base content anonymised on the data controller's instruction under Appendix C.4, which is no longer personal data.

D.9 Structure, versions and acceptance

Composition. The Clauses comprise this Core DPA together with: (a) a Product Annex for each service identified in the Customer Schedule; (b) the Residency Annex covering each data residency boundary selected in the Customer Schedule, whether as the primary boundary or as the boundary of the secondary region (the EU/EEA Residency Annex covers the EU/EEA boundary; the North America Residency Annex covers both the United States and the Canada boundaries); (c) each Jurisdiction Annex selected in the Customer Schedule, which adds the terms required by a non-EU privacy law that applies to the data controller; and (d) the Customer Schedule, including any per-tenant selections recorded in the ordering record under Appendix D.2(g).

Tenants in more than one boundary. Where a tenant's primary and secondary regions are in different boundaries, personal data held in each boundary — including replicated data and backups — is governed by the Residency Annex covering that boundary, including its processing locations and transfer tool. Boundary-dependent sub-processors, such as the provider of transactional e-mail, are those of the Residency Annex for the tenant's primary boundary. The provider of AI-assisted diagnostics does not depend on the boundary; it is the provider selected under Appendix B.1(b).

Versions. The Customer Schedule identifies the version of the Core DPA and of each annex that applies. The data processor may issue new versions. A new version that does not reduce the data controller's rights, expand the purposes of the processing or add categories of personal data applies to the data controller if the data processor notifies it in writing at least 30 (thirty) days in advance and the data controller does not object on reasonable, data-protection-related grounds within that period. Any other new version applies only if the data controller agrees to it. Until then, the versions identified in the Customer Schedule govern. Changes to sub-processors follow Clause 7.3 and Appendix B.2. An amendment signed by both parties prevails over any later version issued by the data processor.

New services. Where the data controller adds a service, the Product Annex for that service, in its current version, applies from the time the service is added, and the ordering record for that service forms part of the Customer Schedule.

Precedence. In the event of conflict, the following order applies: (1) Clauses 1–15; (2) the Customer Schedule; (3) the Jurisdiction Annexes; (4) the Residency Annexes; (5) the Product Annexes; (6) Appendices A–D of this Core DPA. The Customer Schedule may not vary Clauses 1–15 except by completing matters the Clauses leave to the parties.

Acceptance by reference. Where the Clauses are incorporated by reference in the data processor's terms of service and accepted through the ordering process, that acceptance constitutes signature for the

purposes of Clause 14.1, and the ordering record — including the data controller's selection of residency boundaries, of any Jurisdiction Annex, of AI-assisted diagnostics and its AI provider, of extended log retention and of Extended Governance — constitutes the Customer Schedule.

D.10 Definitions

In the Appendices and annexes: **"data residency boundary"** means one of the geographic areas offered for hosting the hosted services — EU/EEA, United States or Canada — each described in a Residency Annex (the United States and Canada boundaries in the North America Residency Annex); **"hosted service"** means a service operated by the data processor in Microsoft Azure; **"customer-deployed service"** means a service that its Product Annex describes as deployed in the data controller's own Azure subscription or other environment; **"tenant"** means an instance of a service provisioned for the data controller or, where Appendix D.2 applies, for one of its customers; **"primary region"** and **"secondary region"** mean the Azure regions in which a tenant of a hosted service is hosted and replicated, each within a data residency boundary selected in the Customer Schedule; **"product data"** means personal data held in the services themselves; **"support data"** means support requests and related correspondence submitted by the data controller's personnel; **"diagnostic data"** means data the data controller submits for AI-assisted diagnostics; and **"operational telemetry"** means monitoring and performance data generated by the operation of the services.

D.11 Optional extended log retention

The data controller may select extended log retention for one or more services in the Customer Schedule or through the ordering process. The selection is a documented instruction for the purposes of Clause 4. For the services selected, it extends the retention of security and access logs containing product data (Appendix C.4), and of the service-specific log records that a Product Annex identifies as subject to extended log retention, from 90 days to 13 months. Records with a different retention period — such as records a Product Annex retains for the duration of the subscription — are not affected.

Extended log retention is a paid option under the service agreement. It does not change the processing locations, sub-processors or technical and organisational measures that apply to the logs.

If the data controller deselects extended log retention, or on termination of the services, the standard 90-day retention applies from that point, counted from each log record's creation, and records older than 90 days are deleted at the next log rotation and no later than 30 days thereafter.

D.12 Extended Governance

The data controller may select Extended Governance under the service agreement for one or more services. Extended Governance is intended for data controllers in scope of Regulation (EU) 2022/2554 (DORA) or Directive (EU) 2022/2555 (NIS2), and its terms are set out in the Extended Governance Addendum to the service agreement, which is not part of the Clauses.

Where the Customer Schedule records that Extended Governance has been selected, the notice period in Appendix B.2 is 90 (ninety) days, and any term of the Extended Governance Addendum that is stricter than the Clauses on the same matter constitutes an agreed amendment of the Clauses to that extent.

Extended Governance does not reduce, and is not a condition for, the data controller's rights under the Clauses, including notification of personal data breaches under Clause 10 and Appendix D.3, and audits and the documentation package under Appendix C.7.

Form of Customer Schedule

Item	Entry
Data controller	[legal name, registration no., address]
Service agreement	[reference / Marketplace offer / reseller agreement]
Core DPA version	Core DPA v[●]
Services and Product Annexes	[service name — Product Annex v[●]] (one line per service)

Item	Entry
Primary data residency boundary (hosted services)	[EU/EEA — Residency Annex EU/EEA v[●] / United States — Residency Annex North America v[●] / Canada — Residency Annex North America v[●]]
Secondary region boundary (hosted services)	[Same as primary / EU/EEA — Residency Annex EU/EEA v[●] / United States — Residency Annex North America v[●] / Canada — Residency Annex North America v[●] / None available]
Acknowledgement	Where the secondary region is in a different boundary from the primary region, the data controller acknowledges that product data, replicated data and backups are also held in that boundary, and that the terms and transfer tool for that boundary apply to them.
Boundaries selected by	[name] on [date]
Jurisdiction Annexes	[None / United States (CCPA/CPRA) — v[●] / Canada (PIPEDA and Quebec) — v[●]]
Optional AI-assisted diagnostics (Appendix B.1(b))	[Not enabled / Enabled for: (services) — AI provider: Mistral AI SAS (EU) / Anthropic PBC (United States) — recorded by (name) on (date)]
Extended log retention (Appendix D.11)	[Not selected / Selected for: (services) — recorded by (name) on (date)]
Extended Governance (Appendix D.12)	[Not selected / Selected for: (services) — Extended Governance Addendum v[●] / Replaced by a separate agreement, see Deviations]
Data controller acts as processor for its customers (Appendix D.2)	[Yes — selections per tenant in the ordering record / No]
Data controller contact for notices and breach notification	[name, role, e-mail, telephone]
Deviations	None. Any deviation from the Clauses requires a separate amendment signed by both parties.

On behalf of the data controller

Name: _____

Position: _____

Date: _____

Signature: _____

On behalf of the data processor

Name: _____

Position: _____

Date: _____

Signature: _____