Extended Governance Addendum

Just Software ApS · Approved

Version	v1.5	**Approved on**	8 November 2026
Approval authority	CISO or CTO	**Next review due**	—
Last reviewed	—	**Review interval**	365 days
Relevant frameworks	NIS2, GDPR, ISO 27001, D-mærket		

Extended Governance Addendum

Addendum to the service agreement for EasyScep and EasyRadius — supplier-side terms for customers in scope of DORA or NIS2

Supplier	Just Software ApS · CVR no. 43432117 · Automatikvej 1, 3., 2860 Søborg, Denmark ("Just Software")
Customer	The customer for whose subscription(s) Extended Governance is selected ("the Customer")
Applies to	The subscriptions for which Extended Governance is recorded in the Customer Schedule or ordering record ("Extended Governance Subscriptions")

1. Purpose, scope and structure

1.1 This addendum sets out the contractual terms Just Software provides so that a Customer that is a financial entity under Regulation (EU) 2022/2554 (DORA), or an essential or important entity under Directive (EU) 2022/2555 (NIS2), can meet its own requirements for ICT third-party arrangements and supply-chain security. Its sections follow Article 30(2) and (3) DORA and Commission Delegated Regulation (EU) 2025/532 on subcontracting.

1.2 Just Software is not itself a financial entity or a designated critical ICT third-party service provider. The obligations in this addendum are contractual obligations towards the Customer.

1.3 All terms in this addendum, including those in sections 8 to 12 that Article 30(3) DORA requires for ICT services supporting critical or important functions, apply to every Extended Governance Subscription. The Customer may therefore use those subscriptions to support critical or important functions without further negotiation. The Customer decides whether the services support a critical or important function and records that classification in its own register.

1.4 This addendum supplements the service agreement (including terms accepted through the Microsoft Azure Marketplace or a reseller) and the Data Processing Agreement between the parties (the "DPA"). It forms part of the service agreement and is not part of the DPA's Clauses. Order of precedence:

- (a) For the processing of personal data, the DPA applies. Where this addendum sets stricter terms than the DPA on the same matter, those terms constitute an agreed amendment of the DPA to that extent, as provided in DPA Appendix D.12.
- (b) Otherwise, this addendum prevails over the service agreement where they conflict.
- (c) Nothing in this addendum reduces the Customer's rights under the DPA.

1.5 Where the Customer resells or provides the services onward to its own customers, this addendum covers the Customer's own use and its customers' tenants under the Extended Governance Subscriptions. The Customer's customers have no direct rights under this addendum unless named in writing as third-party beneficiaries.

2. Description of the services and subcontracting (DORA Art. 30(2)(a))

2.1 The services are described in the service documentation at docs.just-software.com and in the Product Annexes to the DPA. EasyScep is a cloud PKI and SCEP certificate service for Microsoft Intune. EasyRadius is a cloud RADIUS authentication service for network access control with RadSec support.

2.2 Just Software may use ICT subcontractors to provide the services, including for functions that may support the Customer's critical or important functions, on the conditions in section 13. The subcontractors are those listed in Appendix B of the DPA and the applicable Residency Annex, which apply to personal and non-personal data alike.

3. Locations of services and data (DORA Art. 30(2)(b))

3.1 The services are provided, and all Customer data — personal and non-personal, including backups, logs and operational telemetry — is processed and stored, in the Azure regions within the data residency boundaries selected by the Customer, as described in the DPA's Residency Annexes. Each subscription runs in a primary and a secondary region.

3.2 Exceptions to 3.1 are limited to those stated in the DPA and the Residency Annexes, including Microsoft's case-by-case support access to the underlying infrastructure.

3.3 Just Software gives at least 90 days' written notice of any change to the countries or regions where the services are provided or Customer data is processed or stored.

4. Security of data (DORA Art. 30(2)(c) and 30(3)(c))

4.1 Just Software ensures the availability, authenticity, integrity and confidentiality of Customer data through the technical and organisational measures in DPA Appendix C.2 and the Product Annexes. Those measures apply to non-personal data as well as personal data.

4.2 Just Software maintains:

- (a) 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, including annual internal audit and management review;
- (b) a dedicated root certificate authority per customer, so that one customer's certificate infrastructure can be renewed or revoked without affecting other customers;
- (c) continuous security monitoring and automated security testing; and
- (d) penetration testing of the services by a qualified independent third party performed at least once a year.

A summary of the most recent penetration test is made available to the Customer on request.

5. Access, recovery and return of data (DORA Art. 30(2)(d))

5.1 On request, Just Software provides a full export of the Customer's data in a documented, commonly used format within 10 business days, at any time during the subscription and any transition period under section 12.

5.2 On termination for any reason, and in the event of Just Software's insolvency, resolution or discontinuation of business operations, Just Software shall ensure that the Customer can access, recover and obtain the return of all its personal and non-personal data in an easily accessible, commonly used format. Just Software maintains documented procedures to ensure this in those situations.

5.3 Return covers certificates and their issuance and revocation records, configuration, and logs within their retention period. It does not cover certificate authority private keys. They are kept non-exportable to the Customer for security reasons, and a change of provider is carried out by re-keying: a new certificate authority is established with the new provider and new certificates are deployed through the Customer's device management. This exclusion is a specified exemption for the purposes of the switching provisions of Regulation (EU) 2023/2854 (Data Act).

6. Service levels (DORA Art. 30(2)(e) and 30(3)(a))

6.1 Just Software provides the services to the following service levels:

Measure	Target
Availability of certificate issuance and enrolment, revocation status publication (OCSP/CRL) and the authentication plane	99.95% per calendar month
Recovery time and recovery point objectives	As stated per service component in the Product Annexes, measured as set out in DPA Appendix C.2
Response to critical incidents (service unavailable or seriously degraded)	Within 30 minutes, 24/7, via the critical incident phone line

Measure	Target
Response to other support requests	[●] within supported hours (DPA Appendix D.4)

6.2 Availability excludes scheduled maintenance notified under section 7.2 and unavailability caused by the Customer's own equipment, configuration or networks, or by force majeure. [Service credits: ●]

6.3 Just Software reports its service level performance to the Customer on request, and at least once a year.

6.4 Where the service levels are not met, Just Software shall take appropriate corrective action without undue delay, and the Customer has the remedies set out in the service agreement and section 14.

7. Notice of changes and developments (DORA Art. 30(3)(b))

7.1 Just Software notifies the Customer in writing at least 60 days in advance of material changes to the services. Material changes are changes that reduce functionality or security, or change how Customer data is processed. New features are not material changes.

7.2 Scheduled maintenance that may affect availability is notified at least 30 days in advance. Urgent security maintenance is carried out when needed and notified as soon as possible.

7.3 Just Software notifies the Customer without undue delay of any development that may materially affect its ability to provide the services in line with the agreed service levels. This includes developments at its subcontractors and material deterioration of its financial position, such as loss of half of its share capital, a going-concern qualification in its annual report, restructuring, bankruptcy, liquidation or change of control. The notice includes Just Software's assessment of the impact and the measures it is taking.

7.4 Just Software makes its most recent annual report available to the Customer on request.

8. ICT incidents (DORA Art. 30(2)(f); NIS2 Art. 23)

8.1 "ICT incident" means any incident or significant cyber threat that affects, or is reasonably likely to affect, the availability, authenticity, integrity or confidentiality of the services or of Customer data, including personal data breaches.

8.2 Just Software notifies the Customer of an ICT incident:

- (a) **Initial notice:** without undue delay and in any event within 8 hours of becoming aware of it, at any time of day, including weekends and public holidays.
- (b) **Detailed report:** within 72 hours of becoming aware of it.
- (c) **Final report:** within one month of the detailed report; where the incident is still ongoing at that time, a progress report then and a final report within one month of its resolution.

8.3 Notices are sent to the Customer's incident contact in the Customer Schedule. The initial notice of an incident that makes the services unavailable or seriously degraded is also given by telephone. Notices include, as far as known: the nature and timeline of the incident, the services, tenants and data affected, its likely consequences, the measures taken or proposed, and a contact point. For personal data breaches they also include the elements in DPA Clause 10.3 and Appendix D.3.

8.4 Just Software provides the technical information and assistance the Customer reasonably needs to classify the incident and to report it to its competent authorities. This assistance is included at no additional cost.

9. Business continuity (DORA Art. 30(3)(c))

9.1 Just Software maintains a business continuity plan and an ICT disaster recovery plan for the services. They are based on active operation in two Azure regions, with data and backups held in both.

9.2 The plans are tested at least once a year, including an end-to-end re-key exercise of the certificate infrastructure. Backup integrity and restore capability are verified at least quarterly. A summary of the results is made available to the Customer on request.

10. Access, inspection and audit (DORA Art. 30(3)(e))

10.1 The Customer, an independent third party appointed by it, and its competent authorities have unrestricted rights of access, inspection and audit relating to the services, including the right to take copies on site of documentation that is critical to the operation of the services.

10.2 Each year Just Software completes the Customer's ICT third-party risk assessment or questionnaire at no additional cost. It also provides the documentation package in DPA Appendix C.7.

10.3 On-site audits and inspections:

- (a) The Customer gives at least 30 days' written notice. Shorter notice applies where a competent authority requires it, or following an ICT incident.
- (b) Audits are carried out during supported hours, under appropriate confidentiality undertakings, and without unreasonable disruption to the services.
- (c) Audits by the Customer take place once per calendar year, and additionally where required by a competent authority, after an ICT incident, or where the Customer has reasonable grounds to believe that Just Software does not comply with this addendum.
- (d) Pooled audits with other customers of Just Software are permitted.

10.4 Audits and copies do not extend to other customers' tenants or data, or to source code, unless a competent authority requires it. Where an audit would affect other customers' rights, the parties agree an alternative level of assurance, such as reports, written responses or third-party assessments. Copies may be used only for audit and supervisory purposes and are treated as confidential.

10.5 Each party bears its own costs. Just Software's assistance beyond two audit days per calendar year is charged at the rates in section 16.3.

11. Threat-led penetration testing (DORA Art. 30(3)(d))

11.1 Just Software participates and cooperates fully in threat-led penetration testing (TLPT) under Articles 26 and 27 DORA, where the services fall within the scope of the Customer's test. Pooled testing under Article 26(4) DORA is accepted.

11.2 Testing is agreed in advance:

- (a) The Customer gives at least 60 days' written notice of the scope and timing.
- (b) The parties agree rules of engagement that protect other customers' tenants and the stability of the shared platform.
- (c) Testing of Microsoft Azure infrastructure follows Microsoft's rules for penetration testing.

11.3 Just Software bears its own costs of participation. The costs of the testers are borne by the Customer.

12. Exit strategy and transition (DORA Art. 30(3)(f))

12.1 On termination for any reason, Just Software provides a transition period of up to 6 months at the Customer's request.

12.2 During the transition period:

- (a) Just Software continues to provide the services at the agreed prices, so that the risk of disruption is reduced;
- (b) Just Software assists the Customer in migrating to another provider or to its own systems, including the return of data under section 5 and the re-key process described there; and
- (c) the services are not deleted or suspended while they are in use.

12.3 Assistance with switching is provided free of charge. Continued use of the services is charged at the agreed prices.

12.4 For the DPA, the provision of the services ends when the transition period ends, and the deletion periods in the DPA run from that date.

13. ICT subcontracting (DORA Art. 30(2)(a); Delegated Regulation (EU) 2025/532)

13.1 Just Software remains fully responsible for the services, including those parts provided by subcontractors. It monitors its subcontracting chain and assesses the risks of each subcontractor before use and at least annually.

13.2 Just Software imposes on its subcontractors the security, confidentiality, incident reporting and data protection obligations needed for Just Software to meet this addendum, to the extent their standard terms allow. Where a subcontractor's terms cannot be negotiated, as is the case for Microsoft and Mistral AI, Just Software relies on that subcontractor's published commitments and third-party audit reports and informs the Customer on request of any material deviations.

13.3 Changes to subcontractors that support the services are notified in writing at least 90 days before they

take effect for the Customer. The notice contains enough information for the Customer to assess the impact on its risks and on Just Software's ability to meet its obligations.

- (a) A change takes effect for the Customer when the subcontractor first processes the Customer's data. Until then, Just Software may already apply the change to other customers, provided the Customer's subscriptions remain on the existing arrangement — for example because the feature that uses the new subcontractor is not enabled for them, or because their data continues to be routed to the existing subcontractor.
- (b) Where the Customer itself enables a feature that uses a notified subcontractor before the notice period has expired, that is the Customer's instruction to use the subcontractor from that time.

13.4 The Customer may object on reasonable grounds within the notice period, and Just Software responds within 10 business days. If the objection is not resolved, the Customer may terminate the affected Extended Governance Subscriptions without penalty, with section 12 applying. While an objection is being handled, the change does not take effect for the Customer.

13.5 Just Software passes on notifications about changes in its subcontractors' own chains without undue delay when it becomes aware of them.

14. Termination (DORA Art. 28(7) and 30(2)(h))

14.1 The Customer may terminate the affected Extended Governance Subscriptions without penalty in any of the following cases:

- (a) Just Software significantly breaches applicable law, regulation or this addendum.
- (b) Circumstances identified through the Customer's monitoring of ICT third-party risk are deemed capable of altering the performance of the services, including material changes affecting Just Software or its subcontractors.
- (c) Just Software has evidenced weaknesses in its overall ICT risk management, in particular in how it ensures the availability, authenticity, integrity and confidentiality of data.
- (d) The Customer's competent authority can no longer effectively supervise the Customer as a result of the conditions of the arrangement.

14.2 Just Software may terminate an Extended Governance Subscription on at least 6 months' written notice. This does not affect its right to terminate for the Customer's material breach, including non-payment, under the service agreement.

14.3 Section 12 applies on termination for any reason.

15. Authorities, Register of Information and training (DORA Art. 30(2)(g) and (i))

15.1 Just Software cooperates fully with the Customer's competent authorities and resolution authorities, and with persons appointed by them, in relation to the services. This includes giving them access to information, documents, premises and systems as described in section 10. Cooperation is subject to customary confidentiality measures towards other customers and is provided at no additional cost to the Customer.

15.2 Just Software provides, and keeps up to date, the information the Customer needs to maintain its Register of Information for each service, including Just Software's legal identifiers, the services provided, their locations and the subcontracting chain.

15.3 On reasonable request, Just Software takes part in the Customer's ICT security awareness programmes and digital operational resilience training to the extent relevant to the services. This may consist of providing material or attending up to one session per year.

16. Fees

16.1 Extended Governance is charged as the flat annual fee in Just Software's published price list for the number of products selected, regardless of plan size, and is billed annually in advance.

16.2 The fee covers the obligations in this addendum, including incident assistance (section 8.4), the annual assessment (section 10.2), cooperation with authorities (section 15.1) and switching assistance (section 12.3).

16.3 Assistance beyond what this addendum includes is charged at Just Software's rates as published or agreed in writing in advance: [●] per hour.

16.4 Where changes in law or a competent authority's requirements make changes to this addendum

necessary, the parties shall negotiate them promptly and in good faith. Documented additional costs to Just Software are compensated as agreed in writing in advance.

17. Term, confidentiality and general terms

17.1 This addendum applies to an Extended Governance Subscription from the date Extended Governance is selected until the end of the transition period after the subscription ends. Extended Governance may be deselected with effect from the end of an annual billing period.

17.2 Each party treats the other's non-public information received under this addendum as confidential. The Customer may share Just Software's security and compliance documentation with its competent authorities, resolution authorities and auditors to the extent needed to meet its own obligations under DORA, NIS2 or the GDPR, on confidential terms at least as strict as these.

17.3 Liability under this addendum is subject to the limitations and exclusions of liability in the service agreement, except where those cannot apply under mandatory law.

17.4 This addendum is governed by Danish law. Disputes are settled by the ordinary Danish courts at Just Software's registered venue.

17.5 Contact points:

- Just Software: security@just-software.com (incidents, security and compliance notices), support@just-software.com (support), and the 24/7 critical incident line +45 21 99 00 99.
- The Customer: the contacts recorded in the Customer Schedule, including an incident contact reachable 24/7.

17.6 This addendum is accepted by selecting Extended Governance in the ordering process, where the service agreement incorporates it by reference, or by signature of both parties.

On behalf of the Customer	On behalf of Just Software ApS
Name:	Name:
Position:	Position:
Date:	Date:
Signature:	Signature: