Document Name	Annex A - Data Processing Agreement
Effective Date	2026-07-01
Last Updated	2026-11-23
Owner	Compeas AB
Classification	Customer Documentation
Version	1.8

DATA PROCESSING AGREEMENT (DPA)

Agreement in accordance with Article 28(3) of the General Data Protection Regulation EU 2016/679.

This Data Processing Agreement ("**DPA**") forms part of the Master Subscription and Services Agreement ("**MSSA**") entered into between **Compeas AB** ("**Processor**") and **[Customer]** ("**Controller**").

This DPA applies where Compeas processes Personal Data on behalf of Customer in connection with the Services.

1. Parties, positions and contact details

Controller	**Processor**
[Enter the organisations full name]	Compeas AB
Org.nr	**Org.nr**
[Enter the organisations org.nr]	559590-5703
Address	**Address**
[Enter the organisations address]	Östra långgatan 35, 731 30 Köping, Sverige
Contact person for administration of this personal data processing agreement	**Contact person for administration of this personal data processing agreement**
Name: [Enter contact person first- and surname] Email: [Enter contact person email address] Phone: [Enter contact person phone number]	Name: Compeas AB Email: info@compeas.com Phone: +46 10 265 00 70
Contact persons for partner cooperation on data protection	**Contact persons for partner cooperation on data protection**
Name: [Enter contact person first- and surname] Email: [Enter contact person email address] Phone: [Enter contact person phone number]	Name: Compeas AB, data protection Email: privacy@compeas.com Phone: +46 10 265 00 70

2. Definitions and order of precedence

2.1 Capitalised terms not otherwise defined in this DPA shall have the meanings assigned to them in the Agreement.

Item	Description
Data Protection Legislation	All laws and regulations applicable to the processing of Personal Data under this DPA, including the GDPR and any applicable national data protection legislation.

Controller	The natural or legal person, public authority, agency, or other body which determines the purposes and means of the processing of Personal Data, as defined in Article 4(7) GDPR.
Customer	The legal entity entering into the Agreement and acting as Controller of the Customer Personal Data processed under this DPA.
Customer Personal Data	Personal Data processed by Compeas on behalf of Customer in connection with the provision of the Services.
Data Subject	An identified or identifiable natural person to whom Personal Data relates, as defined in Article 4(1) GDPR.
DPA	This Data Processing Agreement, including its annexes and any amendments agreed by the Parties.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).
Instructions	The documented instructions provided by Customer to Compeas regarding the processing of Customer Personal Data under this DPA and the Agreement.
International Transfer	A transfer of Personal Data to a country outside the European Economic Area (EEA) that is subject to Chapter V of the GDPR.
Main Agreement	Means the Master Subscription and Services Agreement, together with all Order Form(s) and incorporated annexes, including the Data Processing Agreement (DPA) and Service Level Agreement (SLA), each forming an integral part of the contractual framework between the Parties.
Personal Data	Any information relating to an identified or identifiable natural person, as defined in Article 4(1) GDPR.
Personal Data Breach	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.

Processing	Any operation or set of operations performed on Personal Data, whether or not by automated means, as defined in Article 4(2) GDPR.
Processor	Compeas AB acting on behalf of Customer with respect to the processing of Customer Personal Data, as defined in Article 4(8) GDPR.
Security Measures	The technical and organisational measures implemented by Compeas and described in Annex C (Security & Compliance Addendum) or equivalent security documentation made available to Customer.
Services	The software and related services provided by Compeas under the Agreement.
Standard Contractual Clauses (SCCs)	The standard contractual clauses adopted by the European Commission pursuant to Article 46 GDPR for transfers of Personal Data to third countries.
Sub-processor	Any third party engaged by Compeas to process Customer Personal Data on behalf of Customer in connection with the Services.
Supervisory Authority	An independent public authority established pursuant to Article 51 GDPR that is responsible for monitoring the application of data protection law.

2.2 References in this DPA to the GDPR shall include any legislation replacing, supplementing, or implementing the GDPR within the European Union, the European Economic Area, or applicable national law.

2.3 In the event of any conflict between this **DPA** and the **Main Agreement** with respect to the processing of Personal Data, the provisions of this DPA shall prevail to the extent of such conflict. This Section 2.3 is without prejudice to Section 3.3, which governs inconsistencies in administrative and procedural provisions only.

3. Background and purpose

3.1 The Processor processes Personal Data on behalf of the Controller under this Data Processing Agreement, together with the Instructions and any list of Sub-

processors (hereinafter collectively referred to as the “DPA”). This DPA is intended to ensure the protection of the rights and freedoms of Data Subjects in connection with such Processing, in accordance with Article 28(3) of Regulation (EU) 2016/679 (the “GDPR”).

3.2 Where this DPA forms part of a set of contractual documents under another agreement, such other agreement is the "Main Agreement" as defined in Section 2.1 of this DPA.

3.3 In the event of any inconsistency between the administrative and procedural provisions set out in Section 2 (Definitions and Order of Precedence), Sections 15 or 16, Clause 17.6, Sections 18–20, or Section 22 of this DPA and the Main Agreement, the provisions of the Main Agreement shall prevail. For the avoidance of doubt, this Section 3.3 applies solely to administrative and procedural matters and does not affect the primacy of this DPA over the Main Agreement with respect to the processing of Personal Data as set out in Section 2.3.

3.4 References in this DPA to national or Union legislation shall be deemed to refer to such legislation as amended and in force from time to time.

4. Processing of Personal Data & Specification

4.1 The Processor processes Personal Data on behalf of the Controller as set out in this DPA.

4.2 The Processor shall process Personal Data only in accordance with the Controller’s written Instructions.

4.3 The Processor shall not process Personal Data otherwise than as set out in this DPA and the Controller’s Instructions as amended from time to time.

4.4 Special Categories of Personal Data

Customer shall not submit special categories of Personal Data (as defined in Article 9 GDPR) to the Services unless: (a) Customer has requested and received Processor's prior written consent; (b) Customer has conducted and provided Processor with a data protection impact assessment (DPIA) where required by Article 35 GDPR; (c) appropriate supplementary technical and organisational safeguards have been implemented as agreed in writing between the Parties;

and (d) the Processing is documented in an updated Annex to this DPA. Processor reserves the right to refuse Processing of special categories of Personal Data where it determines that the associated risks cannot be adequately mitigated.

4.5 Group Use

Where the Order Form names Customer Affiliates, the Controller instructs the Processor to make Customer Personal Data available to the Customer Affiliates and their End Users as configured in the Services, including through the Compeas Auditor Tool. The Controller is responsible for the legal basis for this sharing within its group.

5. Responsibility of the Controller

5.1 The Controller is responsible for ensuring that a valid legal basis exists for the Processing at all times and for issuing appropriate and lawful Instructions, taking into account the nature of the Processing, so that the Processor and any Sub-processor can perform their obligations under this DPA and, where applicable, the Main Agreement.

5.2 The Controller shall, without undue delay, inform the Processor of any changes to the Processing that may affect the Processor's obligations under Data Protection Legislation.

5.3 The Controller is responsible for informing Data Subjects about the Processing and for ensuring that Data Subjects' rights under Data Protection Legislation are respected, as well as for performing any other obligations incumbent upon the Controller under Data Protection Legislation.

6. Responsibility of the Processor

6.1 The Processor undertakes to process Personal Data only in accordance with this DPA and for the specific purposes set out in the Instructions, and to comply with Data Protection Legislation. The Processor shall also keep itself continuously informed of applicable law in this area.

6.2 The Processor shall implement measures to protect Personal Data against any Processing that is not in accordance with this DPA, the Instructions, or Data Protection Legislation.

6.3 The Processor undertakes to ensure that all natural persons acting under its authority comply with this DPA and the Instructions, and that such persons are informed of relevant Data Protection Legislation.

6.4 Upon the Controller's request, the Processor shall assist the Controller in ensuring compliance with Articles 32–36 of the GDPR and shall respond to requests for the exercise of Data Subjects' rights under Chapter III of the GDPR, taking into account the nature of the Processing and the information available to the Processor.

6.5 Where the Processor considers that the Instructions are unclear, contrary to Data Protection Legislation, or missing, and determines that new or supplementary Instructions are necessary to perform its obligations, the Processor shall promptly inform the Controller and temporarily suspend the Processing until new Instructions are received, unless otherwise agreed by the Parties.

6.6 Where the Controller provides new or amended Instructions, the Processor shall, without undue delay after receipt, inform the Controller whether the implementation of such Instructions will result in additional costs for the Processor.

7. Security of Processing

7.1 The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the Processing, including, as appropriate, inter alia, pseudonymisation and encryption of Personal Data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing. The Processor shall ensure that the Processing

complies with this DPA and applicable Data Protection Legislation and that the rights of Data Subjects are protected.

7.2 The Processor shall ensure that persons authorised to process Personal Data are subject to appropriate confidentiality undertakings or statutory obligations of confidentiality. The Processor shall implement access control measures to ensure that access to Personal Data is limited to natural persons acting under its authority who require such access for the performance of their tasks.

7.3 The Processor shall continuously maintain and monitor appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the Processing, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the Processing, and the likelihood and severity of risk for the rights and freedoms of natural persons.

7.4 The Processor shall comply with documented Instructions from the Controller. Any additional or amended security requirements requested by the Controller after the conclusion of this DPA shall only be implemented where mutually agreed between the Parties and where they comply with Data Protection Legislation.

7.5 To the extent necessary for security and compliance purposes, the Processor shall maintain logs of access to Personal Data. Such logs shall be protected against unauthorised access, alteration and loss using appropriate technical and organisational measures and shall be retained only for as long as necessary for security, compliance, or as otherwise required under applicable law or documented Instructions.

7.6 The Processor shall systematically test, assess and evaluate the effectiveness of the technical and organisational measures implemented to ensure the security of the Processing.

7.7 The Processor shall, taking into account the nature of the Processing and the information available to it, assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR and shall also, to the extent possible, assist the Controller in responding to requests for the exercise of Data Subject rights under Chapter III of the GDPR.

7.8 The Processor shall notify the Controller without undue delay after becoming aware of a Personal Data Breach. Such notification shall, where possible, contain at least a description of the nature of the Personal Data Breach, the categories and approximate number of Data Subjects concerned, the categories and approximate number of Personal Data records concerned, the likely consequences of the Personal Data Breach, and the measures taken or proposed to address the Personal Data Breach, including mitigation of its possible adverse effects. The Processor shall provide the Controller with reasonable assistance in handling and remediating the Personal Data Breach.

8. Confidentiality and Communications

8.1 The Processor shall ensure that Personal Data are processed only by persons authorised to process the Personal Data and acting under the Processor's authority. The Processor shall ensure that such persons are bound by appropriate contractual or statutory confidentiality obligations. The Processor and all such authorised persons shall maintain the confidentiality of the Personal Data and shall not use or disclose Personal Data for any purpose other than the performance of this DPA, unless required to do so by Union or Member State law.

8.2 The Processor shall ensure that any Sub-processor is bound by confidentiality obligations equivalent to those set out in this DPA, and that persons acting under the authority of any Sub-processor who are involved in the Processing are subject to appropriate confidentiality obligations.

8.3 The Processor shall promptly inform the Controller of any communication, inquiry, investigation, inspection or other contact from a competent supervisory authority relating to the Processing under this DPA. The Processor shall not respond to, represent the Controller before, or otherwise act on behalf of the Controller in dealings with supervisory authorities unless required to do so by applicable law or expressly authorised in writing by the Controller.

8.4 If the Processor receives any request, complaint or other communication from a Data Subject, supervisory authority or third party relating to the Processing of Personal Data under this DPA, the Processor shall promptly inform the Controller. The Processor shall not disclose Personal Data or other information relating to the Processing to any Data Subject, supervisory authority or third party without the

Controller's prior written authorisation, unless required to do so under applicable Union or Member State law. Where the Processor is legally required to make such disclosure, it shall, to the extent permitted by law, inform the Controller before such disclosure. The Processor shall provide reasonable assistance to the Controller in responding to such requests or communications, taking into account the nature of the Processing and the information available to the Processor.

9. Review, supervision and audit

9.1 As part of the guarantees referred to in Article 28(1) GDPR, the Processor shall, upon the Controller's request and without undue delay, make available information regarding the technical and organisational measures implemented to ensure that the Processing complies with this DPA and Article 28(3)(h) GDPR.

9.2 The Processor shall, at least annually, conduct internal reviews, assessments or audits of the security measures relating to the Processing in order to verify compliance with this DPA and applicable Data Protection Legislation. Upon request, the Processor shall make available to the Controller a summary of the results of such reviews, assessments or audits.

9.3 The Controller may, itself or through an independent third party appointed by the Controller, audit the Processor's compliance with this DPA, the Instructions and applicable Data Protection Legislation. Any third party appointed by the Controller shall not be a competitor of the Processor and shall be subject to appropriate confidentiality obligations. The Processor shall provide reasonable assistance and make available such information and documentation as are reasonably necessary to demonstrate compliance with this DPA. Audits shall be conducted upon reasonable prior written notice, during normal business hours, and in a manner that minimises disruption to the Processor's business operations and security measures. Audits under this Section 9.3 may take place once in any twelve (12) month period, unless a Personal Data Breach has occurred or a Supervisory Authority requires an audit, with at least thirty (30) days' prior written notice. Each Party bears its own costs of an audit. The Controller shall ensure that all persons conducting an audit are subject to confidentiality obligations under law or contract.

9.4 As an alternative to the audits described in Section 9.3, the Processor may satisfy the Controller's audit rights by providing independent third-party audit reports, certifications, attestations, security assessments, or other independent verification mechanisms. The Controller may rely on such reports and assessments to satisfy its audit rights under this DPA. Where reasonably necessary, the Processor shall provide additional information and reasonable assistance to enable the Controller to assess the Processor's compliance with this DPA.

9.5 Access to the Processor's premises, systems, documentation and other facilities shall be limited to the extent reasonably necessary to verify compliance with this DPA and shall be subject to the Processor's reasonable security and confidentiality requirements. The Processor may restrict such access where necessary to protect confidential information, preserve the security of its systems and services, protect the rights of other customers, or comply with legal or regulatory obligations.

9.6 The Processor shall permit competent supervisory authorities, or other public authorities having jurisdiction under applicable law, to conduct inspections or audits as required by applicable law, notwithstanding any conflicting provision of this DPA. The Processor shall inform the Controller of such inspections or audits relating to the Processing under this DPA, unless prohibited from doing so by applicable law.

9.7 The Processor shall ensure that its agreements with Sub-processors provide the Processor with sufficient audit and information rights to enable the Processor to comply with its obligations towards the Controller under this Section 9.

10. Handling of Rectification and Erasure, etc.

10.1 Where the Controller requests rectification or erasure of Personal Data due to incorrect Processing by the Processor, the Processor shall, without undue delay and taking into account the nature of the Processing and the information available to it, take appropriate measures to assist the Controller in complying with such request.

10.2 Where the Controller requests erasure of Personal Data, the Processor shall only process the relevant Personal Data to the extent necessary for the performance of such rectification or erasure and in accordance with documented Instructions from the Controller.

10.3 Where the Processor performs technical or organisational measures (including, for example, maintenance, upgrades or troubleshooting) that may affect the Processing of Personal Data, the Processor shall inform the Controller in writing in advance and within a reasonable period prior to the implementation of such measures, in accordance with the notice provisions set out in Section 18 of this DPA, unless otherwise agreed or where urgent action is required for security or operational reasons.

11. Personal Data Breaches

11.1 The Processor shall implement appropriate technical and organisational measures to ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, in accordance with Article 32(1)(c) GDPR.

11.2 The Processor shall assist the Controller, taking into account the nature of the Processing and the information available to it, in ensuring compliance with the Controller's obligations pursuant to Articles 33 and 34 GDPR and any related obligations under this DPA in relation to Personal Data Breaches.

11.3 The Processor shall notify the Controller without undue delay after becoming aware of a Personal Data Breach. Such notification shall, where possible, be provided together with, or as soon as reasonably possible thereafter, the following information:

- 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;
- the likely consequences of the Personal Data Breach; and
- the measures taken or proposed to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

11.4 Where it is not possible for the Processor to provide all information at the same time, the information may be provided in phases without undue further delay.

11.5 The Processor shall provide the Controller with reasonable assistance in the investigation, mitigation and remediation of the Personal Data Breach, including, where applicable, assistance in enabling the Controller to fulfil its obligations to notify the competent supervisory authority and Data Subjects pursuant to Articles 33 and 34 GDPR.

12. Sub-processors

12.1 The Processor shall be entitled to engage the Sub-processors listed in the "List of sub-processors" set out in the Details of Processing section of this DPA.

12.2 The Processor undertakes to enter into a written agreement with each Sub-processor governing the Processing carried out by the Sub-processor on behalf of the Controller and shall only engage Sub-processors providing sufficient guarantees to implement appropriate technical and organisational measures so that the Processing meets the requirements of Data Protection Legislation. The agreement shall impose on the Sub-processor data protection obligations equivalent to those set out in this DPA.

12.3 Where the Sub-processor's terms allow it, the Processor shall ensure that the agreement with the Sub-processor grants the Controller the right to terminate the Sub-processor's engagement and instruct the Sub-processor to, for example, delete or return Personal Data where the Processor has ceased to exist in fact or in law or has become insolvent.

12.4 The Processor shall remain fully liable to the Controller for the performance of the Sub-processor's obligations under this DPA.

12.5 The Processor shall promptly notify the Controller if a Sub-processor fails to comply with its obligations under this DPA.

12.6 The Processor shall be entitled to engage new Sub-processors and replace existing Sub-processors unless otherwise specified in the Instructions.

12.7 Prior to engaging a new Sub-processor or replacing an existing Sub-processor, the Processor shall ensure that the Sub-processor has sufficient capacity and capability to comply with its obligations under Data Protection Legislation. The Processor shall notify the Controller in writing of:

- the Sub-processor's name, company registration number, and registered seat (address and country);
- the type of Personal Data and categories of Data Subjects involved; and
- the location(s) where Personal Data will be processed.

12.8 The Controller shall be entitled to object to the engagement of a new Sub-processor within thirty (30) days from receipt of the notice referred to above and may, as a result of such objection, terminate this DPA in accordance with Section 16.5 of the DPA.

12.9 The Processor shall at all times maintain an accurate and up-to-date list of Sub-processors engaged for the Processing of Personal Data on behalf of the Controller and shall make such list available to the Controller upon request. The list shall specify the country in which each Sub-processor processes Personal Data and the types of Processing activities performed by each Sub-processor.

12.10 Where the Processor ceases to use a Sub-processor, the Processor shall notify the Controller thereof in writing. Upon termination of the relevant subcontracting relationship, the Processor shall ensure that the Sub-processor deletes or returns the Personal Data.

12.11 Upon the Controller's request, the Processor shall provide a copy of the agreement governing the Sub-processor's Processing of Personal Data and the list of Sub-processors referred to above, subject to redaction of any confidential commercial information where necessary.

13. Location and International Transfers of Personal Data

13.1 The Processor shall ensure that Personal Data are processed and stored within the EU/EEA unless otherwise agreed by the Parties in writing.

13.2 The Processor shall not transfer Personal Data to a third country or international organisation unless such transfer is carried out in compliance with Chapter V of the GDPR and in accordance with this DPA and documented Instructions from the Controller.

13.3 Where Personal Data are transferred to a third country for the purpose of Processing (including, where applicable, support, maintenance, development, hosting or similar services), such transfer shall only take place where appropriate safeguards are in place in accordance with Article 46 GDPR, including, where applicable, the European Commission's Standard Contractual Clauses or an adequacy decision under Article 45 GDPR.

13.4 The Processor shall, prior to carrying out any such transfer, ensure that the applicable transfer mechanism provides appropriate safeguards for the protection of Personal Data and that the Processing complies with the requirements set out in this DPA and applicable Data Protection Legislation.

13.5 The Processor shall make available to the Controller, upon request, information regarding the countries in which Personal Data may be processed and the transfer mechanisms used for such transfers.

13.6 Any engagement of Sub-processors involving transfers of Personal Data to third countries shall be governed by the Sub-processor provisions of this DPA, including the Controller's right to object where applicable.

14. Liability for Damage in Connection with Processing

14.1 Where a Data Subject is entitled to receive compensation for material or non-material damage pursuant to Article 82 GDPR as a result of a breach of this DPA, the Instructions, or applicable Data Protection Legislation, the Parties shall be liable in accordance with Article 82 GDPR.

14.2 Each Party shall be liable for the portion of the damage for which it is responsible. A Party shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

14.3 Where more than one Party is responsible for damage caused to a Data Subject, each Party shall be held jointly and severally liable for the entire damage, without prejudice to the right of recourse against the other Party in accordance with Article 82 GDPR.

14.4 Administrative fines imposed under Article 83 GDPR or under applicable national data protection legislation, including the Swedish Act (2018:218) containing supplementary provisions to the GDPR, shall be borne by the Party on which the fine is imposed, to the extent such allocation is permissible under applicable law.

14.5 Each Party shall promptly inform the other Party if it becomes aware of circumstances that may give rise to liability, claims, investigations or proceedings in connection with the Processing and shall cooperate in good faith to prevent, mitigate and address such claims or risks.

14.6 Liability between the Parties arising from Processing under this DPA, including recourse claims under Article 82(5) GDPR, is subject to the limitations and exclusions in Section 11 of the Main Agreement, including the Data Protection Cap in Section 11.1.2 of the Main Agreement. Nothing in this DPA or the Main Agreement limits a Party's liability towards Data Subjects under Article 82 GDPR or changes the allocation of administrative fines in Section 14.4.

15. Term and Termination

15.1 This DPA enters into force when the Main Agreement enters into force, whether or not it is signed separately, and remains in effect for as long as the Processor processes Personal Data on behalf of the Controller under the Main Agreement or until terminated in accordance with this Section.

15.2 This DPA cannot be terminated separately from the Main Agreement, except under Section 16.5. Termination of this DPA shall not affect any rights or obligations accrued prior to termination. Where the Controller terminates this DPA under Section 16.5, the Processor shall refund the prepaid fees for the period after termination of the affected Services.

15.2A Interdependency of Termination

Termination of this DPA by either Party shall automatically terminate the corresponding Services under the Main Agreement to the extent such Services involve the Processing of Personal Data governed by this DPA. Similarly, termination of the Main Agreement or the relevant Services thereunder shall automatically terminate this DPA with respect to the affected Processing activities. The Parties acknowledge that the Processor cannot perform the Services without Processing Personal Data under this DPA.

15.3 The consequences of termination of this DPA, including the return or deletion of Personal Data, shall be governed by Section 17 of this DPA.

15.4 The confidentiality, security and liability provisions which by their nature are intended to survive termination shall continue to apply in accordance with their terms.

16. Amendments, Suspension and Termination

16.1 Either Party may request renegotiation of this DPA if there is a material change in the other Party's ownership structure, or if applicable Data Protection Legislation or its interpretation changes in a manner that materially affects the Processing. Any such request for renegotiation shall not affect the continued validity of this DPA or suspend the Processing, but shall initiate good faith negotiations between the Parties.

16.2 Any amendments or additions to this DPA shall be made in writing and signed by both Parties.

16.3 Where either Party becomes aware of a material breach of this DPA or the Instructions by the other Party, it shall notify the other Party without undue delay and request that the breach be remedied within a reasonable period of time. The Parties shall cooperate in good faith to remedy such breach without undue delay.

16.4 If the breach is not remedied within a reasonable period of time, taking into account the nature and severity of the breach, the notifying Party shall be entitled to suspend the affected Processing activities to the extent strictly necessary to prevent further unlawful Processing, until the breach has been remedied.

16.5 Where the Controller has exercised its right to object to a new Sub-processor in accordance with Section 12.8 of this DPA, and no commercially reasonable alternative solution can be agreed, the Controller may terminate this DPA with respect to the affected Processing activities by giving reasonable prior written notice.

16.6 Termination under this Section shall not affect Processing carried out prior to termination and shall be without prejudice to any obligations which, by their nature, are intended to survive termination, including obligations relating to confidentiality, deletion or return of Personal Data, and liability under Article 82 GDPR.

17. Return and Deletion of Personal Data

17.1 Upon termination or expiry of this DPA, and subject to Section 15, the Processor shall, without undue delay and at the choice of the Controller, either return or delete all Personal Data processed on behalf of the Controller, unless applicable Union or Member State law requires continued storage of such Personal Data.

17.2 Where the Controller requests return of Personal Data, the Processor shall provide such Personal Data in a structured, commonly used and machine-readable format, unless otherwise agreed by the Parties.

17.3 The Processor shall ensure that all copies of the Personal Data, including copies stored in backup systems, are deleted in accordance with its standard deletion procedures and retention cycles. Where immediate deletion of backup copies is not technically feasible, such data shall be securely isolated and permanently deleted as soon as reasonably practicable.

17.4 The obligation to delete or return Personal Data shall not apply to the extent that retention is required under applicable Union or Member State law. In such cases, the Processor shall ensure that the retained Personal Data is subject to continued protection in accordance with this DPA.

17.5 Upon request, the Processor shall confirm in writing to the Controller that deletion and/or return has been completed in accordance with this Section.

17.6 Until the Personal Data has been deleted or returned, the Processor shall continue to apply the confidentiality, security, and processing restrictions set out in this DPA, but only to the extent necessary for compliance with this Section and applicable law.

17.7 Any Processing of Personal Data after the applicable retention or return obligations under this Section have been fulfilled, unless required by law, shall be considered unauthorised Processing.

18. Notices

18.1 Any notices relating to this DPA, including its administration and termination, shall be made by email or any other secure electronic means agreed between the Parties, and shall be sent to the respective contact persons designated by each Party for matters relating to this DPA.

18.2 Notices relating to data protection matters in connection with the Processing shall be sent to the Parties' designated data protection contact persons, or such other contact points as may be agreed in writing between the Parties from time to time.

18.3 Each Party shall ensure that its designated contact details are kept up to date and that the other Party is informed without undue delay of any changes to such contact details.

18.4 A notice shall be deemed received on the first business day following transmission, provided that no delivery failure notification is received by the sender. Where a delivery failure notification is received, the notice shall be deemed not delivered and shall be resent without undue delay.

19. Contact Persons

19.1 Each Party shall appoint one contact person for matters relating to this DPA.

19.2 Each Party shall appoint one contact person for data protection cooperation between the Parties.

20. Responsibility for Party Information, Contact Persons and Contact Details

20.1 Each Party shall ensure that the information set out in Section 1 of this DPA, including contact details and designated contact persons, is accurate, complete, and kept up to date throughout the term of this DPA.

20.2 Each Party shall notify the other Party without undue delay of any change to such information, including changes to contact persons or contact details, in accordance with Section 18.1 of this DPA.

21. Governing Law and Disputes

21.1 This DPA shall be governed by and construed in accordance with the governing law of the Main Agreement, including any exclusions of conflict of law rules specified therein.

21.2 Any dispute, controversy or claim arising out of or in connection with this DPA, including any question regarding its existence, validity, interpretation, performance, breach or termination, shall be resolved in accordance with the dispute resolution provisions set out in the Main Agreement.

22. Signatures of the Parties

22.1 This DPA is provided either in electronic format for electronic signature or in paper format for manual signature. In the latter case, the DPA is executed in two identical copies, of which each Party shall retain one copy.

22.2 If this DPA is signed electronically, the signature page shall be disregarded.

[The remainder of this page has been intentionally left blank. Signature page follows.]

Controller	**Processor**
[Enter the organisations full name]	Compeas AB
Org.nr	**Org.nr**
[Enter the organisations org.nr]	559590-5703
City and Date	**City and Date**
[Enter the city and date when and where the signature took place]	[Enter the city and date when and where the signature took place]
Name Clarification	**Name Clarification**
Name: [Enter contact person first- and surname]	Name: Martin Karlsson
Signature	**Signature**
[Add written signature]	[Add written signature]

Details of processing

Subject Matter	Description
Subject Matter of the Processing	The provision of the Software and related services by Compeas to Customer in accordance with the Agreement and this DPA.
Purpose of the Processing	To provide, host, operate, maintain, support, secure, and improve the Software and related services used by Customer to manage governance, risk, and compliance (GRC) activities and related compliance programs. Where Customer publishes a Trust Center through the Services, also to publish it and to receive, record and pass to Customer the access requests, subscriptions and document downloads of its visitors, on which Customer decides.
Nature of the Processing	Collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, publication of what Customer chooses to make public, hosting, support, backup, deletion, and other processing activities necessary to provide the Services.
Duration of the Processing	For the duration of the Agreement and any applicable retention period required by applicable law or this DPA.
Categories of Data Subjects	Customer employees, contractors, consultants, users, suppliers, business partners, other individuals whose Personal Data is submitted to the Services by or on behalf of Customer, and visitors to Customer's Trust Center who request access to documents, download them or subscribe to updates.
Categories of Personal Data	Names, contact information, employment information, user account information, organisational information, audit and compliance records, risk management information, usage and log data (such as IP addresses and browser details recorded in sign-in and audit logs), and other Personal Data submitted by Customer through the Services. For Trust Center visitors: name, email address, organisation, the reason given for a request, acceptance of Customer's non-disclosure agreement, which documents were downloaded and when, and the IP address, used only for the bot check and to limit repeated requests.
Special Categories of Personal Data	Customer shall not submit special categories of Personal Data unless expressly agreed in writing and appropriate safeguards have been implemented.
Processing Operations	Hosting, storage, access management, support, maintenance, security monitoring, backup, restoration, deletion, and other processing activities necessary to provide the Services.
Frequency of Processing	Continuous for the duration of the Services.
Location of Processing	European Union, via Ploi Cloud infrastructure
Sub-processors	Sub-processors engaged by Compeas and listed below in the “List of sub-processors”
Security Measures	The technical and organisational measures described in Annex C (Security & Compliance Addendum).

List of sub-processors

Compeas shall ensure that each Sub-processor is bound by written contractual obligations providing a level of protection for Personal Data that is substantially equivalent to the obligations imposed on Compeas under this DPA.

Sub-processor	Services Provided	Categories of Personal Data	Processing Location	Transfer Mechanism	Website
Ploi.cloud	Cloud hosting, application, database, and backups	Customer Data, user account information, system data, metadata	Netherlands and Sweden (EU): application and database in Amsterdam, uploaded files in Stockholm	Not applicable (EEA processing)	ploi.cloud
Google Workspace (Google Ireland Ltd)	Business email and support communications (EU-configured)	Contact details and support communications	Ireland / EU	Not applicable (EEA processing)	google.com
AhaSend (AhaSend B.V.)	Transactional email delivery (notifications, invitations, password resets)	Recipient names and email addresses, email content (not stored), delivery logs	EEA (Germany, Finland, Bulgaria, Norway, France)	Not applicable (EEA processing)	ahasend.com
Cloudflare (Cloudflare, Inc.)	Hosting of published Trust Centers (pages, document copies, access requests) and bot checks; sign-in pages and forwarding of single sign-on to the Customer's installation	Trust Center visitors' names, email addresses and companies; published documents; IP addresses and technical data	EU for stored data (D1 and R2, EU jurisdiction); Cloudflare's global edge network for requests	EU–US Data Privacy Framework and Standard Contractual Clauses (Cloudflare DPA)	cloudflare.com
Wint (Wint AB)	Billing and payment processing	Billing address, payment details	Sweden (EU)	Not applicable (EEA processing)	wint.se

Oneflow (Oneflow AB)	Electronic signing and storage of agreements	Signatories' names, email addresses and phone numbers; IP address and time of signing; personal identity number when signing with BankID	EU: agreements stored in Sweden and Ireland; invitations to sign emailed through Amazon SES in the EU	Not applicable (EEA processing)	oneflow.com

The Service is hosted on Ploi Cloud infrastructure in the European Union. The Trust Centers that Customers publish are hosted on Cloudflare, which keeps their stored data in the EU.

Google Workspace is used for business email and support communications, configured to process data within the EU. AhaSend delivers the emails that the Services send. Oneflow is used to sign agreements electronically and stores the signed agreements in the EU.

Compeas updates this list in accordance with Section 12 of this DPA, including written notice to Customer before a new Sub-processor is engaged.