Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO

zwischen

Kunde

– nachfolgend „**Verantwortlicher**" genannt –

und

Langdock GmbH, Greifswalder Str. 212, 10405 Berlin

– nachfolgend „**Auftragsverarbeiter**" genannt –

1. Vertragsgegenstand

Im Rahmen der Leistungserbringung nach den Allgemeinen Nutzungsbedingungen für die Langdock-Plattform („**Hauptvertrag**") ist es erforderlich, dass der Auftragsverarbeiter personenbezogene Daten verarbeitet, für die der Verantwortliche als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert („**Kundendaten**"). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung der Kundendaten zur Durchführung des Hauptvertrags.

2. Umfang der Beauftragung

(1) Der Auftragsverarbeiter verarbeitet die Kundendaten im Auftrag und nach Weisung des Verantwortlichen i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Verantwortliche bleibt Verantwortlicher im datenschutzrechtlichen Sinn.

(2) Die Einzelheiten der Datenverarbeitung, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die Kundendaten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anlage 1 spezifiziert.

3. Weisungen des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet die Kundendaten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen

Data Processing Agreement

Agreement for the processing of personal data on behalf of a controller pursuant to Art. 28 GDPR

between

Customer

– hereinafter referred to as the "**Controller**" –

and

Langdock GmbH, Greifswalder Str. 212, 10405 Berlin

– hereinafter referred to as "**Processor**" –

1. Subject Matter

As part of the provision of services under the General Terms of Use for the Langdock Platform ("**Main Contract**"), it is necessary for the Processor to process personal data for which the Controller acts as the data controller within the meaning of data protection regulations ("**Controller Data**"). This Agreement specifies the rights and obligations of the Parties under data protection law in connection with the processing of Controller Data for the performance of the Main Contract.

2. Scope of Data Processing

(1) The Processor shall process Controller Data on behalf of and in accordance with the instructions of the Controller within the meaning of Art. 28 GDPR. The Controller shall remain the controller within the meaning of data protection law.

(2) The details of the processing, in particular the categories of personal data and the purposes for which the Controller Data is processed on behalf of the Controller, are specified in Appendix 1.

3. Instructions by the Controller

(1) The Processor shall process the Controller Data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the Processor is subject. In this case, the Processor shall inform the Controller of that

Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

legal requirement before processing, unless the law prohibits this on important grounds of public interest.

(2) Die Weisungen des Verantwortlichen sind in diesem Vertrag festgelegt. Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus Konfigurationsoptionen innerhalb der Langdock-Plattform zur Verfügung, über die der Verantwortliche die Verarbeitung der Kundendaten im Rahmen des bestimmungsgemäßen Plattformbetriebs anpassen kann. Die Nutzung dieser Konfigurationsoptionen gilt als dokumentierte Weisung im Sinne dieses Vertrags. Darüber hinausgehende Einzelweisungen, die eine Anpassung der Standardleistung des Auftragsverarbeiters erfordern, sind nur verbindlich, soweit sie schriftlich vereinbart und im Hauptvertrag oder einem gesonderten Nachtrag dokumentiert wurden.

(2) The Controller's instructions are defined in this Agreement. In addition, the Processor makes available to the Controller configuration options within the Langdock Platform through which the Controller may customize the processing of Controller Data within the scope of the Platform's standard operation. Use of these configuration options constitutes a documented instruction within the meaning of this Agreement. Instructions going beyond the foregoing that require customization of the Processor's standard service are only binding to the extent they have been agreed in writing and documented in the Main Contract or a separate amendment.

(3) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen geltende Datenschutzbestimmungen verstoßen.

(3) The Processor shall immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringe applicable data protection law.

4. Pflichten des Verantwortlichen

4. Responsibility of the Controller

(1) Im Verhältnis der Parteien zueinander ist der Verantwortliche für die Rechtmäßigkeit der erteilten Weisungen und die Zulässigkeit der Verarbeitung der Kundendaten allein verantwortlich. Machen Dritte gegen den Auftragsverarbeiter Ansprüche im Zusammenhang mit der Verarbeitung von Kundendaten nach Maßgabe dieses Vertrags geltend, stellt der Verantwortliche den Auftragsverarbeiter von solchen Ansprüchen frei, soweit diese Ansprüche auf einem Verstoß des Verantwortlichen gegen diesen Vertrag oder anwendbares Recht beruhen.

(1) As between the Parties, the Controller is solely responsible for the lawfulness of the instructions issued and the lawfulness of the processing of Controller Data. Should any third party bring claims against the Processor in connection with the processing of Controller Data under this Agreement, the Controller shall indemnify the Processor against such claims to the extent they are based on the Controller's breach of this Agreement or applicable law.

(2) Der Verantwortliche unterstützt den Auftragsverarbeiter auf Anforderung in angemessenem Umfang bei der Erfüllung seiner datenschutzrechtlichen Pflichten, insbesondere durch Bereitstellung der erforderlichen Angaben für das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO sowie bei der

(2) Upon request, the Controller shall provide the Processor with reasonable assistance in fulfilling its data protection obligations, including by supplying information required for the Processor's records of processing activities pursuant to Art. 30 (2) GDPR and by supporting the Processor in its

Zusammenarbeit mit Aufsichtsbehörden oder sonstigen staatlichen Stellen.

cooperation with supervisory authorities or other public authorities.

5. Sicherheit der Verarbeitung

(1) Der Auftragsverarbeiter wird gemäß Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen ergreifen, die unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Kundendaten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Kundendaten zu gewährleisten.

(2) Die Parteien vereinbaren die in Anlage 3 aufgeführten technischen und organisatorischen Maßnahmen als zum Zeitpunkt des Vertragsschlusses angemessenes Schutzniveau für die Kundendaten. Dem Auftragsverarbeiter ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrags zu ändern oder anzupassen, solange sie weiterhin den gesetzlichen Anforderungen genügen und das in Anlage 3 insgesamt festgelegte Datenschutzniveau nicht unterschritten wird.

5. Security of Processing

(1) The Processor shall take appropriate technical and organizational measures in accordance with Art. 32 GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing of the Controller Data as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects, to ensure a level of security for the Controller Data appropriate to the risk.

(2) The Parties agree that the technical and organizational measures set out in Appendix 3 ensure an appropriate level of protection for the Controller Data at the time of conclusion of this Agreement. The Processor shall be permitted to change or adapt technical and organizational measures during the term of this Agreement as long as such measures continue to meet the statutory requirements and do not reduce the overall level of data protection set out in Appendix 3.

6. Anforderungen an Personal

Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der Kundendaten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

6. Requirements for Personnel

The Processor ensures that persons authorized to process the Controller Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7. Einsatz von Unterauftragsverarbeitern

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter hiermit die allgemeine Genehmigung, Unterauftragsverarbeiter bei der Verarbeitung von Kundendaten einzusetzen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter ergeben sich aus Anlage 2.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen dieser Liste durch das Hinzufügen oder Ersetzen von Unterauftragsverarbeitern mindestens 14 Tage vor dem geplanten Einsatz des neuen

7. Use of Sub-Processors

(1) The Controller hereby grants the Processor general authorization to engage sub-processors with regard to the processing of Controller Data. The sub-processors engaged at the time of the conclusion of the Agreement are set out in Appendix 2.

(2) The Processor shall inform the Controller of any intended changes with regard to the addition or replacement of sub-processors at least 14 days prior to the planned engagement of the new sub-processor. Notification shall be made by publication at

Unterauftragsverarbeiters. Die Information erfolgt durch Veröffentlichung auf https://trust.langdock.com/subprocessors sowie per E-Mail, wenn der Verantwortliche E-Mail-Benachrichtigungen auf dieser Webseite aktiviert hat. Der Verantwortliche ist berechtigt, der beabsichtigten Änderung schriftlich innerhalb von 14 Tagen nach Veröffentlichung der Änderung aus konkreten datenschutzrechtlichen Gründen zu widersprechen. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt. Im Fall eines rechtzeitigen und begründeten Widerspruchs bemühen sich die Parteien um eine einvernehmliche Lösung. Gelingt dies nicht innerhalb von 14 Tagen nach Zugang des Widerspruchs, ist jede Partei berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 30 Tagen zu kündigen.

https://trust.langdock.com/subprocessors and via email if the Controller has subscribed to email notifications on that page. The Controller is entitled to object in writing to the intended change within 14 days of publication of the change, provided that the objection is based on specific data protection grounds. If no objection is raised, the change shall be deemed approved. In the event of a timely and duly reasoned objection, the Parties shall attempt to reach a mutually agreeable solution. If no agreement is reached within 14 days of receipt of the objection, either Party shall be entitled to terminate the Main Contract and this Agreement with a notice period of 30 days.

(3) Der Auftragsverarbeiter verpflichtet die Unterauftragsverarbeiter vertraglich zur Einhaltung von Datenschutzpflichten, die dem Schutzniveau dieses Vertrags entsprechen (Art. 28 Abs. 4 DSGVO). Soweit ein Unterauftragsverarbeiter Kundendaten in einem Drittland verarbeitet, stellt der Auftragsverarbeiter sicher, dass ein geeignetes Instrument zur Gewährleistung eines angemessenen Schutzniveaus im Sinne von Art. 44 ff. DSGVO vorliegt, etwa durch die Vereinbarung von Standardvertragsklauseln gemäß Art. 46 DSGVO nach dem jeweils geltenden Muster der Europäischen Kommission.

(3) The Processor shall contractually impose on sub-processors data protection obligations that correspond to the level of protection under this Agreement (Art. 28 (4) GDPR). Where a sub-processor processes Controller Data in a third country, the Processor shall ensure that an appropriate transfer mechanism ensuring an adequate level of protection within the meaning of Art. 44 et seq. GDPR is in place, such as by entering into standard contractual clauses pursuant to Art. 46 GDPR in accordance with the applicable template of the European Commission.

(4) Der Auftragsverarbeiter ist gegenüber dem Verantwortlichen dafür verantwortlich, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt.

(4) The Processor shall remain responsible to the Controller for the performance of the sub-processor's obligations in accordance with its contract with the Processor.

8. Internationale Datenübermittlungen

8. International Data Transfers

(1) Die Verarbeitung der Kundendaten durch den Auftragsverarbeiter findet grundsätzlich innerhalb der Europäischen Union oder einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt.

(1) The processing of Controller Data by the Processor shall generally take place within the European Union or a member state of the European Economic Area (EEA).

(2) Eine Übermittlung von Kundendaten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage einer Weisung des Verantwortlichen (z.B. wenn der Verantwortliche aktiv in der Langdock-

(2) Any transfer of Controller Data by the Processor to a third country or international organization shall take place only on the basis of an instruction from the Controller (e.g., where the Controller actively enables an LLM with a server location outside the EU

Plattform ein LLM mit einem Serverstandort außerhalb der EU aktiviert) und im Einklang mit Art. 44 ff. DSGVO.

(3) Wenn Kundendaten durch den Auftragsverarbeiter oder einen Unterauftragsverarbeiter an ein Drittland oder eine internationale Organisation übermittelt oder dort verarbeitet werden, stellt der Auftragsverarbeiter sicher, dass ein geeignetes Instrument zur Gewährleistung eines angemessenen Schutzniveaus im Sinne von Art. 44 ff. DSGVO vorliegt, etwa durch die Vereinbarung von Standardvertragsklauseln gemäß Art. 46 DSGVO nach dem jeweils geltenden Muster der Europäischen Kommission.

9. Rechte der betroffenen Personen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen durch geeignete technische und organisatorische Maßnahmen im Rahmen des Zumutbaren dabei, seiner Pflicht zur Beantwortung von Anfragen betroffener Personen zur Ausübung ihrer Rechte gemäß der DSGVO nachzukommen. Zu diesem Zweck stellt der Auftragsverarbeiter dem Verantwortlichen Funktionen innerhalb der Langdock-Plattform zur Verfügung, die es dem Verantwortlichen ermöglichen, typische Betroffenenanfragen selbstständig zu erfüllen.

(2) Der Verantwortliche weist den Auftragsverarbeiter hiermit an, Anfragen betroffener Personen zur Ausübung ihrer Rechte auf (a) Berichtigung von Account- oder Profildaten sowie (b) Deaktivierung oder Löschung des Nutzerkontos und der Daten, die ausschließlich dem Nutzerkonto zugeordnet sind, eigenständig und ohne vorherige Rücksprache mit dem Verantwortlichen umzusetzen, wenn sie direkt beim Auftragsverarbeiter eingehen und die Identität der betroffenen Person mit angemessenen Mitteln verifiziert wurde (z.B. durch die dem Nutzerkonto zugeordnete E-Mail-Adresse).

in the Langdock platform) and in accordance with Art. 44 et seq. GDPR.

(3) Where Controller Data is transferred to or processed in a third country or international organization by the Processor or a sub-processor, the Processor shall ensure that an appropriate transfer mechanism ensuring an adequate level of protection within the meaning of Art. 44 et seq. GDPR is in place, such as by entering into standard contractual clauses pursuant to Art. 46 GDPR in accordance with the applicable template of the European Commission.

9. Data Subject Rights

(1) Taking into account the nature of the processing and the information available, the Processor shall assist the Controller, by appropriate technical and organizational measures to the extent reasonable, to comply with the Controller's obligation to respond to requests to exercise the rights of data subjects under the GDPR. For this purpose, the Processor shall make available to the Controller functionalities within the Langdock platform that enable the Controller to independently handle typical data subject requests.

(2) The Controller hereby instructs the Processor to implement requests from data subjects to exercise their rights regarding (a) the rectification of account or profile data and (b) the deactivation or deletion of the user account and the data exclusively associated with that user account independently and without prior consultation with the Controller, where such requests are submitted directly to the Processor and the identity of the data subject has been verified by appropriate means (e.g., through the email address associated with the user account).

(3) Soweit beim Auftragsverarbeiter eine Anfrage einer betroffenen Person zur Ausübung ihrer Rechte gemäß der DSGVO eingeht, die nicht vom Auftragsverarbeiter eigenständig bearbeitet wird (insbesondere weil sie rechtliche oder tatsächliche Fragen aufwirft oder über die in Absatz 2 genannten Standardfälle hinausgeht), leitet der Auftragsverarbeiter die Anfrage unverzüglich an den Verantwortlichen weiter. Der Auftragsverarbeiter unterstützt den Verantwortlichen in diesem Fall auf Anfrage durch geeignete technische und organisatorische Maßnahmen, soweit möglich und erforderlich, bei der Erfüllung seiner Pflichten.

(3) Where the Processor receives a request from a data subject to exercise the rights under the GDPR that is not handled by the Processor independently (in particular because it raises legal or factual questions or goes beyond the standard cases set out in paragraph 2), the Processor shall forward the request to the Controller without undue delay. Upon the Controller's request, the Processor shall in such cases assist the Controller by appropriate technical and organizational measures, insofar as reasonably possible and necessary, in fulfilling the Controller's obligations.

10. Mitteilungs- und Unterstützungspflichten des Auftragsverarbeiters

(1) Im Falle einer Verletzung des Schutzes von personenbezogenen Daten in Bezug auf Kundendaten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Die Mitteilung erfolgt auf Grundlage der dem Auftragsverarbeiter zum Zeitpunkt der Mitteilung zur Verfügung stehenden Informationen; soweit weitere relevante Informationen verfügbar werden, wird der Auftragsverarbeiter diese dem Verantwortlichen ohne unangemessene Verzögerung nachreichen.

(2) Der Auftragsverarbeiter unterstützt den Verantwortlichen auf dessen Anfrage unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen bei der Erfüllung etwaiger Melde- und Benachrichtigungspflichten nach der DSGVO, soweit die Unterstützung erforderlich und zumutbar ist. Die rechtliche Prüfung, ob und in welchem Umfang eine Melde- oder Benachrichtigungspflicht besteht, obliegt dem Verantwortlichen.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen auf dessen Anfrage unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen bei etwaigen durchzuführenden Datenschutz-Folgenabschätzungen sowie vorherigen Konsultationen von Aufsichtsbehörden, soweit die Unterstützung erforderlich und zumutbar ist. Soweit die Unterstützung einen wesentlichen, über die vertraglich

10. Notification and Support Obligations of the Processor

(1) In the event of a personal data breach affecting Controller Data, the Processor shall notify the Controller thereof without undue delay after becoming aware of the breach. The notification shall be made on the basis of the information available to the Processor at the time of the notification; to the extent that further relevant information becomes available, the Processor shall provide such information to the Controller without undue delay.

(2) Upon the Controller's request, the Processor shall, taking into account the nature of the processing and the information available to the Processor, assist the Controller in fulfilling any notification and communication obligations under the GDPR, insofar as such assistance is necessary and reasonable. The legal assessment as to whether and to what extent any notification or communication obligation exists shall remain the responsibility of the Controller.

(3) Upon the Controller's request, the Processor shall, taking into account the nature of the processing and the information available to the Processor, assist the Controller with any data protection impact assessments and prior consultations with supervisory authorities, insofar as such assistance is necessary and reasonable. To the extent that such assistance causes significant additional effort exceeding the assistance contractually owed, the Parties shall agree in

geschuldete Unterstützung hinausgehenden Mehraufwand verursacht, werden die Parteien vorab eine angemessene zusätzliche Vergütung vereinbaren.

advance on appropriate additional remuneration.

11. Datenlöschung

(1) Der Auftragsverarbeiter löscht die Kundendaten spätestens 30 Tage nach Beendigung des Hauptvertrags, sofern nicht eine gesetzliche Verpflichtung des Auftragsverarbeiters zur weiteren Speicherung der Kundendaten besteht. Der Auftragsverarbeiter bestätigt dem Verantwortlichen die Löschung der Kundendaten auf dessen Anfrage.

(2) Der Verantwortliche hat während der Laufzeit des Hauptvertrags sowie bis zur Löschung der Kundendaten gemäß Abs. 1 die Möglichkeit, seine Kundendaten zu exportieren. Der Auftragsverarbeiter stellt hierfür auf Anfrage die dafür vorgesehenen Exportfunktionen bereit.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung oder zur Erfüllung gesetzlicher Aufbewahrungspflichten dienen, darf der Auftragsverarbeiter auch nach Vertragsende aufbewahren.

11. Data Deletion

(1) The Processor shall delete the Controller Data no later than 30 days after termination of the Main Contract, unless the Processor is subject to a legal obligation to retain the Controller Data for a longer period. The Processor shall confirm deletion of the Controller Data to the Controller upon request.

(2) During the term of the Main Contract and until deletion of the Controller Data pursuant to paragraph 1, the Controller shall have the option to export its Controller Data. Upon request, the Processor shall make available the export functions provided for this purpose.

(3) Documentation that serves as proof of the proper processing of Controller Data in accordance with this Agreement or for complying with statutory retention obligations may be retained by the Processor after expiry of the Agreement.

12. Nachweise und Überprüfungen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anforderung alle Informationen zur Verfügung, die beim Auftragsverarbeiter vorhanden und erforderlich sind, um die Einhaltung der Pflichten nach diesem Vertrag sowie nach Art. 28 DSGVO nachzuweisen.

(2) Der Verantwortliche ist berechtigt, die Einhaltung der Pflichten nach diesem Vertrag sowie nach Art. 28 DSGVO durch den Auftragsverarbeiter zu überprüfen.

(3) Der Nachweis der Einhaltung der Pflichten nach diesem Vertrag sowie nach Art. 28 DSGVO erfolgt in der Regel durch Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz oder eines Prüfberichts im Rahmen einer IT-Sicherheits- oder Datenschutzzertifizierung (z.B. ISO 27001, SOC 2 Type II).

(4) Soweit der Verantwortliche einen konkreten und begründeten Verdacht auf einen

12. Verifications and Audits

(1) The Processor shall provide the Controller, at the Controller's request, with all information necessary and available to the Processor to verify compliance with its obligations under this Agreement and under Art. 28 GDPR.

(2) The Controller shall be entitled to review the Processor's compliance with its obligations under this Agreement and under Art. 28 GDPR.

(3) Compliance with the obligations under this Agreement and under Art. 28 GDPR shall, as a rule, be demonstrated by the provision of an appropriate and up-to-date attestation or report from an independent body or an audit report issued in connection with an IT security or data protection certification (e.g., ISO 27001, SOC 2 Type II).

(4) To the extent that the Controller substantiates a specific and justified

Verstoß gegen die Pflichten nach diesem Vertrag oder nach Art. 28 DSGVO darlegt, oder die nach Abs. 3 zur Verfügung gestellten Nachweise im Einzelfall keine angemessene Überprüfung ermöglichen, ist der Verantwortliche berechtigt, Inspektionen durchzuführen. Solche Inspektionen erfolgen unter angemessener Berücksichtigung der berechtigten Belange des Auftragsverarbeiters und, soweit möglich, vorrangig durch schriftliche Auskünfte oder Remote-Prüfungen.

suspicion of a breach of the obligations under this Agreement or under Art. 28 GDPR, or if the evidence provided pursuant to paragraph 3 does not permit an adequate review in the specific case, the Controller shall be entitled to conduct inspections. Such inspections shall be carried out with due regard to the Processor's legitimate interests and, where possible, primarily by way of written information or remote reviews.

(5) Inspektionen sind nur während der üblichen Geschäftszeiten des Auftragsverarbeiters und nach angemessener Vorankündigung zulässig und dürfen die Betriebsabläufe des Auftragsverarbeiters nicht unangemessen beeinträchtigen.

(5) Inspections shall only be permissible during the Processor's normal business hours and upon reasonable prior notice and shall not unreasonably interfere with the Processor's business operations.

(6) Der Auftragsverarbeiter ist berechtigt, die Offenlegung von Informationen insoweit zu beschränken, als dies erforderlich ist, um die Vertraulichkeit von Daten anderer Kunden, Sicherheitsanforderungen sowie berechtigte Betriebs- und Geschäftsgeheimnisse zu wahren. Beauftragt der Verantwortliche einen Dritten mit der Durchführung einer Inspektion, darf dieser kein Wettbewerber des Auftragsverarbeiters sein und ist vor Durchführung schriftlich auf Vertraulichkeit und Geheimhaltung zu verpflichten.

(6) The Processor shall be entitled to restrict the disclosure of information to the extent necessary to preserve the confidentiality of other customers' data, security requirements, and legitimate trade and business secrets. If the Controller appoints a third party to carry out an inspection, such third party may not be a competitor of the Processor and must be bound in writing to confidentiality and non-disclosure prior to the inspection.

13. Haftung

Im Verhältnis der Parteien zueinander gelten die Regelungen des Hauptvertrags über die Haftung entsprechend, einschließlich der Haftungsausschlüsse und -begrenzungen. Die zwingenden gesetzlichen Haftungsregelungen in Art. 82 DSGVO bleiben unberührt.

13. Liability

As between the Parties, the liability provisions of the Main Contract shall apply accordingly, including any exclusions and limitations of liability. The mandatory statutory liability provisions under Art. 82 GDPR shall remain unaffected.

14. Vertragsdauer und Kündigung

Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Die Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags; dieser Vertrag gilt jedoch bis zum Abschluss der Löschung der Kundendaten fort. Eine isolierte Kündigung dieses Vertrages ist ausgeschlossen.

14. Term and Termination

The term and termination of this Agreement shall be governed by the provisions on the term and termination of the Main Contract. Termination of the Main Contract shall automatically result in termination of this Agreement; this Agreement shall, however, remain in force until the deletion of the Controller Data has been completed. An individual termination of this Agreement is excluded.

15. Schlussbestimmungen

(1) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder

15. Final Provisions

(1) Should individual provisions of this Agreement be or become invalid or contain a

eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des Art. 28 DSGVO genügt.

gap, the remaining provisions shall remain unaffected. The Parties shall replace the invalid provision with a legally permissible provision that comes closest to the purpose of the invalid provision and meets the requirements of Art. 28 GDPR.

(2) Soweit in diesem Vertrag nichts Abweichendes geregelt ist, gelten die Bestimmungen des Hauptvertrags entsprechend, insbesondere hinsichtlich des anwendbaren Rechts und des Gerichtsstands. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

(2) Unless otherwise provided in this Agreement, the provisions of the Main Contract shall apply accordingly, in particular with regard to the governing law and jurisdiction. In the event of contradictions between this Agreement and other agreements between the Parties, in particular the Main Contract, the provisions of this Agreement shall take precedence.

(3) Nur die deutsche Fassung dieses Vertrages ist bindend. Die englische Übersetzung dient ausschließlich zu Informationszwecken.

(3) Only the German version of this Agreement shall be legally binding. The English translation is provided for information purposes only.

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung	Appendix 1: Purpose, nature, and scope of data processing
Zweck der Datenverarbeitung: Bereitstellung der Langdock-Plattform zur Nutzung von LLMs gemäß Hauptvertrag	**Purpose of data processing:** Provision of the Langdock platform for the use of LLMs according to the Main Contract
Art und Umfang der Datenverarbeitung: • Nutzerstammdaten: Namen, E-Mail-Adressen, Rollenbezeichnung und Authentifizierungsdaten von Nutzern • Inhaltsdaten: Kommunikationsinhalte mit LLMs (z.B. vom Nutzer eingegebene Chat-Nachrichten, hochgeladene Dokumente und KI-generierte Antworten) • Konfigurationsdaten: Gespeicherte Prompts, Assistenten, Workflows und Wissensdatenbanken (soweit in den Instruktionen oder Dokumenten personenbezogene Daten enthalten sind) • Nutzungsdaten: Session und User ID, nutzerbezogene Metadaten (z.B. Zeitstempel der Konversationen) • Integrationen: Personenbezogene Daten aus vom Verantwortlichen konfigurierten Integrationen mit Services von Drittanbietern, die über die Langdock-Plattform abgerufen werden	**Nature and scope of data processing:** • User account data: Names, email addresses, job titles and authentication credentials of users • Content data: Communications with LLMs (e.g., chat messages entered by users, uploaded documents and AI-generated responses) • Configuration data: Stored prompts, assistants, workflows and knowledge bases (to the extent that instructions or documents contain personal data) • Usage data: Session and user ID, user-related metadata (e.g., conversation timestamps) • Integration data: Personal data from third-party service integrations configured by the Controller and accessed via the Langdock platform
Kategorien betroffener Personen: • Mitarbeiter und sonstige Nutzer des Verantwortlichen, die Zugang zur Langdock-Plattform erhalten (zusammen „Nutzer") • Dritte, deren personenbezogene Daten vom Verantwortlichen über Dokumente, Prompts oder Integrationen in die Langdock-Plattform eingebracht werden	**Categories of data subjects:** • Employees and other users of the Controller who are granted access to the Langdock platform (collectively "Users") • Third parties whose personal data is submitted to the Langdock platform by the Controller via documents, prompts or integrations

Anlage 2:

Weitere Auftragsverarbeiter

Appendix 2:

List of authorized Sub-Processors

Unternehmen, Sitz / Company, Seat	**Zweck / Purpose**	**Art der Daten / Type of Data**	**Ort der Verarbeitung / Location of data processing**	**Transfer-mechanismus / Transfer mechanism**
Microsoft Ireland Operations Limited, Ireland	Cloud-Infrastruktur und Hosting der Langdock-Plattform / Cloud infrastructure and hosting of Langdock platform	Kundendaten / Controller Data	EU	-
Microsoft Ireland Operations Limited, Ireland	Bereitstellung von LLMs über Microsoft Azure / Provision of LLMs via Microsoft Azure	Kundendaten / Controller Data	EU	-
Amazon Web Services EMEA SARL, Luxembourg	Bereitstellung von LLMs über AWS / Provision of LLMs via AWS	Kundendaten / Controller Data	EU	-
Google Cloud EMEA Limited, Irland	Bereitstellung von LLMs über Google Cloud / Provision of LLMs via Google Cloud	Kundendaten / Controller Data	EU	-
OpenAI Ireland Limited, Ireland	Bereitstellung von LLMs über OpenAI / Provision of LLMs via OpenAI	Kundendaten / Controller Data	EU	-
Black Forest Lab Inc., USA	Bereitstellung von Bildgenerierung über Black Forest Labs / Provision of image generation via Black Forest Labs	Kundendaten / Controller Data	EU	EU SCCs, UK SCCs
Functional Software Inc. (Sentry), USA	Sammlung von Fehlermeldungen / Error tracking	IP-Adressen, MAC-Adressen / IP addresses, MAC addresses	EU	EU-U.S. Data Privacy Framework, UK Extension, Swiss-U.S. Data Privacy Framework, EU SCCs, UK SCCs, Swiss Addendum
Cloudflare Inc., USA	Schutz vor bösartigem Verkehr / Protection against malicious traffic	IP-Adressen / IP addresses	Ort des Nutzers ist Ort der Verarbeitung / Location of user is location of processing	EU-U.S. Data Privacy Framework, UK Extension, Swiss-U.S. Data Privacy Framework, EU SCCs, UK SCCs, Swiss Addendum

Die folgenden Unterauftragsverarbeiter kommen nur zum Einsatz, wenn der Verantwortliche LLMs dieser Anbieter mit “global deployment” aktiv in den Einstellungen der Langdock-Plattform auswählt. /
The following sub-processors are only used if the Controller actively chooses LLMs of these providers with “global deployment” in the settings of the Langdock platform.

Microsoft Ireland Operations Limited, Ireland	Bereitstellung von LLMs mit globaler Bereitstellung über Microsoft Azure / Provision of LLMs with global deployment via Microsoft Azure	Kundendaten / Controller Data	Speicherung in der EU, Verarbeitung (Inferenz) in anderen Microsoft-Datenzonen, einschließlich USA / Storage at rest in EU, processing (inference requests) in other Microsoft data zones, including USA	EU-U.S. Data Privacy Framework, UK Extension, Swiss-U.S. Data Privacy Framework, EU SCCs, UK SCCs
Amazon Web Services EMEA SARL, Luxembourg	Bereitstellung von LLMs mit globaler Bereitstellung über AWS / Provision of LLMs with global deployment via AWS	Kundendaten / Controller Data	Weltweit, einschließlich USA / Worldwide, including US	EU-U.S. Data Privacy Framework, UK Extension, Swiss-U.S. Data Privacy Framework, EU SCCs, UK SCCs, Swiss Addendum
Google Cloud EMEA Limited, Irland	Bereitstellung von LLMs mit globaler Bereitstellung über Google Cloud / Provision of LLMs with global deployment via Google Cloud	Kundendaten / Controller Data	Weltweit, einschließlich USA / Worldwide, including US	EU-U.S. Data Privacy Framework, UK Extension, Swiss-U.S. Data Privacy Framework, EU SCCs, UK SCCs, Swiss Addendum
OpenAI Ireland Limited, Ireland	Bereitstellung von LLMs mit globaler Bereitstellung über OpenAI / Provision of LLMs with global deployment via OpenAI	Kundendaten / Controller Data	Weltweit, einschließlich USA / Worldwide, including US	EU SCCs, UK SCCs
Black Forest Lab Inc., USA	Bereitstellung von Bildgenerierung mit globaler Bereitstellung über Black Forest Labs / Provision of image generation with global deployment via Black Forest Labs	Kundendaten / Controller Data	Weltweit, einschließlich USA / Worldwide, including US	EU SCCs, UK SCCs

Anlage 3:

Technische und organisatorische Maßnahmen des Auftragsverarbeiters

(English convenience translation below)

Die technischen und organisatorischen Maßnahmen werden von Langdock in Übereinstimmung mit Art. 32 DSGVO umgesetzt. Sie werden von Langdock entsprechend der Machbarkeit und dem Stand der Technik kontinuierlich weiterentwickelt und auf ein höheres Sicherheits- und Schutzniveau gebracht. Zu dem hohen Sicherheitsniveau tragen auch die ISO 27001 und SOC 2 Typ II-Zertifizierungen bei.

1. Vertraulichkeit

1.1 Physische Zugangskontrolle: Maßnahmen, die geeignet sind, Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Türen mit Außenknauf	Schlüsselverwaltung/-liste
Manuelle Schließsysteme	Besucher werden durch Mitarbeiter begleitet
	Sorgfältige Auswahl von Reinigungspersonal
	Informationssicherheitsrichtlinie
1.2 Logische Zugangskontrolle: *Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.*	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Logins mit Benutzernamen und sicheren Passwörtern	Verwaltung von Benutzerberechtigungen
Verschlüsselung von Endgeräten	Erstellung von Benutzerprofilen
Einsatz von Multi-Faktor-Authentifizierung (MFA)	Informationssicherheitsrichtlinie
Zero-Trust-Prinzip für administrative Systeme und kritische Komponenten	
Automatische Desktop-Sperre	
1.3 Berechtigungskontrolle: *Maßnahmen, die sicherstellen, dass die zur Nutzung eines Datenverarbeitungssystems Berechtigten nur auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten während der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.*	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	Informationssicherheitsrichtlinie
SSH-verschlüsselter Zugang	Mindestanzahl an Administratoren
Zertifizierte SSL-Verschlüsselung	Verwaltung von Benutzerrechten durch Administratoren
Rollenbasiertes Zugriffskonzept (RBAC)	Regelmäßige Überprüfung von Zugriffsberechtigungen (mindestens jährlich)
1.4 Trennungskontrolle: *Maßnahmen, die sicherstellen, dass Daten, die für unterschiedliche Zwecke erhoben wurden, getrennt verarbeitet werden können. Dies kann zum Beispiel durch eine logische und physische*	

Trennung der Daten gewährleistet werden.	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Trennung von Produktiv- und Testumgebung	Steuerung über Berechtigungskonzept
Mehrmandantenfähigkeit von relevanten Anwendungen	Festlegung von Datenbankrechten
	Informationssicherheitsrichtlinie
	Datenschutzrichtlinie
1.5 Pseudonymisierung: *Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer bestimmten betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen getrennt aufbewahrt werden und geeigneten technischen und organisatorischen Maßnahmen unterliegen.*	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Speicherung in einem separaten System (verschlüsselt)	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschungsfrist so weit wie möglich zu anonymisieren/pseudonymisieren
	Informationssicherheitsrichtlinie
	Datenschutzrichtlinie
1.6 Verschlüsselung: *Maßnahmen, die sicherzustellen, dass Daten im Ruhezustand und bei der Übertragung für Unbefugte nicht lesbar sind und kryptografische Schlüssel sicher verwaltet werden.*	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Verschlüsselung aller gespeicherten Daten im Ruhezustand (mindestens AES-256)	Richtlinie zur Datenverschlüsselung und Schlüsselverwaltung
Verschlüsselung aller Datenübertragungen (mindestens TLS 1.2)	Key-Rotation-Policy für kryptografische Schlüssel und Zertifikate
Verschlüsselung von Backups	
Zentralisiertes Secret-Management für kryptografische Schlüssel und Zertifikate	

2. Integrität

2.1 Weitergabekontrolle: *Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.*	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Protokollierung von Zugriffen und Abrufen	Übersicht über regelmäßige Abruf- und Übermittlungsverfahren
Bereitstellung über verschlüsselte Verbindungen wie https und sichere Cloudstores	Übermittlung in anonymisierter oder pseudonymisierter Form
Einsatz von Web Application Firewall (WAF)	Informationssicherheitsrichtlinie

Einsatz von E-Mail-Sicherheitslösungen, einschließlich Spam- und Malware-Filter	Datenschutzrichtlinie
Einsatz von Endpoint-Security-Software (EDR/Antivirus) mit regelmäßiger Aktualisierung	

2.2 Eingabekontrolle: *Maßnahmen, die sicherstellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder aus ihnen gelöscht worden sind. Die Eingabekontrolle erfolgt durch Protokollierung, die auf verschiedenen Ebenen (z. B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) erfolgen kann.*

Technische Maßnahmen	**Organisatorische Maßnahmen**
Nachvollziehbarkeit von Systemzugriffen und Konfigurationsänderungen über Audit-Trails	Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
Manuelle oder automatische Kontrolle der Protokolle (nach strengen internen Vorgaben)	Vergabe von Rechten zur Eingabe, Änderung und Löschung Daten auf der Grundlage eines Berechtigungskonzepts
	Klare Zuständigkeiten für Löschungen
	Informationssicherheitsrichtlinie

2.3 Entwicklungssicherheit: *Maßnahmen zur Sicherstellung der Integrität im Softwareentwicklungs- und Deployment-Prozess.*

Technische Maßnahmen	**Organisatorische Maßnahmen**
Automatisiertes Dependency Scanning mit Schwachstellenmonitoring für alle eingesetzten Komponenten	Code-Review- und Freigabe-Prozess
Infrastructure as Code mit Versionskontrolle und Protokollierung	
Automatisiertes Testing von allen sicherheitsrelevanten Komponenten	

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle: *Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (USV, Klimatisierung, Brandschutz, Datensicherung, sichere Aufbewahrung von Datenträgern, Virenschutz, Raid-Systeme, Festplattenspiegelung, usw.).*

Technische Maßnahmen	**Organisatorische Maßnahmen**
Hosting in zertifizierten Rechenzentren von Microsoft Azure mit redundanter Infrastruktur	Backup-Konzept
Verfügbarkeitsüberwachung und automatische Benachrichtigung über Anomalien bei System- und Infrastrukturkomponenten	Notfallplan
Schutz vor Überlastungsangriffen durch CDN und Bot-Management	Definierte Reaktionszeiten und Eskalationspfade bei Verfügbarkeitsunterschreitungen

3.2 Wiederherstellbarkeit: *Maßnahmen zur raschen Wiederherstellung der Verfügbarkeit von und des Zugangs zu personenbezogenen Daten im Falle eines physischen oder technischen Zwischenfalls.*

Technische Maßnahmen	Organisatorische Maßnahmen
Backup-Überwachung und Reporting	Konzept für die Wiederherstellung
Wiederherstellbarkeit durch Automatisierungstools	Kontrolle des Backup-Prozesses
Backup-Konzept gemäß Kritikalität und Kundenspezifikationen	Regelmäßige Tests der Datenwiederherstellung und Protokollierung der Ergebnisse
	Notfallplan
	Informationssicherheitsrichtlinie

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Management	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Zentrale Dokumentation aller datenschutzrechtlichen Vorgaben mit Zugang für Mitarbeiter	Externer Datenschutzbeauftragter bestellt
Eine Überprüfung der Wirksamkeit der TOM wird mindestens jährlich durchgeführt und die TOM werden aktualisiert	Geschultes und zur Vertraulichkeit/Datenschutz verpflichtetes Personal
Datenschutz-Checkpoints durchgängig in toolgestützter Risikobewertung umgesetzt	Regelmäßige, mindestens jährliche Schulungen zur Sensibilisierung der Mitarbeiter über Datenschutz und Informationssicherheit
	Datenschutz-Folgenabschätzung (DSFA) wird durchgeführt, soweit erforderlich
	Prozesse bezüglich Informationspflichten gemäß Art. 13 und 14 DSGVO umgesetzt
	Formalisiertes Verfahren für Auskunftsersuchen von betroffenen Personen eingerichtet
	Datenschutzaspekte als Teil des Risikomanagement des Unternehmens etabliert
4.2 Schwachstellenmanagement: *Proaktive Maßnahmen zur Identifikation, Bewertung und Behebung von Sicherheitsschwachstellen.*	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Automatisierte Scans auf Schwachstellen	Bug-Bounty-Programm zur koordinierten Offenlegung von Schwachstellen
Regelmäßige Penetrationstests (mindestens jährlich)	Informationssicherheitsrichtlinie mit dedizierten Meldewege und definierten Reaktionszeiten
4.3 Vorfallsreaktionsmanagement: *Unterstützung bei der Reaktion auf Sicherheitsverletzungen und Prozess bei Datenschutzverletzungen.*	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Zentralisiertes Log-Management und Security Monitoring mit automatischem Alerting bei sicherheitsrelevanten Ereignissen	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenschutzverletzungen (auch im Hinblick auf Meldepflicht an die Aufsichtsbehörde)

Echtzeit-Fehler- und Anomaliemonitoring mit automatischer Benachrichtigung über kritische Incidents	Formalisiertes Verfahren für den Umgang mit Sicherheitsvorfällen
Möglichkeit zur sofortigen Sperrung kompromittierter Nutzerkonten und Zugriffstoken	Einbindung des DSB und des CTO bei Sicherheitsvorfällen und Datenschutzverletzungen
	Dokumentation von Sicherheitsvorfällen und Datenschutzverletzungen über Ticketsystem
	Formales Verfahren zur Nachverfolgung von Sicherheitsvorfällen und Datenschutzverletzungen

4.4 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen: *Maßnahmen nach Art. 25 DSGVO zur Wahrung der Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.*

Technische Maßnahmen	**Organisatorische Maßnahmen**
Es werden nicht mehr personenbezogene Daten erhoben als für den jeweiligen Zweck erforderlich sind	Datenschutzrichtlinie (enthält die Grundsätze „Datenschutz durch Technikgestaltung/durch Voreinstellungen")
Einsatz von datenschutzfreundlichen Voreinstellungen in Standard- und Individualsoftware	Perimeteranalyse für Webanwendungen

4.5 Auftragskontrolle (Outsourcing, Unterauftragnehmer und Auftragsverarbeitung): *Maßnahmen, die sicherstellen, dass personenbezogene Daten, die im Auftrag des Kunden verarbeitet werden, nur gemäß den Anweisungen des Kunden verarbeitet werden*

Technische Maßnahmen	**Organisatorische Maßnahmen**
Überwachung des Fernzugriffs durch externe Dritte, z.B. im Rahmen des Fernsupports	Arbeitsanweisungen zum Anbietermanagement und zur Anbieterbewertung
Überwachung von Unterauftragsverarbeitern nach den Grundsätzen und mit den Technologien gemäß den vorangegangenen Kapiteln 1, 2	Sorgfältige Auswahl von Unterauftragsverarbeitern (insbesondere im Hinblick auf Datenschutz und Datensicherheit)
	Abschluss der erforderlichen Verträge zur Auftragsverarbeitung und/oder EU Standardvertragsklauseln
	Sicherstellung der Löschung von Daten nach Beendigung des Vertragsverhältnisses

5. Organisation und Datenschutz bei Langdock

Langdock hat sich in seiner Qualitäts-, Risiko- und Compliance-Richtlinie u.a. zum Ziel gesetzt, seinen Kunden die Produkte und Dienstleistungen auf dem höchstmöglichen Niveau der Informationssicherheit in Einklang mit den gesetzlichen Vorschriften bereitzustellen.

Die Mitarbeiter werden kontinuierlich im Bereich des Datenschutzes informiert und geschult. Darüber hinaus sind alle Mitarbeiter vertraglich auf den Datenschutz und die Vertraulichkeit verpflichtet. Externe Personen, die im Rahmen ihrer Tätigkeit für Langdock mit personenbezogenen Daten in Berührung kommen können, werden vor Aufnahme ihrer Tätigkeit durch ein sogenanntes NDA (Non-Disclosure Agreement) zur Geheimhaltung und Vertraulichkeit sowie zur Einhaltung des Datenschutzes verpflichtet.

Appendix 3:

Technical and Organizational Measures implemented by the Processor

(English convenience translation)

The technical and organizational measures are implemented by Langdock in accordance with Art. 32 GDPR. They are continuously improved by Langdock according to feasibility and state of the art and brought to a higher level of security and protection. The high level of security is also supported by ISO 27001 and SOC 2 Type II certifications.

1. Confidentiality

1.1 Physical Access Control: *Measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used.*	
Technical Measures	**Organizational Measures**
Doors with external handles/knobs	Key management / key register
Manual locking systems	Visitors accompanied by employees
	Care in selection of cleaning services
	Information Security Policy
1.2 Logical Access Control: *Measures suitable for preventing data processing systems from being used by unauthorized persons.*	
Technical Measures	**Organizational Measures**
Login with username + strong password	User permission management
Encryption of devices	Creating user profiles
Enforced MFA	Information Security Policy
Automatic desktop lock	
Zero-Trust principle for administrative systems and critical components	
1.3 Authorization Control: *Measures to ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.*	
Technical Measures	**Organizational Measures**
Logging of accesses to applications, specifically when entering, changing, and deleting data	Information Security Policy
SSH encrypted access	Minimum number of administrators
Certified SSL encryption	Management of user rights by administrators
Role-based access control (RBAC)	Regular review of access permissions (at least annually)
1.4 Separation Control: *Measures that ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data.*	
Technical Measures	**Organizational Measures**

Separation of productive and test environments	Control via authorization concept
Multi-tenancy of relevant applications	Determination of database rights
	Information Security Policy
	Data Protection Policy

1.5 Pseudonymization: *The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures.*

Technical Measures	**Organizational Measures**
In case of pseudonymization: separation of the mapping data and storage in separate system (encrypted)	Internal instruction to anonymize/pseudonymize personal data as far as possible in the event of disclosure or even after the statutory deletion period has expired
	Information Security Policy
	Data Protection Policy

1.6 Encryption: *Measures to ensure that data at rest and in transit cannot be read by unauthorized persons and that cryptographic keys are managed securely.*

Technical Measures	**Organizational Measures**
Encryption of all stored data at rest (minimum AES-256)	Encryption and key management policy
Encryption of all data transmissions (minimum TLS 1.2)	Key rotation policy for cryptographic keys and certificates
Encryption of backups	
Centralized secret management for cryptographic keys and certificates	

2. Integrity

2.1 Transfer Control: *Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.*

Technical Measures	**Organizational Measures**
Logging of accesses and retrievals	Survey of regular retrieval and transmission processes
Provision via encrypted connections such as https and secure cloud storage services	Transmission in anonymized or pseudonymized form
Use of Web Application Firewall (WAF)	Information Security Policy
Use of Email Security solutions, including spam and malware filters	Data Protection Policy
Use of Endpoint Security Software (EDR/Antivirus) with regular updates	

2.2 Input Control: *Measures that ensure that it is possible to check and establish retrospectively whether and by whom personal data has been entered into, modified or removed from data processing systems. Input control is achieved through logging, which can take place at various levels (e.g., operating system, network, firewall, database, application).*	
Technical Measures	**Organizational Measures**
Traceability of system accesses and configuration changes via audit trails	Traceability of data entry, modification and deletion through individual usernames (not user groups)
Manual or automated control of the logs (according to strict internal specifications)	Assignment of rights to enter, change and delete data on the basis of an authorization concept
	Clear responsibilities for deletions
	Information Security Policy
2.3 Development Security: *Measures to ensure the integrity of the software development and deployment process.*	
Technical Measures	**Organizational Measures**
Automated dependency scanning with vulnerability monitoring for all deployed components	Code review and approval process
Infrastructure as Code with version control and logging	
Automated testing of all security-relevant components	

3. Availability and Resilience

3.1 Availability Control: *Measures to ensure that personal data is protected against accidental destruction or loss (UPS, air conditioning, fire protection, data backups, secure storage of data media, virus protection, raid systems, disk mirroring, etc.).*	
Technical Measures	**Organizational Measures**
Hosting in certified data centers by Microsoft Azure with redundant infrastructure	Backup concept
Availability monitoring and automatic notification of anomalies at system and infrastructure components	Emergency response plan in place
Protection against overload attacks through CDN and bot management	Defined response times and escalation paths when availability thresholds are exceeded
3.2 Recoverability Control: *Measures capable of rapidly restoring the availability of and access to personal data in the event of a physical or technical incident.*	
Technical Measures	**Organizational Measures**
Backup monitoring and reporting	Recovery concept
Restorability supported by automation tools	Control of the backup process
Backup concept according to criticality and customer specifications	Regular testing of data recovery and logging of results
	Existence of an emergency plan

	Information Security Policy

4. Procedures for Regular Review, Assessment and Evaluation

4.1 Data Protection Management	
Technical Measures	**Organizational Measures**
Central documentation of all data protection regulations with access for employees	External data protection officer appointed
A review of the effectiveness of the TOMs is carried out at least annually and TOMs are updated	Staff trained and obliged to confidentiality/data secrecy
Data protection checkpoints consistently implemented in tool-supported risk assessment	Regular awareness trainings at least annually
	Data Protection Impact Assessment (DPIA) is carried out as required
	Processes regarding information obligations according to Art. 13 and 14 GDPR established
	Formalized process for requests for information from data subjects is in place
	Data protection aspects established as part of corporate risk management
4.2 Vulnerability Management: *Proactive measures for identifying, assessing and remediating security vulnerabilities.*	
Technical Measures	**Organizational Measures**
Automated vulnerability scans	Bug bounty program for coordinated vulnerability disclosure
Regular penetration tests (at least annually)	Information Security Policy with dedicated escalation paths and defined response times
4.3 Incident Response Management: *Support for security breach response and data breach process.*	
Technical Measures	**Organizational Measures**
Centralized log management and security monitoring with automatic alerting for security-relevant events	Documented process for detecting and reporting security incidents / data breaches (also with regard to reporting obligation to supervisory authority)
Real-time error and anomaly monitoring with automatic notification of critical incidents	Formalized procedure for handling security incidents
Ability to immediately lock compromised user accounts and access tokens	Involvement of DPO and CTO in security incidents and data breaches
	Documentation of security incidents and data breaches via ticket system
	A formal process for following up on security incidents and data breaches

	Information Security Policy
	Data Protection Policy
4.4 Data Protection by Design and by Default: *Measures pursuant to Art. 25 GDPR that comply with the principles of data protection by design and by default.*	
Technical Measures	**Organizational Measures**
No more personal data is collected than is necessary for the respective purpose	Data Protection Policy (includes principles “privacy by design / by default”)
Use of data protection-friendly default settings in standard and individual software	Perimeter analysis for web applications
4.5 Provider Control (Outsourcing, Subcontractors and Order Processing): *Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client’s instructions.*	
Technical Measures	**Organizational Measures**
Monitoring of remote access by external parties, e.g. in the context of remote support	Work instruction supplier management and supplier evaluation
Monitoring of subcontractors according to the principles and with the technologies according to the preceding chapters 1, 2	Prior review of the security measures taken by the contractor and their documentation
	Selection of the contractor under due diligence aspects (especially with regard to data protection and data security)
	Conclusion of the necessary data processing agreement on commissioned processing or EU standard contractual clauses
	Agreement on effective control rights over the contractor
	Ensuring the destruction of data after termination of the contract

5. Organization and Data Protection at Langdock

In its Quality, Risk and Compliance Policy, Langdock has set itself the goal, among other things, of providing its customers with the products and services to be delivered at the highest possible level of information security in compliance with the law.

Employees are continuously informed and trained in the area of data protection. In addition, all employees are contractually bound to data secrecy and confidentiality. External parties who may come into contact with personal data in the course of their work for Langdock are obliged to maintain secrecy and confidentiality as well as to comply with data protection and data secrecy by means of a so-called NDA (Non-Disclosure Agreement) before they begin their work.