Vertrag zur Auftragsverarbeitung

Artikel 28 DSGVO

Vertrag

zwischen

der bei Registrierung genannten Organisation

– Verantwortlicher, nachfolgend „Auftraggeber“ genannt –

und

Caya GmbH

Ritterstraße 24 - 27, 10969 Berlin

– Auftragsverarbeiter, nachfolgend „Auftragnehmer“ genannt –

Auftraggeber und Auftragnehmer jeweils einzeln als „Partei“ und gemeinsam als „Parteien“ bezeichnet.

1. Vertragsgegenstand

Data Processing Agreement

Article 28 GDPR

Agreement

between

the organization specified during registration

– Controller, hereinafter referred to as “the Client” –

and

Caya GmbH

Ritterstraße 24 - 27, 10969 Berlin

– Processor, hereinafter referred to as “the Agent” –

Client and Agent individually designated as “Party” and collectively as “Parties”.

1. Subject-matter

1.1 Im Rahmen des zwischen den Parteien bestehenden Leistungsverhältnisses über die Bereitstellung und Nutzung dieses Dienstes Caya (nachfolgend „Hauptvertrag“ genannt) ist es erforderlich, dass der Auftragnehmer als Auftragsverarbeiter i. S. d. Art. 4 Nr. 8 DSGVO mit personenbezogenen Daten umgeht, für die der Auftraggeber Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO ist (nachfolgend „Auftraggeber-Daten“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

1.1 Within the framework of the service relationship existing between the Parties regarding the provision and use of the Caya service (hereinafter referred to as the “Main Contract”), it is necessary for the Contractor, as a processor within the meaning of Art. 4 No. 8 GDPR, to handle personal data of which the Client is the controller in the meaning of Art. 4 No 7 GDPR (hereinafter referred to as “Client Data”). This Contract specifies the rights and obligations of the Parties under data protection law in connection with the Contractor’s handling of Client Data for the purpose of executing the Main Contract.

1.2 Dieser Vertrag tritt gemeinsam mit den Allgemeinen Geschäftsbedingungen automatisch mit Abschluss der Registrierung in Kraft, ohne dass eine Unterschrift erforderlich ist.

1.2 This agreement, together with the General Terms and Conditions, takes effect automatically upon completion of registration, without the need for a signature.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen, Dauer der Auftragsverarbeitung

2. Nature and purpose of the processing, nature of the personal data, categories of data subjects, duration of the processing

2.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nur nach Weisung des Auftraggebers. Der Auftraggeber bleibt gemäß Art. 5 Abs. 2 DSGVO im datenschutzrechtlichen Sinn Verantwortlicher („Herr der Daten“).

2.1 The Contractor processes the Client Data on behalf of the Client and only according to the Client’s instructions. In accordance with Art. 5 para. 2 GDPR, the Client remains the Controller within the meaning of data protection law (“master of the data”).

2.2 Die Verarbeitung der Auftraggeber-Daten im Rahmen der Auftragsverarbeitung erfolgt entsprechend den in Anlage 1 zu diesem Vertrag enthaltenen Festlegungen zu Art und Zweck der Verarbeitung. Sie bezieht sich auf die in Anlage 1 festgelegte Art der Auftraggeber-Daten und auf die dort bestimmten Kategorien betroffener Personen.

2.2 The processing of Client Data shall be performed within the scope of processing in accordance with the provisions on the type and purpose of processing contained in Annex 1 to this Contract. It relates to the type of Client Data and the categories of data subjects specified in Annex 1.

2.3 Dieser Vertrag gilt für die Dauer des Hauptvertrages.

2.3 The agreement shall be valid for the duration of the Main Contract.

2.4 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

2.4 The provision of the contractually agreed data processing takes place exclusively in a Member State of the European Union (EU) or the European Economic Area (EEA). Any relocation to a third country may only take place if the special requirements of Art. 44 et seq. GDPR is met.

3. Weisungsrechte des Auftraggebers

3. Client's rights to give instructions

3.1 Der Auftragnehmer verwendet die Auftraggeber-Daten ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers, wie sie abschließend in den Bestimmungen dieses Vertrags Ausdruck finden.

3.1 The Contractor uses the Client Data exclusively in accordance with the Client's instructions, as finally expressed in the provisions of this Contract.

3.2 Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt, wird er den Auftraggeber möglichst zeitnah darauf hinweisen. Außerdem ist der Auftragnehmer berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen.

3.2 If the Contractor is of the opinion that an instruction violates the GDPR or other data protection regulations of the EU or Member States, it shall inform the Client of this as soon as possible. In addition, the Contractor shall be entitled to hold off on the execution of the instruction until the Client confirms the instruction.

3.3 Soweit der Auftragnehmer durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist, die personenbezogenen Daten auch ohne Weisung des Auftraggebers zu verarbeiten, teilt der Auftragnehmer dem Auftraggeber die entsprechenden rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.3 If the law of the Union or of the Member States to which the Contractor is subject requires the Contractor to process personal data even without instructions from the Client, the Contractor shall notify the Client of the relevant legal requirements prior to processing, unless the law in question prohibits such notification on grounds of an important public interest.

3.4 Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers. Aufgrund der Standardisierung der Software beschränken sich Einzelweisungen im Wesentlichen auf gesondert zu vereinbarende Anpassungen der Software oder auf Datenmigrationen. Geht der Inhalt der Weisung über die Leistungen des Hauptvertrages hinaus, hat der Auftraggeber die entsprechenden Leistungen dem Auftragnehmer gesondert zu vergüten.

3.4 Individual instructions which deviate from the provisions of this Contract or which impose additional requirements shall require the prior consent of the Contractor. Due to the standardization of the software, individual instructions shall essentially be limited to software adaptations to be agreed separately or to data migrations. If the content of the instruction goes beyond the services specified in the Main Contract, the Client shall pay the Contractor separately for the corresponding services.

3.5 Sofern gegen den Auftragnehmer wegen eines Verstoßes gegen die DSGVO Ansprüche auf Zahlung von Schadenersatz gemäß Art. 82 DSGVO geltend gemacht werden, ohne dass der Auftragnehmer gegen eine vom Auftraggeber erlassene Weisung verstoßen hat, stellt der Auftraggeber den Auftragnehmer auf erstes Anfordern von allen Ansprüchen frei. Der Auftraggeber übernimmt hierbei auch die Kosten der notwendigen Rechtsverteidigung des Auftragnehmers einschließlich sämtlicher Gerichts- und Anwaltskosten. Die Freistellungspflicht gilt nicht, soweit der Schadenersatzanspruch auf die Verletzung einer speziell den Auftragsverarbeitern auferlegten Pflicht aus der DSGVO gestützt wird.

3.5 If claims for payment of damages pursuant to Art. 82 GDPR are asserted against the Contractor on account of a violation of the GDPR, without the Contractor having violated any instructions issued by the Client, the Client shall indemnify the Contractor against all claims upon first request. In this case, the Client shall also assume the costs of the necessary legal defense of the Contractor, including all court and attorney's fees. The obligation to indemnify shall not apply if the claim for damages is based on the violation of a duty arising from the GDPR that is specifically imposed on processors.

4. Pflichten des Auftraggebers

4. Duties of the Client

4.1 Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

4.1 The Client is responsible for the lawfulness of the processing of the Client's data and for the protection of the rights of the data subjects. Should third parties assert claims against the Contractor due to the processing of Client Data, the Client shall indemnify the Contractor from all such claims upon first request.

4.2 Der Auftraggeber ist Eigentümer der Auftraggeber-Daten und Inhaber aller etwaigen Rechte, die die Auftraggeber-Daten betreffen.

4.2 The Client is the owner of the Client Data and holder of any rights concerning the Client Data.

4.3 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

4.3 The Client must inform the Contractor immediately and exhaustively if the examination of the Contractor's performances reveals errors or irregularities with regard to data protection regulations or Client's instructions.

4.4 Soweit sich der Auftragnehmer gegen einen Anspruch auf Schadenersatz nach Art. 82 DSGVO, gegen ein drohendes oder bereits verhängtes Bußgeld nach Art. 83 DSGVO oder sonstige Sanktionen im Sinne des Art. 84 DSGVO mit rechtlichen Mitteln verteidigen will, erlaubt der Auftraggeber dem Auftragnehmer Details der Auftragsverarbeitung inklusive erlassener Weisungen zum Zweck der Verteidigung offenzulegen.

4.4 If the Contractor seeks to defend himself by legal means against a claim for damages under Art. 82 GDPR, against a threatened or already imposed fine under Art. 83 GDPR or other sanctions within the meaning of Art. 84 GDPR, the Client shall allow the Contractor to disclose details of the processing, including issued instructions, for the purpose of such defense.

4.5 Der Auftraggeber unterstützt den Auftragnehmer bei Kontrollen durch eine Aufsichtsbehörde, bei Ordnungswidrigkeiten- oder Strafverfahren, bei der Geltendmachung eines Haftungsanspruchs einer betroffenen Person oder eines Dritten oder bei der Geltendmachung eines anderen Anspruchs im Rahmen des Zumutbaren und Erforderlichen, soweit ein Zusammenhang mit dieser Auftragsverarbeitung besteht.

4.5 The Client shall support the Contractor in the event of inspection by a supervisory authority, in administrative offense or criminal proceedings, in the assertion of a liability claim by a data subject or a third party or in the assertion of another claim within the scope of what is reasonable and necessary, insofar as there is a connection with this processing.

5. Pflichten des Auftragnehmers

5. Duties of the Agent

5.1 Der Auftragnehmer darf ohne vorherige Zustimmung durch den Auftraggeber im Rahmen der Auftragsverarbeitung keine Kopien oder Duplikate der Auftraggeber-Daten anfertigen. Hiervon ausgenommen sind jedoch Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen gemäß dem Hauptvertrag (einschließlich der Datensicherung) erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

5.1 The Contractor may not make any copies or duplicates of the Client Data within the scope of processing without the prior consent of the Client. However, this shall not apply to copies which are necessary to ensure proper data processing and the proper provision of services in accordance with the Main Contract (including data backup), as well as copies required to comply with statutory storage obligations.

5.2 Der Auftragnehmer unterstützt den Auftraggeber bei Kontrollen durch die Aufsichtsbehörde, bei Ordnungswidrigkeiten- oder Strafverfahren, bei der Geltendmachung eines Haftungsanspruchs einer betroffenen Person oder eines Dritten oder bei der Geltendmachung eines anderen Anspruchs im Rahmen des Zumutbaren und Erforderlichen, soweit ein Zusammenhang mit dieser Auftragsverarbeitung besteht.

5.2 The Contractor shall support the Client in the event of inspections by a supervisory authority, in administrative offense or criminal proceedings, in the assertion of a liability claim by a data subject or a third party or in the assertion of another claim within the scope of what is reasonable and necessary, insofar as there is a connection with this processing.

5.3 Der Auftragnehmer hat die bei der Verarbeitung von Auftraggeber-Daten beschäftigten Personen gemäß Art. 28 Abs. 3 Satz 2 lit. b) DSGVO schriftlich auf die Vertraulichkeit zu verpflichten und sie zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut zu machen. Dies ist nicht erforderlich, wenn die bei der Verarbeitung von Auftraggeber-Daten beschäftigten Personen bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

5.3 In accordance with Art. 28 para. 3 sentence 2(b) GDPR, the Contractor must obligate the persons employed in the processing of Client Data to confidentiality in writing and must first familiarize them with the provisions on data protection relevant to them. This is not necessary if the persons employed in the processing of Client Data are already subject to an appropriate statutory duty of confidentiality.

5.4 Sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind, ist der Auftragnehmer verpflichtet, einen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis fachkundigen, für die Aufgaben nach Art. 39 DSGVO fähigen und zuverlässigen betrieblichen Datenschutzbeauftragten schriftlich zu

5.4 If and as long as the legal requirements for an appointment obligation are met, the Contractor shall be obliged to appoint in writing a reliable company data protection officer who is competent in the field of data protection law and practice, capable of performing the tasks set out in Art. 39 GDPR, and who performs his duties in accordance with Art. 38, 39 GDPR and § 38 para. 2 BDSG [Federal Data Protection Act].

benennen, der seine Tätigkeit gemäß Art. 38, 39 DSGVO und § 38 Abs. 2 BDSG ausübt.

5.5 Der Auftragnehmer unterliegt der behördlichen Aufsicht nach § 40 BDSG sowie den Bußgeld- und Strafvorschriften in § 42, 43 BDSG sowie in Art. 83 Abs. 4-6 DSGVO nach Maßgabe von § 41 BDSG.

5.6 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der nach Anlage 2 zu treffenden technischen und organisatorischen Maßnahmen im Rahmen der Kontrollrechte nach Ziffer 8 dieses Vertrages nachzuweisen.

6. Sicherheit der Verarbeitung

6.1 Der Auftragnehmer hat vor Beginn der Verarbeitung der Auftraggeber-Daten die in Anlage 2 dieses Vertrags aufgelisteten technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 Satz 2 lit. c), Art. 32 DSGVO zu implementieren und während des Vertrags aufrechtzuerhalten. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

5.5 The Contractor is subject to supervision by the authorities in accordance with § 40 BDSG as well as the provisions on administrative fines and penal provisions in § 42, 43 BDSG and in Art. 83 para. 4-6 GDPR in accordance with § 41 BDSG.

5.6 The Contractor shall ensure that the Client can confirm that the Contractor complies with Contractor's obligations under Art. 28 GDPR. The Contractor undertakes to provide the Client, upon request, with the necessary information and, in particular, to provide evidence of the implementation of the technical and organizational measures to be taken in accordance with Annex 2 within the scope of the rights of control under Clause 8 of this Contract.

6. Security in the processing

6.1 Prior to the start of the processing of Client Data, the Contractor shall implement the technical and organizational measures listed in Annex 2 of this Contract in accordance with Art. 28 para. 3 sentence 2(c), Art. 32 GDPR and maintain them during the contract. Overall, the measures to be taken are data security measures as well as measures to ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and resilience of the systems. In this context, the state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the different probabilities of occurrence and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 (1) GDPR shall be taken into account.

6.2 Da die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der technologischen Weiterentwicklung unterliegen, ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der in Anlage 2 festgelegten Maßnahmen nicht unterschritten wird. Der Auftragnehmer wird solche Änderungen dokumentieren. Wesentliche Änderungen der Maßnahmen sind vom Auftragnehmer zu dokumentieren und dem Auftraggeber zur Verfügung zu stellen.

6.2 Since the technical and organizational measures are subject to technical progress and technological development, the Contractor shall be permitted to implement alternative adequate measures, provided that they are not inferior to the security level of the measures specified in Annex 2. The Contractor shall document such changes. The Contractor shall document substantial changes to the measures and make them available to the Client.

7. Unterstützung des Auftragnehmers zur Einhaltung der Pflichten des Auftraggebers nach Art. 32 – 36 DSGVO

7. Contractor's assistance in complying with Client's obligations under Article 32 -36 GDPR

7.1 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen. Hierzu gehören

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,

b) die Unterstützung des Auftraggebers im Falle einer Verletzung des Schutzes personenbezogener Daten nach Art. 33 DSGVO,

c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht nach Art. 34 DSGVO gegenüber einem Betroffenen zu unterstützen,

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzungen i. S. d. Art. 35 DSGVO,

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde nach Art. 36 DSGVO.

7.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung des Hauptvertrages enthalten oder auf ein Fehlverhalten des Auftraggebers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

8. Kontrollrechte des Auftraggebers

7.1 Taking into account the nature of the processing and the information available to the Contractor, the Contractor shall assist the Client in complying with the obligations referred to in Articles 32 to 36 GDPR regarding the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. This includes

a) ensuring an adequate level of protection by technical and organizational measures that take into account the circumstances and purposes of the processing and the predicted probability and severity of a possible violation of law by security breaches and allow for an immediate detection of relevant breach events,

b) supporting the Client in case of a violation of the protection of personal data according to Art. 33 GDPR,

c) the obligation to support the Client within the scope of his duty to inform data subjects in accordance with Art. 34 GDPR,

d) supporting the Client with regard to his data protection impact assessments within the meaning of Art. 35 GDPR,

e) supporting the Client in the context of prior consultations with the supervisory authority in accordance with Art. 36 GDPR.

7.2 The Contractor may claim reasonable compensation for support services which are not included in the performance specification of the Main Contract or which are the result of misconduct on the part of the Client.

8. Control rights of the Client

8.1 Der Auftraggeber ist berechtigt, im Rahmen der üblichen Geschäftszeiten auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers, in denen Auftraggeber-Daten verarbeitet werden, zu betreten, um sich von der Einhaltung der aus diesem Vertrag ergebenden Pflichten, insbesondere der technischen und organisatorischen Maßnahmen gemäß Anlage 2 zu diesem Vertrag, zu überzeugen. Der Auftragnehmer weist dem Auftraggeber auf Anforderung die Umsetzung der technischen und organisatorischen Maßnahmen nach.

8.2 Der Auftragnehmer gewährt dem Auftraggeber die zur Durchführung der Kontrollen nach Ziffer 8.1 erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte.

8.3 Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des Auftraggebers, weitere Kontrollen im Fall von besonderen Vorkommnissen durchzuführen.

8.1 The Client shall be entitled to enter the business premises of the Contractor in which Client Data are processed during normal business hours at his own expense, without disrupting the business process and under strict secrecy of the business and trade secrets of the Contractor, in order to be assured of compliance with the obligations arising from this agreement, in particular the technical and organizational measures in accordance with Annex 2 to this Contract. Upon request, the Contractor shall provide the Client with evidence showing that the technical and organizational measures have been implemented.

8.2 The Contractor shall grant the Client the rights of access, information and inspection required for the performance of the controls in accordance with Clause 8.1.

8.3 The Client shall inform the Contractor in due time (as a rule, at least two weeks in advance) of all circumstances related to the performance of the control. As a rule, the Client may carry out one control per calendar year. This shall not affect the right of the Client to carry out further controls in the event of special events.

8.4 Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 8 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen.

8.4 If the Client commissions a third party to carry out the control, the Client shall obligate the third party in writing in the same way as the Client is obligated to the Contractor under Clause 8 of this Contract. In addition, the Client shall obligate the third party to maintain secrecy and confidentiality, unless the third party is subject to an occupational obligation of secrecy. At the request of the Contractor, the Client shall provide to the Contractor the obligation agreements entered into with the third party without undue delay. The Client may not commission any competitor of the Contractor to perform the control.

8.5 Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 2 anstatt einer Vor-Ort-Kontrolle auch durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren nach Art. 42 DSGVO, die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – („Prüfungsberichts“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 2 zu diesem Vertrag zu überzeugen.

8.5 At the discretion of the Contractor, proof of compliance with the technical and organizational measures in accordance with Annex 2 may - instead of by means of an on-site control - also be furnished by compliance with approved rules of conduct in accordance with Art. 40 GDPR, certification in accordance with an approved certification procedure in accordance with Art. 42 GDPR, submission of a suitable, up-to-date certificate, reports or report extracts from independent bodies (e.g. auditor, revision, data protection officer, IT security department, data protection auditors or quality auditors) or a suitable certification by IT security or data protection audit - e.g. in accordance with BSI-Grundschutz - ("audit report"), if the audit report enables the Client to confirm in a reasonable manner that the technical and organizational measures in accordance with Annex 2 to this Contract have been observed.

8.6 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen angemessenen Vergütungsanspruch geltend machen.

8.6 The Contractor can claim appropriate remuneration for enabling the Client to carry out controls.

9. Unterauftragsverhältnisse

9.1 Der Auftragnehmer darf Unterauftragsverhältnisse (Unterauftragnehmer) hinsichtlich der Verarbeitung oder Nutzung von Auftraggeber-Daten begründen. Zurzeit sind für den Auftragnehmer die in Anlage 3 mit Namen, Anschrift und Auftragsinhalt bezeichneten Unterauftragnehmer beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragnehmers. Sofern der Auftraggeber keine Einwände gegen neue Unterauftragnehmer innerhalb von 2 Wochen ab Zugang der Mitteilung über den neuen Unterauftragnehmer erhebt, gilt dessen Einschaltung als durch den Auftraggeber genehmigt. Widerspricht der Auftraggeber der Hinzuziehung oder der Ersetzung eines Unterauftragnehmers, kann der Auftragnehmer wahlweise die Leistung ohne Hinzuziehung oder Ersetzung dieses Unterauftragnehmers erbringen oder den Hauptvertrag außerordentlich kündigen. Die Kündigungsfrist beträgt 30 Tage.

9.2 Nicht als Unterauftragsverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

9. Subcontracting relationships

9.1 The Contractor may establish subcontracting relationships (subcontractors) with regard to the processing or use of Client Data. Currently, the Contractor has commissioned the subcontractors listed in Annex 3 with their names, addresses and order contents. The Client consents to their commissioning. The Contractor shall always inform the Client of any intended change with regard to the involvement or replacement of a subcontractor. If the Client does not raise any objections to new subcontractors within 2 weeks of receipt of the notification about the new subcontractor, the Client shall be deemed to have consented to the commissioning of the new subcontractor. If the Client objects to the involvement or replacement of a subcontractor, the Contractor may, at its option, perform the service without involving or replacing this subcontractor or terminate the Main Contract extraordinarily. The notice period is 30 days.

9.2 Subcontractual relationships within the meaning of this provision shall not be deemed to include services which the Contractor commissions from third parties as an ancillary service to support the performance of the order. This includes, for example, telecommunications services, maintenance and user service, cleaning staff, inspectors or the disposal of data media. However, in order to guarantee the protection and security of the Client Data, the Contractor shall be obliged to make appropriate and legally compliant contractual agreements and to take control measures to ensure that the Client Data is protected and secure, even in the case of

ancillary services commissioned from third parties.

9.3 Die Verpflichtung des Unterauftragnehmers muss schriftlich erfolgen, was auch in einem elektronischen Format erfolgen kann. Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, ob dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer stellt bei jeder Unterbeauftragung sicher, dass die in Art. 28 Abs. 2 und Abs. 4 DSGVO genannten Bedingungen eingehalten werden.

9.3 Subcontractors must be commissioned in writing, provided that electronic formats are permissible in this context. The Contractor shall carefully select the subcontractor and check before the commissioning that the subcontractor is able to comply with the agreements made between the Client and the Contractor. Whenever the Contractor commissions a subcontractor, he shall ensure that the conditions set out in Art. 28 para. 2 and para. 4 GDPR are complied with.

9.4 Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

9.4 The Contractor shall ensure that the provisions agreed to in this Contract as well as supplementary instructions of the Client, if any, shall also apply to the subcontractor.

9.5 Die Regelungen in dieser Ziffer 9 gelten auch, wenn ein Unterauftragnehmer in einem Drittstaat eingeschaltet wird. Der Auftragnehmer stellt in einem solchen Fall die datenschutzrechtliche Zulässigkeit durch geeignete Rechtsinstrumente, beispielsweise EU-Standardvertragsklauseln, sicher.

9.5 The provisions in this Clause 9 shall also apply when commissioning a subcontractor in a third country. In such a case, the Contractor shall rely on suitable legal instruments, e.g. EU standard contractual clauses, to ensure the admissibility under data protection law.

9.6 Die Weitergabe von Auftraggeber-Daten an den Unterauftragnehmer und dessen erstmaliges Tätigwerden ist erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

9.6 The disclosure of Client Data to the subcontractor and the subcontractor taking initial action are only permitted after all subcontracting requirements have been met.

10. Rechte der Betroffenen

10. Rights of data subjects

10.1 Die Rechte der durch die Datenverarbeitung betroffenen Personen nach Kapitel 3 DSGVO (Art. 12-23 DSGVO) unter Berücksichtigung von Teil 2, Kapitel 2 BDSG (§§ 32-37 BDSG), insbesondere auf Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch der gespeicherten Auftraggeber-Daten, sind gegenüber dem Auftraggeber geltend zu machen.

10.1 The rights of data subjects affected by the data processing according to Chapter 3 GDPR (Art. 12-23 GDPR) under consideration of Part 2, Chapter 2 BDSG (§§ 32-37 BDSG), in particular the rights to information, access, rectification, erasure, restriction of processing, data portability or objection with regard to the stored Client Data, must be asserted against the Client.

10.2 Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks der unter Ziffer 10.1 aufgeführten Rechte wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

10.2 If a data subject contacts the Contractor directly for the purpose of the rights listed under Clause 10.1, the Contractor shall forward this request to the Client without undue delay.

10.3 Für den Fall, dass eine betroffene Person ihre Rechte im Sinne von Ziffer 10.1 geltend macht, hat der Auftragnehmer den Auftraggeber bei der Erfüllung dieser Ansprüche angesichts der Art der Verarbeitung in angemessenem und für den Auftraggeber erforderlichen Umfang mit geeigneten technischen und organisatorischen Maßnahmen zu unterstützen.

10.3 In the event that a data subject asserts his or her rights within the meaning of Clause 10.1, the Contractor shall support the Client in the fulfillment of these claims with suitable technical and organizational measures to a reasonable extent which is necessary for the Client in view of the type of processing.

10.4 Der Auftragnehmer wird es dem Auftraggeber ermöglichen, Auftraggeber-Daten zu berichtigen, zu löschen oder zu sperren oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Löschung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

10.4 The Contractor shall enable the Client to rectify, erase or lock Client Data or, at the Client's request, carry out the rectification, locking or erasure himself if and to the extent the Client is incapable of doing so himself.

11. Rückgabe und Löschung überlassener Daten

11. Duration and termination

11.1 Der Auftraggeber kann die in der Software hinterlegten Daten jederzeit exportieren. Der Export (Download) erfolgt in einem gängigen Dateiformat (z.B. PDF). Bei Beendigung des Hauptvertrages kann der Auftraggeber die Löschung seines Accounts verlangen (danach ist kein Export mehr möglich!). Die übrigen Daten hat der Auftragnehmer nach Abschluss der Erbringung der Verarbeitungsleistungen und insbesondere nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung des Hauptvertrags) an den Auftraggeber herauszugeben oder nach Wahl des Auftraggebers datenschutzgerecht zu löschen (inkl. vorhandener Kopien). Dies gilt nicht, sofern nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Im Übrigen gelten die Bestimmungen des Hauptvertrages.

11.1 The Client may export the data stored in the software at any time. The export (download) shall be carried out in a common file format (e.g. PDF). Upon termination of the Main Contract, the Client may demand the deletion of his account (after which no more export is possible!). The Contractor shall return the remaining data to the Client after completion of the processing services and in particular after completion of the contractual performance (in particular in case of the termination or other discontinuation of the Main Contract) or, at the Client's option, erase the data in compliance with data protection laws (including existing copies). This shall not apply where there is

11.2 Den Auftragnehmer treffen keine Unterstützungspflichten bei Migration der Auftraggeber-Daten zu einem anderen Anbieter. Das Recht der betroffenen Personen auf Datenübertragbarkeit gemäß Art. 20 DSGVO wird jedoch nicht eingeschränkt.

11.2 The Contractor shall have no support obligations in the event the Client Data is migrated to another provider. However, the right of the data subjects to data portability in accordance with Art. 20 GDPR shall not be restricted.

11.3 Die Löschung von Auftraggeber-Daten ist in geeigneter Weise zu dokumentieren.

11.3 The erasure of Client Data must be documented in a suitable manner.

11.4 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, dürfen durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt werden.

11.4 The Contractor may retain beyond the end of the contract in accordance with the respective retention periods documentation which serves as evidence that the data processing complies with the order and the regulations or statutory retention periods.

12. Vertragsdauer und Kündigung

12. Term of contract and termination

Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

The term and termination of this Contract shall be governed by the provisions governing the term and termination of the Main Contract. A termination of the Main Contract automatically results in a termination of this Contract. An isolated termination of this Contract is excluded.

13. Vorrangklausel

13.1 Die Bestimmungen dieses Vertrags bleiben grundsätzlich in Kraft. Abweichend hiervon gehen jedoch individuelle Verträge zum Datenschutz, die nach dem 1. Oktober 2025 wirksam geschlossen wurden, diesem Vertrag vor, sofern sie ausdrücklich entgegenstehende Regelungen enthalten.

13.2 Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrags. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

13.3 Bei Widersprüchen zwischen verschiedenen Sprachversionen dieses Vertrags ist die deutsche Version maßgeblich.

13. Priority clause

13.1 The provisions of this agreement shall remain in effect. Notwithstanding the foregoing, individual agreements on data protection concluded after February 1, 2025, shall take precedence over this agreement to the extent that they expressly include conflicting provisions or are incompatible with this agreement.

13.2 Insofar as no special provisions are contained in this Contract, the provisions of the Main Contract shall apply. In the event of contradictions between this Contract and regulations of other agreements, in particular of the Main Contract, the regulations of this Contract shall prevail.

13.2 In the event of conflicts between different language versions of this Agreement, the German version shall prevail.

Anlagen:

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kreis der Betroffenen

Anlage 2: Technische und organisatorische Maßnahmen

Anlage 3: Unterauftragnehmer

Anlage 4: Ergänzende Bestimmungen gemäß DORA-Verordnung (EU) 2022/2554

Appendix:

Appendix 1: Nature and purpose of the processing, Type of personal data, Categories of data subjects

Appendix 2: Technical and organizational measures

Appendix 3: Subcontractors

Appendix 4: Supplementary Provisions in accordance with the DORA Regulation (EU) 2022/2554

Anlage 1: Art und Zweck der Datenverarbeitung, Art der Daten und Kategorien betroffener Personen

Art und Zweck der Datenverarbeitung:

Art und Zweck der Datenverarbeitung ergeben sich aus der Leistungsbeschreibung des vom Kunden ausgewählten Caya-Plans, die unter www.getcaya.com abrufbar ist. Die Leistungen umfassen insbesondere:

Inempfangnehmen, Öffnen und Archivieren von Briefsendungen und Dokumenten, Digitalisierung und inhaltliche Auswertung der Briefsendungen oder Dokumente sowie Mitteilung einer kurzen Information über den Inhalt der Briefsendung per E-Mail oder Push-Funktion.

„Digitalisierung“ bezeichnet das Scannen von Briefsendungen oder Dokumenten, das Speichern des Scans in einem gängigen Format (z.B. PDF) als Datei, die von Computern lesbar ist, und das Einstellen der Datei auf der Caya-Plattform.

„Auswertung“ bezeichnet die Texterkennung und inhaltliche Analyse von Briefsendungen und Dokumenten, um dem Kunden mitteilen zu können, welche Sendungen er erhalten hat und um Zusatzleistungen anbieten zu können.

Zum Auftrag gehören Hosting und Wartung der Software sowie die Archivierung von Briefsendungen.

Art der personenbezogenen Daten:

Name, Anschrift, von der Datenverarbeitung erfasste Inhalte der Briefsendungen

Kategorien betroffener Personen:

Absender von Briefsendungen an den Auftraggeber

Appendix 1: Nature and purpose of the processing, Type of personal data, Categories of data subjects

Nature and purpose of the processing:

The type and purpose of data processing are defined in the performance specification of the Caya plan selected by the Client, which can be found at www.getcaya.com. The performances include in particular:

Receipt, opening and archiving of letters and documents, digitalization and content analysis of letters or documents, and notification by means of brief information about the content of the letter by email or push function.

“Digitization” means the scanning of letters or documents, the saving of the scan in a common format (e.g. PDF) as a computer-readable file and the provision of the file on the Caya platform.

“Evaluation” refers to the text recognition and content analysis of letters and documents in order to be able to inform the Client which deliveries he has received and to be able to offer additional services.

The order includes hosting and maintenance of the software as well as the archiving of letters.

Type of personal data:

Name, address, contents of the letters recorded by the data processing

Categories of data subjects:

Senders of letters sent to the Client

Anlage 2: Technische und organisatorische Maßnahmen

Organisation

Das Unternehmen verfügt über ein Datenschutzmanagement, um sicherzustellen, dass die gesetzlichen Anforderungen adäquat umgesetzt werden.

Gewisse Datenverarbeitungen erfolgen in Rechenzentren der Amazon Web Services EMEA SARL., die über eigene technische und organisatorische Maßnahmen verfügen. Die Speicherung von Dokumenten erfolgt im Rechenzentren Frankfurt am Main, Deutschland. Das Sicherheitskonzept ist hier abrufbar: https://aws.amazon.com/de/security/.

Der Versand von E-Mails erfolgt im AWS-Rechenzentren Dublin, Irland. Das Sicherheitskonzept ist hier abrufbar: https://aws.amazon.com/de/compliance/eu-data-protection/.

Die Archivierung und Digitalisierung der Briefpost erfolgt durch spezialisierte Dienstleister, die über eigene technische und organisatorische Maßnahmen verfügen. Die Sicherheitskonzepte sind nicht öffentlich einsehbar, gerne gewähren wir Ihnen auf Anfrage Einsicht.

Im Übrigen gelten die nachfolgenden Festlegungen:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO) und Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)

Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

Appendix 2: Technical and organizational measures

Organization

The company has a data protection management system to ensure that legal requirements are adequately implemented.

Certain data processing takes place in data centers of Amazon Web Services, Inc., which have their own technical and organizational measures. Documents are stored in data centers in Frankfurt am Main, Germany.

The security concept is available here: https://aws.amazon.com/de/security/.

Email is sent from the AWS data centers in Dublin, Ireland. The security concept is available here:

https://aws.amazon.com/de/compliance/eu-data-protection/.

The archiving and digitization of letters is carried out by specialized service providers who have their own technical and organizational measures. The security concepts are not shared with the public. We will be happy to allow you to inspect them upon request.

In all other respects, the following provisions shall apply:

1. Confidentiality (Article 32 (1) Point b GDPR) and Encryption (Article 32 (1) Point a GDPR)

Physical Access Control

No unauthorized access to Data Processing Facilities:

Geschäftsräume der Caya GmbH:

- Eingangstüren werden stets verschlossen gehalten.
- Schlüsselverzeichnis
- Besucher werden begleitet bzw. abgeholt und werden in den Geschäftsräumen stets beaufsichtigt.

Business premises of Caya GmbH:

- Entrance doors remain locked at all times.
- Key directory
- Visitors are accompanied or picked up and are always supervised while on business premises.

Zugangskontrolle/Verschlüsselung

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

- Jeder Berechtigte verfügt über einen eigenen Zugang zu Datenverarbeitungssystemen.

- Zugangsberechtigungen werden dokumentiert.

- Zugang zu IT-Systemen, die Zugriff auf Kundendokumente haben, sind nur mit Zwei-Faktor-Authentifizierung (Passwort + mobiles Gerät) möglich.

- IT-Systeme werden bei wiederholtem erfolglosem Anmeldeversuch automatisch gesperrt.

- Bildschirmsperre an Arbeitsstationen, automatische Sperrung bei längerer Abwesenheit.

- Passwortrichtlinie

Electronic Access Control/Encryption

No unauthorized use of the Data Processing and Data Storage Systems:

- Each authorized person has their own access to data processing systems.

- Access authorizations are documented.

- Access to IT systems that have access to Client documents requires two-factor

- authentication (password + mobile device).

- IT systems are automatically locked if a repeated unsuccessful login attempt is made.

- Screen lock at workstations, automatic lock during longer absence.

- Password policy

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

Internal Access Control

No unauthorized Reading, Copying, Changes or Deletions of Data within the system:

- Individuelle Zugriffsrechte für jeden einzelnen Benutzer (in einem schriftlichen Berechtigungskonzept dokumentiert), zentrale Verwaltung und Steuerung.

- Zugriffsberechtigungen werden aufgabenbezogen und nach dem Need-to-know-Prinzip erteilt.

- Entwicklerzugänge, die Zugriff auf Rohdaten über Komponenten (beispielsweise Datenbanken) ermöglichen, sind auf das erforderliche Maß beschränkt. Einen Zugriff auf das Kundensystem hat nur der CTO. Alle anderen Entwickler können ausschließlich auf Testsysteme Zugreifen. Entwicklerzugänge sind grundsätzlich mit Zwei-Faktor-Authentifizierung geschützt.

- Regelmäßige Überprüfung der Zugriffsberechtigungen. Nicht mehr erforderliche Berechtigungen (Versetzung, Ausscheiden eines Mitarbeiters) werden unverzüglich entzogen, Zugänge zum IT-System werden gesperrt.

Trennungskontrolle/Zweckbindungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Verteilung der Systeme auf unterschiedliche Ausführungscontainer. Jeder Container hat nur Zugriff auf den Teil des Systems, den er braucht.

- Trennung von Produktiv- und Testsystemen

2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

- Individual access rights for every single user (documented in a written authorization concept),

- central administration and control.

- Access authorizations are granted on a task-related basis and according to the need-to-know principle.

- Developer access to raw data via components (e.g. databases) is limited to the necessary extent. Only

- The CTO has access to the Client system. All other developers can only access test systems. Developer

- accesses are generally protected with two-factor authentication.

- Regular checking of access permissions. Authorizations no longer required

- (transfer, departure of an employee) are immediately withdrawn, accesses to IT systems are locked.

Isolation Control

The isolated Processing of Data, which is collected for differing purposes:

- Allocation of the systems to different execution containers. Each container has access only to the part of the system it needs.

- Separation of production and test systems

2. Integrity (Article 32 (1) Point b GDPR)

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 entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Übermittlungen personenbezogener Daten sind in Verfahrensübersicht dokumentiert.

- Datenspeicherung und -verarbeitung erfolgt auf IT-Systemen im Rechenzentrum. Die Verbindung zwischen Clients und Server ist besonders gesichert (SSL-Verschlüsselung).

- Mitbringen und verwenden privater Datenträger ist untersagt. Es dürfen nur verschlüsselte betriebliche Datenträger genutzt werden.

- Das Kopieren von personenbezogenen Daten auf mobile Datenträger ist bedarf der Freigabe durch den CTO, sowie der Dokumentation. Diese wird nur in Ausnahmefällen, beispielsweise bei Gefahr des Datenverlustes, gewährt.

- Kontrollierte Vernichtung von Dokumenten und Datenträgern mit Protokollierung durch zertifizierte Entsorger.

- Besucher haben keinen Zugriff auf betriebliche Netzwerke.

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

Data Transfer Control

No unauthorized Reading, Copying, Changes or Deletions of Data with electronic transfer or transport:

- The transmission of personal data is documented in the procedure overview.

- Data storage and processing takes place on IT systems in the data center. The connection between clients and servers is specially secured (SSL encryption).

- The provision and use of private data media is prohibited. Only encrypted company data media may be used.

- The copying of personal data to mobile data media requires the approval of the CTO and must be documented. This is only granted in exceptional cases, for example, if there is a risk of data loss.

- Controlled destruction of documents and data media with logging by certified disposal companies.

- Visitors have no access to company networks.

Data Entry Control

Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted:

- Protokollierung der Dateneingabe, Änderung oder Löschung.

- Protokollierung aller Aktivitäten auf dem Server.

- Sicherung der Protokolldaten gegen Verlust oder Veränderung.

- Dokumentation der Eingabeprogramme.

- Logging of data entry, alteration or deletion.

- Logging of all activity on the server.

- Backup of log data to protect against loss or alteration.

- Documentation of the input programs.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO), rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c) DSGVO

3. Availability and Resilience (Article 32 (1) Point b GDPR), Rapid Recovery (Article 32 (1) Point c GDPR)

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (die Angaben beziehen sich auf eigene IT-Systeme des Auftragnehmers):

Availability Control

Prevention of accidental or wilful destruction or loss

- IT-Sicherheitskonzept.

- Versionierte Daten- und Systembackups nach Backup-Plan.

- Backup auf dafür vorgesehenen redundanten Systemen im Rechenzentrum.

- Lösch / Änderungsversuche werden auf Auffälligkeiten kontrolliert und automatisch gemeldet.

- Unterbrechungsfreie Stromversorgung im Rechenzentrum.

- IT security concept

- Versioned data and system backups according to backup plan

- Backup on dedicated redundant systems in the data center.

- Deletion / alteration attempts are checked for anomalies and automatically reported.

- Uninterruptible power supply in the data center

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO, Art. 25 Abs. 1 DSGVO)

4. Procedures for regular testing, assessment and evaluation (Article 32 (1) Point d GDPR; Article 25 (1) GDPR)

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den

Order or Contract Control

No third party data processing as per Article 28 GDPR without corresponding instructions from the Client:

Weisungen des Auftraggebers verarbeitet werden können:

- Auftragnehmer werden sorgfältig ausgesucht.

- Vertragliche Regelung zur Datenverarbeitung mit Dienstleistern (gemäß Art. 28 DSGVO) mit Festlegung der Weisungsbefugnisse des Auftraggebers.

- Formalisierte Weisungen

- Kontrolle des Auftragnehmers durch die Geschäftsführung oder den Datenschutzbeauftragten.

Datenschutz-Management

Maßnahmen, die eine Steuerung der Datenschutzprozesse ermöglichen und die Einhaltung der datenschutzrechtlichen Vorgaben nachweisbar sicherstellen:

- Es gibt ein dokumentiertes Datenschutz-Management-System

- Alle Beschäftigten wurden auf die Vertraulichkeit von Daten verpflichtet.

- Regelmäßige Schulungen und Sensibilisierungen im Datenschutz für Beschäftigte.

- Personengebundene Datenverarbeitungen sind in Verfahrensbeschreibungen dokumentiert.

- Es wurde eine fachkundige Person zum betrieblichen Datenschutzbeauftragten benannt: Rechtsanwalt Sebastian Herting, zertifizierter Datenschutzbeauftragter (TÜV) E-Mail: datenschutz@getcaya.com, Telefon 040-228691140.

- Contractors are carefully selected.

- Contractual regulation for data processing with service providers (in accordance with Art. 28 GDPR)

- including specification of the Client's authority to issue instructions.

- Formalized instructions

- Control of the Contractor by the Management or the data protection officer.

Data Protection Management

Control of data protection measures and compliance with data protection regulations in a verifiable manner:

- A documented data protection management system is in place

- All employees have been bound to maintain confidentiality of data.

- Regular data protection training and sensitization for/of employees.

- Personal data processing is documented in process descriptions.

- An expert has been appointed as the company's data protection officer: Attorney Sebastian Herting, Certified Data Protection Officer (TÜV) Email: datenschutz@getcaya.com, Phone: 040-228691140.

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a) DSGVO, Art. 25 Abs. 1 DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten in einer Weise verarbeitet werden, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

5. Pseudonymisation (Article 32 (1) Point a GDPR, Article 25 (1) GDPR)

The processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organizational measures.

Anlage 3: Unterauftragnehmer **Appendix 3: Subcontractors**

Name **name**	**Anschrift/Land address/country**	**Auftragsinhalt** **subject-matter/service:**
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy 99137 Luxemburg Luxemburg	Hosting der Daten (ausschließlich im Frankfurter Serverzentrum) Data hosting (exclusively at the Frankfurt server center)
Satz-Rechen-Zentrum Hartmann + Heenemann GmbH & Co. KG	Bessemerstr. 83–91 12103 Berlin Deutschland	Digitalisierung von Dokumenten Digitization of documents
SPS Germany GmbH	Am Börstig 5 96052 Bamberg Deutschland	Digitalisierung von Dokumenten Digitization of documents
Rhenus Archiv Services GmbH	Rhenus Platz 1 59439 Holzwickede Deutschland	Archivierung von Dokumenten Archiving of documents
Workato, Inc.	215 Castro Street Suite 300 Mountain View CA 94041 USA	Automatisierung von Workflows Workflow automation
natif.ai GmbH	Campus Starterzentrum Gebäude A1 1 66123 Saarbrücken	Datenextraktion (Hosting in Deutschland) Data extraction (Hosting in Germany)

Anlage 4: Ergänzende Bestimmungen gemäß DORA-Verordnung (EU) 2022/2554

Anwendungsbereich

Diese Regelungen gelten ergänzend zur Vereinbarung zur Auftragsverarbeitung, sofern der Auftraggeber unter den Anwendungsbereich der Verordnung (EU) 2022/2554 („DORA“) fällt und die von Caya erbrachten Leistungen im konkreten Fall als IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen im Sinne von DORA genutzt werden.

In diesem Fall gelten die nachfolgenden Regelungen als Ergänzung zur bestehenden Vereinbarung zur Auftragsverarbeitung.

1. Dienstleistungsumfang, Leistungsniveaus und Änderungsmanagement

Die im Hauptvertrag sowie in dieser Vereinbarung definierten Pflichten, Leistungen, Supportprozesse und Informationspflichten gelten auch im Hinblick auf die Verordnung (EU) 2022/2554 („DORA“), sofern der Auftraggeber deren Anwendungsbereich unterfällt.

Caya behält sich Änderungen an Funktionen und der technischen Infrastruktur vor, sofern diese keine wesentliche Beeinträchtigung der Sicherheit oder Verfügbarkeit der vereinbarten Leistungen darstellen. Sobald es für DORA regulatorisch erforderlich oder inhaltlich geboten wird, wird Caya den Auftraggeber über relevante Änderungen in geeigneter Weise informieren.

2. Unterauftragsvergabe

Caya informiert den Auftraggeber in angemessener Weise über wesentliche Änderungen bei der Beauftragung von Unterauftragnehmern, soweit diese Änderungen für die Verarbeitung personenbezogener Daten im Rahmen der

Appendix 4: Supplementary provisions in accordance with the DORA Regulation (EU) 2022/2554

Scope

These provisions apply in addition to the agreement on order processing if the customer falls within the scope of Regulation (EU) 2022/2554 ("DORA") and the services provided by Caya are used in the specific case as ICT services to support critical or important functions within the meaning of DORA.

In this case, the following provisions apply as a supplement to the existing agreement on order processing.

1. Scope of services, service levels and change management

The obligations, services, support processes, and information duties defined in the main agreement and in this agreement also apply with regard to Regulation (EU) 2022/2554 ("DORA"), provided that the client falls within its scope.

Caya reserves the right to make changes to functions and the technical infrastructure, provided that these do not represent a significant impairment of the security or availability of the agreed services. As soon as it becomes regulatorily necessary or substantively appropriate for DORA, Caya will inform the client of relevant changes in an appropriate manner.

2. Subcontracting

Caya will inform the client in an appropriate manner about significant changes in the engagement of subcontractors, insofar as these changes are substantial for the processing of personal data within the scope of the agreed services. The client may, in a justified individual

vereinbarten Leistungen erheblich sind. Der Auftraggeber kann im begründeten Einzelfall Bedenken gegenüber der Änderung äußern. Die Parteien werden in einem solchen Fall gemeinsam eine angemessene Lösung anstreben.

Sofern der Auftraggeber aufgrund regulatorischer Vorgaben – insbesondere im Anwendungsbereich der Verordnung (EU) 2022/2554 (DORA) – verpflichtet ist, kritische oder wichtige Funktionen besonders abzusichern, kann er innerhalb von 10 Werktagen nach Zugang der Mitteilung der Änderung aus berechtigten Gründen widersprechen. Caya hat anschließend 10 Tage die Möglichkeit, eine Einigung hinsichtlich der Änderung zu erzielen oder diese rückgängig zu machen. Wird keine Einigung erzielt, sind beide Parteien berechtigt, die betroffenen Leistungen außerordentlich zu kündigen.

Weitere vertragliche Rechte bleiben unberührt.

3. Ort der Leistungserbringung und Datenverarbeitung

Die in Anlage 1 und Anlage 2 definierten Datenverarbeitungsorte und Sicherheitsmaßnahmen gelten fort.

Caya gewährleistet jederzeit ein angemessenes Schutzniveau für personenbezogene Daten gemäß den Anforderungen der DSGVO sowie – soweit anwendbar – der Verordnung (EU) 2022/2554 (DORA).

Der Auftraggeber trägt die Verantwortung, regulatorische Anforderungen – insbesondere aus DORA – selbst zu bewerten und etwaige Informations- oder Mitwirkungspflichten gegenüber Caya im Einzelfall anzuzeigen.

Caya stellt dem Auftraggeber auf Anfrage die Informationen zur Verfügung, die zur Erfüllung gesetzlicher oder aufsichtsrechtlicher Pflichten im Zusammenhang mit der Leistungserbringung erforderlich sind.

case, raise concerns regarding the change. In such a case, the parties will jointly strive for a reasonable solution.

If the client is obliged, due to regulatory requirements – especially within the scope of Regulation (EU) 2022/2554 (DORA) – to specifically secure critical or important functions, they may object for legitimate reasons within 10 business days of receiving the notification of the change. Caya then has 10 days to reach an agreement regarding the change or to reverse it. If no agreement is reached, both parties are entitled to extraordinarily terminate the affected services.

Further contractual rights remain unaffected.

3. Location of Service Provision and Data Processing

The data processing locations and security measures defined in Appendix 1 and Appendix 2 remain in effect.

Caya guarantees an appropriate level of protection for personal data at all times, in accordance with the requirements of the GDPR and – where applicable – Regulation (EU) 2022/2554 (DORA).

The client bears the responsibility to assess regulatory requirements – particularly those stemming from DORA – themselves and to indicate any information or cooperation obligations towards Caya in individual cases.

Caya will provide the client, upon request, with the information necessary to fulfill legal or supervisory obligations related to the service provision.

4. IKT-Vorfallmanagement

Ein IKT-bezogener Vorfall im Sinne von DORA wird von Caya wie eine Datenschutzverletzung gemäß Artikel 33 DSGVO behandelt. Die Meldepflichten und Unterstützungsleistungen im Rahmen des AVV (insb. Ziff. 7.1 lit. b und c) gelten entsprechend. Caya unterstützt den Auftraggeber auf Anfrage bei der Wiederherstellung der Dienste und – soweit gesetzlich erforderlich – bei der Erfüllung von regulatorischen Meldepflichten im Zusammenhang mit IKT-Vorfällen.

5. Prüfungsrechte und behördliche Unterstützung

Der Auftraggeber ist berechtigt, nach vorheriger Abstimmung mit Caya eine Prüfung durchzuführen oder durchführen zu lassen, um die Einhaltung der vertraglich vereinbarten Sicherheitsmaßnahmen zu verifizieren.

Prüfungen sind mit einer angemessenen Vorankündigungsfrist von mindestens 30 Kalendertagen anzumelden und dürfen den Geschäftsbetrieb von Caya nicht unangemessen beeinträchtigen.

Caya stellt auf Anfrage geeignete Nachweise zur Verfügung (z. B. Auditberichte, Zertifikate, technische Unterlagen), die eine angemessene Prüfung ermöglichen.

Soweit gesetzlich erforderlich, gewährt Caya Aufsichtsbehörden Zugang zu den relevanten Informationen und Systemen auch seiner Unterauftragnehmer.

6. Schulung und Sensibilisierung

Caya führt regelmäßig Schulungen zu den geltenden Sicherheits- und Datenschutzrichtlinien durch. Ein separater Schulungsaufwand beim Auftraggeber ist nicht erforderlich.

Auf Anfrage gibt Caya Auskunft über Umfang und Inhalte der durchgeführten Schulungen,

4. ICT Incident Management

An ICT-related incident within the meaning of DORA will be treated by Caya as a data breach pursuant to Article 33 GDPR. The reporting obligations and support services within the framework of the DPA (Data Processing Agreement) (especially sections 7.1 lit. b and c) apply accordingly. Caya will support the client upon request in restoring services and – to the extent legally required – in fulfilling regulatory reporting obligations related to ICT incidents.

5. Audit Rights and Regulatory Assistance

The client is entitled, after prior consultation with Caya, to conduct or have conducted an audit to verify compliance with the contractually agreed security measures.

Audits must be announced with a reasonable notice period of at least 30 calendar days and must not unreasonably impair Caya's business operations.

Caya will provide suitable evidence upon request (e.g., audit reports, certificates, technical documents) that enable an appropriate audit.

To the extent legally required, Caya will grant supervisory authorities access to the relevant information and systems, including those of its subcontractors.

6. Training and Awareness

Caya regularly conducts training on the applicable security and data protection policies. Separate training efforts on the client's part are not required.

Upon request, Caya will provide information on the scope and content of the training

soweit dies zur Erfüllung gesetzlicher Prüfpflichten erforderlich ist.

7. Exit-Strategie und Übergang

Bei Beendigung des Hauptvertrages stellt Caya dem Auftraggeber auf Anfrage angemessene Übergangsunterstützung zur Verfügung, um einen reibungslosen Wechsel zu einem anderen Anbieter zu ermöglichen. Die Einzelheiten der Übergangsleistungen richten sich nach den vertraglich vereinbarten Bedingungen; etwaige darüber hinausgehende Unterstützungsleistungen werden gesondert vergütet.

conducted, insofar as this is necessary for the fulfillment of legal audit obligations.

7. Exit Strategy and Transition

Upon termination of the main contract, Caya will provide the client with reasonable transition support upon request to enable a smooth transfer to another provider. The details of the transition services will be governed by the contractually agreed terms; any additional support services beyond that will be remunerated separately.