Allgemeine Geschäftsbedingungen zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO als Anlage zu einem oder mehreren vom Auftraggeber genutzten Vertrag oder Verträgen

Präambel

Diese Anlage (im Folgenden „AV-Vertrag“ genannt) konkretisiert die Verpflichtungen zum Datenschutz, die sich aus einem vom Auftraggeber genutzten Dienstleistungsvertrag (nachstehend „Vertrag“ oder „Hauptvertrag“ genannt) ergeben. Der AV-Vertrag findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen personenbezogene Daten (nachfolgend „Daten“ genannt) durch den Auftragnehmer oder durch den vom Auftragnehmer Beauftragten verarbeitet werden.

Dieser AV-Vertrag trägt Art. 28 Abs. 3 DSGVO (Datenschutzgrundverordnung) Rechnung, nach dem jedes Unternehmen, das Daten im Auftrag verarbeiten lässt, einen Vertrag oder ein anderweitiges Rechtsinstrument nutzen muss, um die Verarbeitung von Daten zu regeln. Es sind speziell Vereinbarungen zu den Verantwortlichkeiten, dem Gegenstand und der Dauer der Verarbeitung, Art und Zweck der Verarbeitung, der Art der verarbeiteten Daten sowie den Rechten und Pflichten der Vertragsparteien zu treffen.

Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Textform nach § 126 b BGB gemeint, zu deren Wirksamkeit auch eine E-Mail genügt.

Der vorliegende AV-Vertrag ist nur gültig in Verbindung mit einem aktiven Dienstleistungsvertrag mit der cituro GmbH zur Nutzung von cituro.

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Auftragnehmer ist der Hersteller und Betreiber von cituro:

cituro GmbH
Peter-Dörfler-Straße 30
86199 Augsburg

Tel: (+49) 821 9997 3940

(2) Gegenstand der Vereinbarung sind die Rechte und Pflichten des Auftragnehmers und seiner Kunden (Auftraggeber) im Rahmen der Leistungserbringung gemäß der Leistungsbeschreibung des Hauptvertrags, soweit eine Auftragsverarbeitung von personenbezogenen Daten durch den Auftragnehmer gemäß Art. 28 DSGVO erfolgt. Dies umfasst alle Tätigkeiten, die der Auftragnehmer im Rahmen dieser

Auftragsverarbeitung, durchführt. Dies gilt auch, sofern der Vertrag nicht ausdrücklich auf diese Vereinbarung zur Auftragsverarbeitung verweist.

(3) Die Dauer der Verarbeitung richtet sich nach der Dauer und der Laufzeit des Hauptvertrags.

§ 2 Art und Zweck der Verarbeitung

(1) Die Art der Verarbeitung umfasst alle Arten von Verarbeitung im Sinne der DSGVO zur Erfüllung des Hauptvertrags.

(2) Zweck der Verarbeitung sind alle, zur Erbringung der im Hauptvertrag vereinbarten Leistungen, insbesondere der Online-Terminbuchung, Online-Terminplanung und dem IT-Support, erforderlichen Zwecke.

§ 3 Art der personenbezogenen Daten und Kategorien von Betroffenen

(1) Die Art der verarbeiteten personenbezogenen Daten wird vom Auftraggeber, durch die Konfiguration des cituro Accounts, festgelegt.

(2) Die Art der personenbezogenen Daten umfasst in der Regel:

a. Personenstammdaten, also Daten über Namen, Anschrift der Kunden oder andere persönliche Informationen zu der Person
b. Kontaktdaten wie Telefonnummern und E-Mail-Adressen
c. Sonstige für Termine erforderliche Informationen, die vom jeweiligen Auftraggeber festgelegt werden können (Bspw. Alter, Kfz-Kennzeichen, o.Ä.)

(3) Die Kategorien betroffener Personen umfassen Kunden, Interessenten und Mitarbeiter des Auftraggebers, die dessen durch den Auftragnehmer zur Verfügung gestellte Online Terminbuchung nutzen oder manuell erfasst wurden, Anwender der cituro Administratorenanwendung, also Mitarbeiter oder Beauftragte des Auftraggebers und Mitarbeiter des Auftraggebers, die in cituro verwaltet werden.

§ 4 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen schriftlich. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich schriftlich bestätigen.

(2) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme und -prozesse vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer, soweit erforderlich, Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Kontrollen finden grundsätzlich nach angemessener Vorankündigung, nach Unterzeichnung einer entsprechenden Verschwiegenheitserklärung und zu den üblichen Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten

Datenschutzpflichten dieses Vertrages wie vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen.

(3) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (Verantwortlicher im Sinne Art. 4 Nr. 7 DSGVO).
(4) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
(5) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung hat auch nach Beendigung des Hauptvertrags Bestand.

§ 5 Weisungen

(1) Die Weisungen werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form, oder in einem elektronischen Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Insbesondere wird der Auftragnehmer nur nach dokumentierter Weisung des Auftraggebers Daten, die im Auftrag verarbeitet werden, berichtigen, löschen oder deren Verarbeitung einschränken.
(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich schriftlich.
(3) Der Auftraggeber kann einzelne zur Weisung befugte Personen benennen.
(4) Weisungsempfänger sind Supportmitarbeiter des Auftragnehmers.
(5) Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich die Nachfolger bzw. die Vertreter mitzuteilen.
(6) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis diese durch den Verantwortlichen beim Auftraggeber entsprechend geändert wird oder die rechtliche Zulässigkeit der Weisung nachgewiesen wird.
(7) Rechtswidrige Weisungen wird der Auftragnehmer ablehnen.

§ 6 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.
(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.
(4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.
(5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.
(6) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.
(7) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in Art. 32 – 36 DSGVO geregelten Pflichten zur Sicherheit der Verarbeitung, Meldung bei Verletzungen des Schutzes personenbezogener Daten und Datenschutzfolgeabschätzung im erforderlichen Umfang, insbesondere im Falle einer Kontrolle des Auftraggebers durch Aufsichtsbehörden oder andere Stellen oder einer Geltendmachung von Rechten betroffener Personen, soweit die Verarbeitung im Auftrag betroffen ist.
(8) Der Auftragnehmer ist gemäß Art. 33 Abs. 2 DSGVO verpflichtet, dem Auftraggeber jedwede Verletzung des Schutzes personenbezogener Daten, die im Rahmen des vorliegenden Vertrages verarbeitet werden, unverzüglich zu melden.
(9) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 7 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer verpflichtet sich, seine innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes und dem Risiko für die Rechte und Freiheiten der betroffenen Personen angemessenem Schutzniveau gerecht werden. Er ergreift technische und organisatorische Maßnahmen zum Schutz der Daten des Auftragnehmers, die den Anforderungen der DSGVO gemäß Art. 32 genügen.
(2) Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit sowie die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Der Auftragnehmer verpflichtet sich die getroffenen Maßnahmen in diesem Zusammenhang stets auf dem aktuellen Stand der Technik zu halten.
(3) Die Beschreibung der technischen und organisatorischen Maßnahmen gemäß Anhang 1 „TOM“ ist Bestandteil des AV Vertrags.
    a. Der Auftragnehmer verpflichtet sich die Wirksamkeit der getroffenen Maßnahmen regelmäßig, zumindest aber jährlich, zu prüfen, zu bewerten und gegebenenfalls anzupassen.

b. Änderungen an den getroffenen Maßnahmen bleiben dem Auftragnehmer vorbehalten, wobei sichergestellt werden muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
c. Wesentliche Änderungen sind dem Auftraggeber in schriftlicher Form mitzuteilen.

§ 8 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit dem Anliegen der Auskunft, Berichtigung oder Löschung an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung der Person zu dem jeweiligen Auftraggeber möglich und zulässig ist.
(2) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Pflichten gegenüber betroffenen Personen nach Kapitel 3 DSGVO (Recht auf Auskunft, Information, Berichtigung, Löschung, Datenübertragbarkeit und Widerspruch) im Rahmen seiner Möglichkeiten und gemäß den vertraglich vereinbarten Bedingungen.
(3) Der Auftragnehmer haftet nicht für die Einhaltung der im Rahmen der Anfrage geltenden Vorschriften auf Vollständigkeit und Korrektheit sowie der gesetzlichen Fristen.

§ 9 Unterauftragsverhältnisse

(1) Als Untervertragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die unmittelbar mit der Erbringung der im Hauptvertrag beschriebenen Dienstleistung in Zusammenhang stehen und durch verbundene oder fremde Unternehmen erbracht werden.
(2) Mit dem Hinzuziehen verbundener oder fremder Unternehmen durch den Auftragnehmer ist der Auftraggeber einverstanden. Der Auftragnehmer hat den Auftraggeber von der Beauftragung in Kenntnis zu setzen, sodass dieser innerhalb einer Frist von 14 Tagen widersprechen kann. Verweigert der Auftraggeber durch seinen Einspruch die Zustimmung, behält sich der Auftragnehmer das Recht vor, die Anlage sowie den dazugehörigen Vertrag fristlos zu kündigen.
(3) Eine Liste der aktuell eingesetzten Unterunternehmen inklusive deren jeweiliger Geschäftssitz sind den Allgemeinen Geschäftsbedingungen (https://www.cituro.com/agb) zu entnehmen. Diese Liste wird bei etwaigen Erweiterungen oder Anpassungen zeitnah aktualisiert.
(4) Beauftragt der Auftragnehmer Subunternehmer so obliegt es dem Auftragnehmer, seine aus diesem Vertrag hervorgehenden datenschutzrechtlichen Verpflichtungen auf diesen zu übertragen. In diesem Zusammenhang verpflichtet sich der Auftragnehmer dem Untervertragsverhältnis einen vertraglichen Rahmen gemäß Art. 28 Abs. 2-4 zu Grunde zu legen. Der Auftragnehmer behält die volle Verantwortung für die von ihm eingesetzten Subunternehmen.

§ 10 Außerordentliche Kündigung

Bei einem schwerwiegenden Verstoß gegen gesetzliche Datenschutzbestimmungen und im Speziellen gegen Bestimmungen des vorliegenden Vertrages kann der Auftraggeber den Hauptvertrag ohne Einhaltung einer Frist schriftlich kündigen.

§ 11 Beendigung des AV-Vertrages

(1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandenen Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen ohne unverhältnismäßig hohen Aufwand nicht mehr möglich ist.
(2) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.
(3) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren.

§ 12 Haftung und Schadensersatz

Auftragnehmer und Auftraggeber haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelungen.

§ 13 Schlussbestimmungen

(1) Erweiterungen und Änderungen dieses Vertrages sind zu ihrer Wirksamkeit schriftlich zu formulieren und dem Auftraggeber unverzüglich mitzuteilen.
(2) Sollte das Eigentum oder die zu verarbeitenden Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlicher im Sinne der DSGVO liegen.
(3) Es gilt das deutsche Recht.
(4) Für Rechtsstreitigkeiten aus einem Vertrag mit dem Anbieter wird der Gerichtsstand am Sitz des Anbieters vereinbart, sofern die Vertragspartner Kaufleute, juristische Personen des öffentlichen Rechts oder des öffentlich-rechtlichen Sondervermögens sind. Der Anbieter bleibt jedoch dennoch berechtigt den Dienstleister bei Vertragsverstoß an dessen Sitz zu verklagen.
(5) Bei etwaigen Widersprüchen gehen Regelungen dieses Vertrages den Regelungen des Hauptvertrages vor.
(6) Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Statt den unwirksamen oder undurchführbaren Bestimmungen gelten diejenigen wirksamen und durchführbaren Regelungen, deren Wirkung der wirtschaftlichen Zielsetzung am nächsten kommt, die die Vertragsparteien mit den unwirksamen bzw.

undurchführbaren Bestimmungen verfolgt haben. Die vorstehenden Bedingungen gelten gleichermaßen im Falle einer Vertragslücke.

Dieser Vertrag wird elektronisch geschlossen und ist ohne Unterschrift gültig.

Anlagenverzeichnis:

Anlage 1: TOMs

Anlage 1: Technische und Organisatorische Maßnahmen (TOM)

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle – Unsere Server befinden sich in deutschen Rechenzentren von IONOS. Der Zutritt ist strengstens geregelt und unter anderem durch folgende Maßnahmen gesichert:
    - Empfangs- und Ausweispflicht
    - Zutritt externer Besucher nur in Begleitung
    - Pförtner
    - Sicherheitsdienst
    - Protokollierter Zutritt
    - Zutritt wird durch Zutrittskarten mit strengen Auflagen reglementiert
    - Zutrittskontrollsystem
    - Videokameras
    - Sicherheitstüren
    - Einbruchmeldeanlage
- Zugangskontrolle Infrastruktur:
    - Fernzugriffe auf die internen Systeme sind durch eine Firewall geschützt
    - Fernzugriffe sind nur in authentifizierter Form möglich
    - 2 Faktor Authentifizierung am Cloud Backend
    - Systeme sind durch Virenschutz abgesichert
    - Privates Netzwerk mit VPN Zugriff
- Zugangskontrolle cituro Backend:
    - Zugriff ist nur in authentifizierter Form möglich
    - Protokollierung der Zugänge
- Zugriffskontrolle Infrastruktur:
    - Zugriff auf System nur durch ausgewählte Administratoren
    - Verschlüsselung von Zugangsdaten zu den internen System
- Zugriffskontrolle cituro Backend:
    - Der Zugriff auf Daten unterliegt einem Rollen- und Rechtekonzept
    - Minimale Anzahl von Administratoren, die durch den Kunden verändert werden kann
- Trennungskontrolle:
    - Physikalische Trennung zwischen Produktions-/Test-/Entwicklungsumgebung
    - Strikte Trennung der Datensätze durch Mandantenkonzept
    - Trennung der Daten nach Verwendungszweck
- Verschlüsselung:
    - Alle Verbindungen zu unseren Systemen sind TLS (1.3 oder 1.2) verschlüsselt.
    - Es werden nur sichere Protokolle (ssh, sftp, https) verwendet
    - Die Verschlüsselung wird immer auf dem Stand der Technik gehalten
- Homeoffice:
    - Zugriff auf Serverinfrastruktur nur über gesicherte und verschlüsselte Verbindung (VPN)
    - Einsatz von aktueller Hard- und Software für Arbeitsplatzgeräte
    - Keine private Nutzung von Arbeitsplatzgeräten

    - Schutz vor unbefugtem Zugang zu Arbeitsplatzgeräten durch Authentifizierung (Kennwort oder Biometrisch)
    - Beim Verlassen des Arbeitsplatzes werden Arbeitsplatzgeräte stets gesperrt
    - Ausschließlich datenschutzrechtlich geschultes und sensibilisiertes Personal greift für Supportzwecke auf personenbezogene Daten zu
    - Keine lokale Datenhaltung
    - Keine Datenverarbeitung in Anwesenheit Dritter
- Pseudonymisierung:
    - Laufzeitdaten wie Termine, Erinnerungen u.Ä. werden pseudonymisiert und erlauben ohne Zugriff auf die Stammdaten keinen Rückschluss auf eine konkrete Person
    - Es erfolgt keine Verwendung von Echtdaten außerhalb der Produktionsumgebung

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
    - Daten werden nur über sichere Protokolle transportiert
    - Eine Weitergabe von Daten erfolgt ausschließlich gesichert (verschlüsselt und/oder passwortgeschützt)
- Eingabekontrolle
    - Änderungen (Anlegen, Aktualisierung) an Datensätzen werden stets protokolliert
    - Änderungen an Systemeinstellungen werden stets protokolliert
    - Berechtigungen der Eingabe/Änderung/Löschung unterliegen einem Berechtigungskonzept, das jeder Kunde selbst für seine Benutzer festlegt

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Unsere Server befinden sich in einem IONOS Rechenzentrum in Deutschland, das nach ISO 27001 und ISO 9001 zertifiziert ist und höchsten Ansprüchen an Verfügbarkeit gerecht wird.
- Das IONOS Netz ist mehrstufig vor Hackerangriffen, wie DDos-Attacken geschützt.
- Updates und Patches werden zeitnah eingespielt.
- Daten werden regelmäßig gesichert.
- Es werden regelmäßig Backups der Daten erstellt, die räumlich getrennt aufbewahrt werden.
- Die zentralen Dienste werden stets durch ein Monitoring überwacht.
- Virenschutz, Firewalls und andere relevante Sicherheitssysteme werden stets aktuell gehalten.
- Die Serverhardware ist mehrfach redundant und ausfallsicher ausgelegt.
- Es existiert eine Brandschutzanlage.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mindestens einmal jährlich durchgeführt
- Regelmäßige Schulung aller mit personenbezogenen Daten in Berührung kommenden Personen, um die Einhaltung der gesetzlichen Vorschriften zu gewährleisten
- Datenschutzfreundliche Voreinstellungen unserer Dienste minimieren die anfallenden personenbezogenen Daten
- Sorgfältige Auswahl von Subunternehmern/Auftragsverarbeitern, vor allem in Bezug auf den Datenschutz
- Abschluss notwendiger Vereinbarungen mit eventuellen Subunternehmern/Auftragsverarbeitern und deren Überprüfung
- Kundenspezifische Dokumentation von Weisungen und Tätigkeiten im Rahmen der Auftragsverarbeitung
- Datenschutzvorfälle werden unverzüglich dokumentiert und ausgewertet.