Vereinbarung über eine Auftragsdatenverarbeitung nach Art. 28 DSGVO

Geltungsbereich

Der Verantwortliche:

...
...
...

(im Folgenden Auftraggeber)

Der Auftragsverarbeiter:

5FSoftware GmbH
Franz-Mayer-Str. 1
93053 Regensburg

(im Folgenden Auftragnehmer)

1. Gegenstand der Vereinbarung

(1) Der Auftragnehmer ist Anbieter von Branchensoftware für die sichere Kommunikation zwischen Kanzlei und Mandant und erbringt für den Auftraggeber auf Grundlage der Leistungsvereinbarung vom 28.10.2022 (Hauptvertrag) Leistungen gemäß der im Hauptvertrag enthaltenen Leistungsbeschreibung.
(2) Im Rahmen der Leistungserbringung erhält der Auftragnehmer Zugriff auf personenbezogene Daten, diese werden vom Auftragnehmer anlassbezogen ausschließlich im Auftrag und nach Weisung des Auftraggebers verarbeitet. Dies geschieht sowohl in ausschließlich technisch- organisatorischer Form (d.h. zum Zweck der Fehlerbehebung oder zur Hilfestellung im technischen oder inhaltlichen Umgang mit den Programmen) als auch durch eine inhaltliche Verarbeitung (z.B. durch Speicherung und/oder Versand von Saldenbestätigungen an für diesen Zweck vom Auftraggeber übermittelte E-Mail Adressen).
(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer, seine Beschäftigten oder durch den Auftragnehmer Beauftragte (Subunternehmer) mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.
(4) Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

2. Art und Zweck der verarbeiteten Daten, Kreis der Betroffenen

(1) Die Programme des Auftragnehmers dienen dem sicheren Datenaustausch zwischen dem Auftraggeber und dessen Mandanten oder Geschäftspartnern.
(2) In den Programmen des Auftragnehmers werden die Daten für die Auftragsabwicklung des Auftraggebers und dessen interne Verwaltung verarbeitet. Im Einzelnen sind davon die nachfolgend genannten Datenarten/-kategorien personenbezogener Daten betroffen:
- Personalstammdaten
- Daten über Verwaltungsinterna des Auftraggebers
- Mandantenstammdaten
- Lieferantenstammdaten
- Steuerdaten von Mandanten
- Daten über wirtschaftliche Verhältnisse von Mandanten
- Kommunikationsdaten (z. B. Telefon, E-Mail, Adressen)
- Kontodaten

- Lohnabrechnungsdaten
- Prozessdaten der Workflows (Datum, Uhrzeit, Fälligkeiten, Formulardaten, Logging-Daten)
- von den Nutzern selbst hochgeladene Fotos

(3) Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:
   a. Mandanten des Auftraggebers
   b. Mitarbeiter des Auftraggebers
   c. Lieferanten des Auftraggebers
   d. Gesellschafter von Mandanten des Auftraggebers
   e. Mitarbeiter von Mandanten des Auftraggebers
   f. Kunden von Mandanten des Auftraggebers
   g. Lieferanten von Mandanten des Auftraggebers
   h. Ansprechpartner

(4) Zum Empfängerkreis der personenbezogenen Daten zählen die zur Verschwiegenheit verpflichteten Mitarbeiter des Auftragnehmers sowie etwaige vom Auftragnehmer beauftragte Subunternehmer.

3. Dauer der Vereinbarung

Die Rechte und Pflichten aus diesem Auftragsdatenverarbeitungsvertrag bestehen für die Dauer der Wirksamkeit des Hauptvertrages und überdauern das Vertragsende soweit die Datenverarbeitung einschließlich der erforderlichen Löschung von Daten beim Auftragnehmer noch nicht beendet sein sollte.

4. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.
(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.
(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Dies umfasst Weisungen im Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.
(4) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.
(5) Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.
(6) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.
(7) Der Auftraggeber kann weisungsberechtigte Personen benennen. Für den Fall, dass weisungsberechtigte Personen des Auftraggebers benannt werden oder sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.
(8) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.
(9) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder eine sonstige, für den Auftraggeber geltende gesetzliche Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

5. Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere mindestens die in Anlage 1 aufgeführten Maßnahmen zur

   i. Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung
   ii. Wiederherstellung der Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
   iii. Bereitstellung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite.

(4) Der Auftragnehmer verpflichtet sich die für den Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen. Hierzu wird eine gesonderte Vereinbarung getroffen.

(5) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet, es sei denn diese unterliegen einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung. Die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen bleibt auch nach der Beendigung ihrer Tätigkeit und dem Ausscheiden beim Auftragnehmer bestehen. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

6. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, personenbezogene Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der mit dem Auftraggeber vertraglich getroffenen Vereinbarungen und unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen zu verarbeiten.

(2) Der Auftragnehmer verpflichtet sich, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die im Auftrag des Auftragnehmers verarbeiteten Daten im erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.

(3) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung durch ihn oder andere mit der Verarbeitung beschäftigte Personen erfolgt ist, unverzüglich in Textform mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so wird er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber informieren und die Behörde an diesen verweisen.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der diesem im Falle von Datenschutzverletzungen obliegenden Meldepflichten nach Art. 33, 34 DSGVO. Insbesondere wird der

Auftraggeber dem Auftragnehmer jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich mitteilen. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(6) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12 bis 23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(7) Unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer vorliegenden Informationen unterstützt der Auftragnehmer den Auftraggeber bei der Erfüllung dessen Pflichten bezüglich der Sicherheit der Verarbeitung (wie in Artikel 32 DSGVO ausgeführt), der Datenschutz-Folgenabschätzungen (wie in Artikel 35 DSGVO ausgeführt) und der vorherigen Konsultation (wie in Artikel 36 DSGVO ausgeführt) zu unterstützen.

(8) Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gemäß § 30 Abs. 2 DSGVO enthält. Der Auftragnehmer stellt das Verzeichnis dem Auftraggeber auf Anforderung zur Verfügung.

(9) 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 Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

(10) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, zu vernichten. Der Auftragnehmer hat die unverzügliche Vernichtung von Verarbeitungsergebnissen und Daten enthaltenden Unterlagen auch bei Subunternehmern herbeizuführen.

7. Ort der Durchführung der Datenverarbeitung

Die Verarbeitung der Daten durch den Auftragnehmer findet ausschließlich in Rechenzentren im Territorium der Bundesrepublik Deutschland statt. Die Auftragsverarbeitung durch einen Subunternehmer richtet sich nach Ziffer 8 der Vereinbarung.

8. Einsatz von Subunternehmern

(1) Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung Subunternehmer zur Auftragsverarbeitung einzusetzen. Der Auftragnehmer verpflichtet sich, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat die Subunternehmer entsprechend den Regelungen dieser Vereinbarung zu verpflichten, insbesondere
a) die Subunternehmer unter Berücksichtigung seiner technischen und organisatorischen Maßnahmen zum Datenschutz sorgfältig auszuwählen und
b) die Subunternehmer durch schriftlichen Vertrag zu beauftragen und
c) die Subunternehmer mindestens in demselben Umfang zur Erfüllung datenschutzrechtlicher Anforderungen zu verpflichten, wie dies in dieser Vereinbarung mit dem Auftraggeber gilt.

(2) Die Parteien stellen fest, dass die Voraussetzungen gemäß Ziffer 8. Absatz 1 für die Subunternehmer vorliegen, die zum Zeitpunkt des Abschlusses dieser Vereinbarung bereits bestehen. Eine Liste der mit der

Verarbeitung personenbezogener Daten betrauter Subunternehmer wird dem Auftraggeber auf Anfrage zur Verfügung gestellt.

(3) Kommt ein Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Subunternehmers.

(4) Der Auftragnehmer informiert den Auftraggeber über die beabsichtigte Hinzuziehung neuer Subunternehmer oder Ersetzung bisheriger Subunternehmer schriftlich oder in elektronischer Form. Der Auftraggeber kann gegen die in Satz 1 genannten Änderungen innerhalb einer Frist von 4 Wochen nach Zugang der Information aus wichtigem Grund Einspruch beim Auftragnehmer erheben. Der Einspruch ist zu begründen. In Notsituationen ist der Auftragnehmer befugt, die Einspruchsfrist durch Mitteilung an den Auftraggeber auf einen im konkreten Fall angemessenen Zeitraum zu verkürzen. Im Fall eines fristgerechten Einspruchs kann der Auftragnehmer nach eigener Wahl entweder seine Leistungen ohne Hinzuziehung des Subunternehmers fortsetzen oder das Vertragsverhältnis mit dem Auftraggeber (einschließlich des Hauptvertrages) innerhalb einer Frist von 4 Wochen schriftlich kündigen.

(5) Die Verarbeitung durch einen Subunternehmer findet innerhalb der EU oder des EWR statt, soweit nicht anders von den Parteien vereinbart ist. Die Parteien vereinbaren, dass auch beim Einsatz eines genehmigten Subunternehmers Buchführungsdaten nicht ohne Zustimmung des Auftraggebers außerhalb der Bundesrepublik Deutschland verarbeitet werden. Jegliche Verarbeitung (einschließlich des Zugriffs auf Daten) in einem Drittland (d. h. weder EU noch EWR) erfordert die Genehmigung des Auftraggebers sowie die Erfüllung der speziellen Anforderungen von Art. 44 ff. DSGVO. Sofern der Subunternehmer keine gültige BCR- oder Privacy Shield-Zertifizierung oder einen Angemessenheitsbeschluss für den Ort der Datenverarbeitung vorweisen kann, sind nach Weisung des Auftraggebers EU Standardvertragsklauseln abzuschließen.

(6) Ein Subunternehmerverhältnis im Sinne dieser Vereinbarung liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfungsleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

9. Schlussbestimmungen

(1) Für Nebenabreden ist die Schriftform erforderlich.

(2) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit des Vertrages im Übrigen nicht.

Für den Auftraggeber:

Für den Auftragnehmer:

Christian Lang,
Geschäftsführer

Anlage 1 – Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Der Auftragnehmer hat als Auftragsverarbeiter für den Auftraggeber die folgenden technischen und organisatorischen Sicherheitsmaßnahmen implementiert, um die laufende Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit der Verarbeitungssysteme und -dienste zu gewährleisten:

1. Vertraulichkeit

Der Auftragnehmer hat folgende technische und organisatorische Sicherheitsvorkehrungen getroffen, um insbesondere die Vertraulichkeit der Verarbeitungssysteme und –dienste sowie der personenbezogenen Daten zu gewährleisten:

- Der Auftragnehmer hat Maßnahmen ergriffen, dass unbefugte keinen Zutritt zu seinen Räumlichkeiten haben, in denen personebezogene Daten des Auftraggebers verarbeitet werden:
  - ein mehrschichtiges Sicherheitsmodell, das Sicherheitsvorkehrungen wie maßgeschneiderte elektronische Zugangskarten/Transponder, Alarme, Absicherung von Gebäudeschätzen, Sicherheitsschlössern;
  - Regelungen zur Schlüsselausgabe;
  - Einsatz von Aktenvernichtern gemäß aktuellen Anforderungen;
  - Protokollierung der Besucher; und
  - Sorgfältige Auswahl von Wachpersonal und Reinigungspersonal.
- Der Auftragnehmer verarbeitet alle Kundendaten an deutschen Serverstandorten, die von branchenführenden Cloud Service Providern betrieben werden, die hochentwickelte Maßnahmen zum Schutz vor unbefugtem Zugriff auf Datenverarbeitungsanlagen (insbesondere Telefone, Datenbank- und Applikationsserver und zugehörige Hardware) anbieten.
  Zu diesen Maßnahmen gehören:
  - ein mehrschichtiges Sicherheitsmodell, das Sicherheitsvorkehrungen wie maßgeschneiderte elektronische Zugangskarten, Alarme, Fahrzeugzutrittsschranken, Umzäunungen, Metalldetektoren und Biometrie umfasst, sowie eine Ausstattung des Bodens des Rechenzentrums mit einer Laserstrahleinbruchhemmung;
  - Rechenzentren werden rund um die Uhr von hochauflösenden Innen- und Außenkameras überwacht, die unberechtigte Personen erkennen und verfolgen können;
  - Zugriffsprotokolle, Aktivitätsaufzeichnungen und Kameraaufnahmen sind für den Fall eines Einbruchs verfügbar;
  - Rechenzentren werden außerdem routinemäßig von erfahrenen Sicherheitskräften patrouilliert, die strenge Hintergrundüberprüfungen und Schulungen durchlaufen haben;
  - Der Zugang zum Boden des Rechenzentrums ist nur über einen Sicherheitskorridor möglich, der eine mehrstufige Zugangskontrolle mittels Sicherheitsausweisen und Biometrie ermöglicht; und
  - Nur berechtigte Mitarbeiter mit bestimmten Rollen können eintreten.
- Der Auftragnehmer trifft geeignete Maßnahmen, um zu verhindern, dass seine Datenverarbeitungssysteme von Unbefugten benutzt werden. Dies wird erreicht durch:

- Authentifizierung durch Benutzername und Passwort;
- Einsatz von Anti-Viren Software;
- automatisches Timeout des User-Terminals, wenn dieser im Leerlauf bleibt, Identifikation und Passwort zum erneuten Zugreifen erforderlich;
- sichere Aufbewahrung von Datenträgern. Beim physischen Transport der Datenträger sorgfältige Auswahl des Transporteurs;
- Verschlüsselung nach Industriestandard und Anforderungen an Passwörter (Mindestlänge, Verwendung von Sonderzeichen usw.);
- Alle Zugriffe auf Dateninhalte werden protokolliert, überwacht und verfolgt;
- Nutzung der eigenen Kommunikationsplattform für den Austausch von personenbezogenen Daten mit Kunden; und
- Zugriff auf die Datenverarbeitungssysteme über externe Schnittstellen (USB etc.).

- Der Auftragnehmer löscht die Daten nach Weisung des Auftraggebers unter Berücksichtigung des Stands der Technik.
- Die Mitarbeiter des Auftragnehmers, die zur Nutzung seiner Datenverarbeitungssysteme berechtigt sind, können nur im Rahmen und in dem Umfang auf personenbezogene Daten zugreifen, der durch ihre jeweilige Zugriffsberechtigung (Berechtigung) abgedeckt ist und soweit es ihr Benutzerprofil im jeweiligen System erlaubt. Insbesondere basieren die Zugriffsrechte und -ebenen auf der Funktion und Rolle der Mitarbeiter, wobei die Konzepte der geringsten Privilegien und des Wissensbedarfs verwendet werden, um die Zugriffsrechte an definierte Verantwortlichkeiten anzupassen. Dies wird erreicht durch:
  - Die Anzahl der Administratoren ist auf das Notwendigste reduziert;
  - Mitarbeiterpolitik und -schulung;
  - wirksame und angemessene Disziplinarmaßnahmen gegen Personen, die unbefugt auf personenbezogene Daten zugreifen;
  - beschränkter Zugriff auf personenbezogene Daten nur für autorisierte Personen;
  - Verschlüsselung nach Industriestandard und
  - Verpflichtung der Mitarbeiter auf das Datengeheimnis;
  - Richtlinien zur Kontrolle der Aufbewahrung von Sicherungskopien.

2. Integrität

Der Auftragnehmer hat die folgende technische und organisatorische Sicherheit implementiert, um insbesondere die Integrität der Verarbeitungssysteme und -dienste zu gewährleisten:

- Der Auftragnehmer trifft geeignete Maßnahmen, um zu verhindern, dass personenbezogene Daten auf der Kommunikationsplattform, bei der Übermittlung oder beim Transport der Datenträger von Unbefugten gelesen, kopiert, verändert oder gelöscht werden. Dies wird erreicht durch:
  - Den Einsatz modernster Firewall- und Verschlüsselungstechnologien zum Schutz der Torwege und Pipelines, durch die die Daten fließen;
  - Einsatz von Anti-Viren Software;

- Verschlüsselung nach Industriestandard und
- Vermeidung der Speicherung personenbezogener Daten auf tragbaren Speichermedien für Transportzwecke und auf firmeneigenen Laptops oder anderen mobilen Geräten.

- Der Auftragnehmer führt eine logische Mandantentrennung auf der Plattform durch. Der Auftragnehmer trennt Test- und Produktivsystem.
- Der Auftragnehmer greift auf keine Kundeninhalte zu, es sei denn, dies ist notwendig, um dem Kunden die von ihm ausgewählten Produkte und professionelle Dienstleistungen zur Verfügung zu stellen. Der Auftragnehmer greift nicht auf Kundeninhalte für andere Zwecke zu. Entsprechend weiß der Auftragnehmer nicht, welche Inhalte Kunden auf seinen Systemen speichern und kann nicht zwischen persönlichen Daten und anderen Inhalten unterscheiden, so dass der Auftragnehmer alle Kundeninhalte gleichbehandelt. Auf diese Weise profitieren alle Kundeninhalte von den gleichen hohen Sicherheitsmaßnahmen des Auftragnehmers, unabhängig davon, ob diese Inhalte personenbezogene Daten enthalten oder nicht.
- Der Auftragnehmer protokolliert Zugriffe, Eingaben, Änderungen und Löschungen in Bezug auf die Daten.

3. Verfügbarkeit

Der Auftragnehmer hat die folgenden technischen und organisatorischen Sicherheitsmaßnahmen implementiert, um insbesondere die Verfügbarkeit von Verarbeitungssystemen und -diensten zu gewährleisten:

- Der Auftragnehmer trifft geeignete Maßnahmen, um sicherzustellen, dass personenbezogene Daten vor unbeabsichtigter Zerstörung oder Verlust geschützt sind. Dies wird erreicht durch:
  - Redundanz der Infrastruktur
  - Vorliegen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können;
  - Richtlinien, die eine permanente lokale (Arbeitsplatz) Speicherung personenbezogener Daten verbieten;
  - Einsatz von Anti-Viren Software und
  - Durchführung regelmäßiger Datensicherungen sowie Test der Datenwiederherstellung.

4. Belastbarkeit

Der Auftragnehmer hat die folgenden technischen und organisatorischen Sicherheitsmaßnahmen implementiert, um insbesondere die Ausfallsicherheit der Verarbeitungssysteme und -dienste zu gewährleisten:

- Der Auftragnehmer führt Penetrationstests und Schwachstellenbewertungen durch, einschließlich automatischer Überprüfung der System- und Anwendungssicherheit auf Systemen, die für die Datenverarbeitung verwendet werden. Der Auftragnehmer unternimmt angemessene Schritte, um hierbei eine Unterbrechung der erbrachten Dienste zu vermeiden.
- Der Auftragnehmer unterhält Richtlinien und Verfahren, um die mit der Umsetzung von Änderungen an seinen Diensten verbundenen Risiken zu bewerten und zu kontrollieren.
- Der Auftragnehmer führt ein Inventar aller IT-Assets, die für die Verarbeitungstätigkeiten verwendet werden. Der Auftragnehmer überwacht in diesem Zusammenhang den Zustand und die Verfügbarkeit der Verarbeitungsaktivitäten kontinuierlich.

- Der Auftragnehmer bewertet die Verarbeitungsaktivitäten auf Business Continuity und Disaster Recovery-Anforderungen. Dazu gehören definierte, dokumentierte, gewartete und validierte Business Continuity und Disaster Recovery Pläne, die branchenüblichen Verfahren entsprechen.

- Der Auftragnehmer erstellt regelmäßig Backups von Systemen, die personenbezogene Daten enthalten, stellt sicher, dass sich mindestens ein Backup-Ziel an einem von den Produktionssystemen getrennten Ort befindet, verschlüsselt Backup-Daten, die auf tragbaren Backup-Medien gespeichert sind, und überprüft die Integrität des Backup-Prozesses durch regelmäßige Datenwiederherstellungs-tests.