Auftragsdatenbearbeitungsvereinbarung ADV inkl. TOM

Inhaltsverzeichnis:

Bestimmungen über die Auftragsbearbeitung 2
1) Begriffe: 2
2) Auftragsbearbeitung: 2
1. Geltungsbereich und Merkmale der Auftragsdatenbearbeitung 2
2. Bearbeitung von Personendaten 3
Pflichten der Auftraggeberin 3
Pflichten des Dienstleisters 3
Schadloshaltung 5
3) Sonstige Bestimmungen: 5
Anhang: Technische & Organisatorische Massnahmen (TOM) 6
1. Allgemeine Sicherheitsmassnahmen 6
Zutrittskontrolle 6
Zugangskontrolle 7
Zugriffskontrolle 7
2. Spezifische Massnahmen 7
Übermittlungskontrolle 7
Auftragskontrolle 7
3. Datenintegrität 8
Integritätskontrolle 8
Verfügbarkeitskontrolle 8
4. Organisatorische Massnahmen (Art. 26 DSG) 8
5. Art und Zweck der Verarbeitung 9
Art der personenbezogenen Daten 9
Kategorien der betroffenen Personen 9
Zweck der Datenverarbeitung 9
Ort der Datenverarbeitung 10
Rückgabe und Löschung 10
6. Sensibilisierung und Schulung 10
Mitarbeiterschulungen 10
7. Kontinuierliche Verbesserung 10
Auditierung und Überprüfung 10

Mit dieser Auftragsdatenbearbeitungsvereinbarung (Vereinbarung) regeln die Parteien das Bearbeiten von Personendaten an bzw. durch den Dienstleister im Rahmen des zugrundeliegenden Rahmenvertrages. Der Umfang der Datenbearbeitung (Gegenstand, Zweck, Kategorien der Daten etc.) ergibt sich direkt aus dem Rahmenvertrag, es sei denn, nachstehend wird anderes angewählt und ausgeführt.

Die Dauer der Auftragsverarbeitung richtet sich nach der Laufzeit des zugrundeliegenden Rahmenvertrags und kann nur mit diesem zusammen ordentlich oder ausserordentlich gekündigt werden.

Bestimmungen über die Auftragsbearbeitung

Die Parteien haben einen Rahmenvertrag geschlossen, in dessen Rahmen der Dienstleister Personendaten im Auftrag der Auftraggeberin bearbeitet. Mit der Vereinbarung soll diese Auftragsbearbeitung für die Zwecke des DSG und, soweit anwendbar, der DSGVO geregelt werden. Eine Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau (gemäss Anhang 1 der Datenschutzverordnung (DSV)) ist nicht zulässig. Eine allfällige Bearbeitung von Personendaten für eigene Zwecke des Dienstleisters bedarf einer ausdrücklichen und separaten Vereinbarung und ist ansonsten untersagt.

1) Begriffe:

In dieser Vereinbarung werden die folgenden definierten Begriffe verwendet. Im Übrigen gelten Begriffe wie im DSG und, soweit anwendbar, wie in der DSGVO definiert, so insbesondere "Personendaten", "Bearbeiten", "Auftragsbearbeiter" und "Verantwortlicher".

"DSG" ist das Bundesgesetz über den Datenschutz in seiner jeweils gültigen Fassung, inkl. seinen Verordnungen.

"DSGVO" ist die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

"EWR" ist der Europäische Wirtschaftsraum.

"**Land mit angemessenem Datenschutzniveau**" ist ein Land oder ein Gebiet welches im Anhang 1 der Datenschutzverordnung (DSV) aufgeführt wird.

"**Verbundenes Unternehmen**" ist eine juristische Person, welche direkt oder indirekt von der Auftraggeberin kontrolliert wird oder welche die Auftraggeberin direkt oder indirekt kontrolliert oder die direkt oder indirekt unter der Kontrolle derselben juristischen Person steht wie die Auftraggeberin.

2) Auftragsbearbeitung:

1. Geltungsbereich und Merkmale der Auftragsdatenbearbeitung

Diese Vereinbarung regelt im Rahmen der Erfüllung des Hauptvertrags das **Bearbeiten von Personendaten** durch den Dienstleister als Auftragsbearbeiter für die Auftraggeberin als Verantwortliche.

Alternativ kann der Dienstleister als Unterauftragsbearbeiter der Auftraggeberin und die Auftraggeberin als Auftragsbearbeiterin eines Dritten fungieren.

Soweit die Auftraggeberin selbst Auftragsbearbeiterin ist (z.B. eines Kunden), ist, soweit zulässig, ausschliesslich sie für die Kommunikation mit dem Verantwortlichen zuständig und ihre Anweisungen gelten als jene des Verantwortlichen.

Als Personendaten sind alle Daten gemeint, die der Dienstleister im Rahmen der Bearbeitung von der Auftraggeberin, einem verbundenen Unternehmen oder einem Dritten erhält

Gegenstand, Dauer, Art und Zweck der Bearbeitung, sowie die Kategorien der bearbeiteten Personendaten und der betroffenen Personen sind wie unter lit. c, Ziff. 5 der Vereinbarung angegeben festgelegt.

2. Bearbeitung von Personendaten

Pflichten der Auftraggeberin

Die Auftraggeberin bestätigt gegenüber dem Dienstleister, dass:

sie alle Mitteilungen, Registrierungen, behördliche Genehmigungen und Einwilligungen von betroffenen Personen, die für eine rechtmässige Bearbeitung von Personendaten durch den Dienstleister als Auftragsbearbeiter nach DSG und, soweit anwendbar, DSGVO erforderlich sind, gemacht oder eingeholt hat; und

sie alle Anfragen von betroffenen Personen beantwortet, die ihre Rechte gemäss den anwendbaren Datenschutzvorschriften ausüben.

Pflichten des Dienstleisters

Der Dienstleister verpflichtet sich und gewährleistet gegenüber der Auftraggeberin:

a) Personendaten nur für die **Zwecke** der Auftraggeberin und jeweils nur zum Zwecke der Erfüllung des Hauptvertrages gemäss den dokumentierten Weisungen der Auftraggeberin zu bearbeiten;
b) Personendaten nur an den allenfalls vereinbarten oder anderweitig von der Auftraggeberin genehmigten **Standorten** zu bearbeiten**;**
c) keine Personendaten ins Ausland bekanntzugeben oder zu übermitteln, ausser der Kunde verlangt es im Sinne des beauftragen Service.

d) geeignete technische und organisatorische Massnahmen vorzusehen (TOM gemäss Anhang von dieser ADV) und aufrechtzuerhalten, um die Vertraulichkeit, Integrität und Verfügbarkeit von Personendaten jederzeit zu gewährleisten und Personendaten vor unbefugter Bearbeitung, unbefugtem Zugriff oder unbefugter Offenlegung sowie vor versehentlicher oder unrechtmässiger Verfälschung, Zerstörung oder Verlust zu schützen, insbesondere und mindestens die im DSG und, soweit anwendbar, die in Art. 32 DSGVO sowie in anderen zur Anwendung kommenden Datenschutzvorschriften genannten Massnahmen der Datensicherheit; der Dienstleister wird diese Massnahmen regelmässig auf ihre Einhaltung und Wirksamkeit überprüfen und der Auftraggeberin Verbesserungen oder Anpassungen vorschlagen, wo dies angezeigt erscheint;

   sich bei der Bearbeitung von Personendaten nur auf Mitarbeiter und andere Hilfspersonen (einschliesslich aller Unterauftragsbearbeiter, die auf Anweisung des Dienstleisters arbeiten) zu verlassen, die vertraglich oder gesetzlich zur **Vertraulichkeit** sowie dazu verpflichtet sind, Personendaten nicht für andere Zwecke zu verwenden oder zu bearbeiten, als für die Erfüllung der Aufgaben, die ihnen vom

Dienstleister in Übereinstimmung mit dem Hauptvertrag und dieser Vereinbarung übertragen wurden, wobei zwischen den Parteien ferner als vereinbart gilt, dass der Dienstleister für das Verhalten seiner Mitarbeiter und anderen Hilfspersonen wie für sein eigenes Verhalten verantwortlich bleibt;

die Bearbeitung von Personendaten an Unterauftragsbearbeiter nur zu delegieren, wenn die Auftraggeberin dem Beizug nicht widersprochen hat. Der Dienstleister hat die Auftraggeberin sechzig (60) Tage vor dem Beizug des Unterauftragsbearbeiters darüber zu informieren. Der Beizug gilt als genehmigt, wenn die Auftraggeberin nicht innert dreissig (30) Tagen widerspricht. Iomarket darf bei der Bearbeitung von Personendaten, die unter dem Titel «Unterauftragsbearbeiter der io market AG» genannten Unterauftragsbearbeiter zu den jeweils genannten Leistungen einsetzen. Der Unterauftragsbearbeiter ist durch den Dienstleister zur Einhaltung von Bestimmungen über Vertraulichkeit und Datenschutz zu verpflichten, die mindestens ebenso streng sind wie die Bestimmungen des Hauptvertrages und dieser Vereinbarung, wobei zwischen den Parteien ferner als vereinbart gilt, dass der Dienstleister für das Verhalten seiner Unterauftragsbearbeiter wie für sein eigenes Verhalten verantwortlich bleibt, und dass er jede Änderung der Kontaktdaten, des Standorts oder anderer wichtiger Aspekte seiner Unterauftragsbearbeiter der Auftraggeberin unverzüglich und in geeigneter Weise mitteilt. Die Anpassung datenschutzrechtlich relevanter Aspekte setzt eine erneute Genehmigung voraus. Eine weitere Unterbeauftragung durch den Unterauftragsbearbeiter ist nicht zulässig.

der Auftraggeberin unverzüglich, in jedem Fall innerhalb von 24 Stunden an die von der Auftraggeberin bezeichnete Adresse (und mangels einer solchen an die Kontaktadresse auf dem Unterschriftenblatt) zu melden: (i) jede tatsächliche oder vermutete **Verletzung des Schutzes von Personendaten bzw. der Datensicherheit** (was auch jeden Verstoss gegen diese Ziffer 2.0, und jede andere Verletzung des Schutzes von Personendaten im Sinne der DSGVO, des DSG und sonst anwendbarer Datenschutzvorschriften umfasst) zusammen mit allen Informationen gemäss Artikel 33 Absatz 3 DSGVO, den entsprechenden Bestimmungen des DSG und der sonst anwendbaren Datenschutzvorschriften sowie auf erstes Verlangen jene weitere Information und Auskunft, welche gemäss Ziffer 2 (v) (z.B. Root Cause Analysis), (ii) jede tatsächliche oder drohende Beeinträchtigung oder Unzulänglichkeit des Dienstleisters bei der Einhaltung einer der Bestimmungen dieser Vereinbarung einschliesslich der vernünftigerweise verlangten **Informationen und Auskünft**e dazu, (iii) jedes Ersuchen um Zugriff und jeden tatsächlichen **Zugriff auf Personendaten** durch Behörden oder andere Stellen, es sei denn, das anwendbare Recht verbietet die Meldung aus wichtigen Gründen des öffentlichen Interesses ausdrücklich; im Falle von (iii) wird der Dienstleister zudem jeden solchen Zugriff auf Personendaten, soweit zumutbar und von der Auftraggeberin nicht anders verlangt, abzuwehren und einzuschränken versuchen;

die Auftraggeberin auf ihr Ersuchen hin bei der Einhaltung der DSGVO, des DSG und der sonst anwendbaren Datenschutzvorschriften auf die von ihr gewünschte Art und Weise und unter Berücksichtigung der Art der Bearbeitung sowie der dem Dienstleister zur Verfügung stehenden Informationen auf erstes Verlangen zu unterstützen, insbesondere bei der Erfüllung ihrer Verpflichtungen (i) gegenüber betroffenen Personen, die ihre Rechte gemäss den anwendbaren Datenschutzvorschriften (einschliesslich Kapitel III der DSGVO und den entsprechenden Bestimmungen des DSG und anderer anwendbarer Datenschutzvorschriften) ausüben, und (ii) gemäss den Artikeln 32 bis 36 DSGVO und den entsprechenden Bestimmungen des DSG und anderer anwendbarer Datenschutzvorschriften;

die Auftraggeberin unverzüglich zu informieren, wenn eine **Weisung der Auftraggeberin** seiner Meinung nach gegen anwendbare datenschutzrechtliche oder andere anwendbare Vorschriften verstösst; so weit zumutbar wird er die Bearbeitung mangels anderer Anweisung fortsetzen;

der Auftraggeberin alle Informationen zur Verfügung zu stellen, die erforderlich sind, um die Einhaltung der Pflichten durch den Dienstleister nachzuweisen, und **Prüfungen und Inspektionen** (auch vor Ort) durch die Auftraggeberin oder durch von der Auftraggeberin dazu beauftragte Prüfgesellschaften zuzulassen und daran mitzuwirken; der Dienstleister stellt der Auftraggeberin unaufgefordert oder jederzeit auf ihre Anfrage hin von seinen Prüfgesellschaften erstellte Prüfberichte, welche die Einhaltung der in dieser Vereinbarung festgelegten Pflichten oder der gesetzlichen Vorgaben durch den Dienstleister bestätigen oder dessen bzw. deren Verletzung dokumentieren, ohne weitere Kosten zur Verfügung; der Dienstleister stellt sicher, dass die Auftraggeberin diese Prüfrechte auch in Bezug auf Unterauftragsbearbeiter wahrnehmen kann; der Dienstleister wird ferner festgestellte Mängel ohne schuldhaften Verzug und auf eigene Kosten wie erforderlich beheben und dies nachweisen; werden im Rahmen einer Prüfung oder Inspektion nicht unwesentliche Mängel entdeckt oder gibt der Dienstleister Anlass zur Prüfung oder Inspektion, trägt er die damit zusammenhängenden Kosten und Aufwendungen; und

entsprechend der Wahl der Auftraggeberin, vorbehaltlich anwendbarer gesetzlicher Aufbewahrungspflichten, bei Beendigung des Hauptvertrages oder auf Verlangen der Auftraggeberin alle oder bestimmte Personendaten an die Auftraggeberin zurückzugeben oder zu löschen, ohne eine Kopie davon aufzubewahren, und der Auftraggeberin diese **Löschung** zu bestätigen**.**

Schadloshaltung

Der Dienstleister hat die Auftraggeberin gegen jegliche Ansprüche Dritter aufgrund einer Verletzung dieser Vereinbarung oder anwendbarer Datenschutzvorschriften schad- und klaglos zu halten. Eine solche Schadloshaltung gilt insbesondere bezüglicher aller Schäden, Kosten, Administrativsanktionen, Ansprüche oder Aufwendungen, die der Auftraggeberin als Folge solcher Verletzungen entstehen. Sie unterliegt, wie auch ein etwaiger Schadenersatzanspruch der Auftraggeberin und ihrer verbundenen Unternehmen, mangels ausdrücklich in Bezug auf diese Klausel abweichende Vereinbarung der doppelten Höhe einer etwaigen im Hauptvertrag vereinbarten Haftungsbegrenzungen. Ein allfälliger Haftungsausschluss für leichte Fahrlässigkeit gilt nicht.

3) Sonstige Bestimmungen:

Ferner vereinbaren die Parteien das Folgende:

Diese Vereinbarung gilt auch zugunsten der **verbundenen Unternehme**n der Auftraggeberin, für die der Dienstleister Personendaten gemäss dem Hauptvertrag bearbeitet. Dementsprechend können die verbundenen Unternehmen der Auftraggeberin gegenüber dem Dienstleister die gleichen Rechte wie die Auftraggeberin geltend machen, und der Dienstleister hat ihnen gegenüber, die gleichen Pflichten gemäss dieser Vereinbarung wie gegenüber der Auftraggeberin.

Jede Partei kommt ihren **Pflichten** gemäss den auf sie anwendbaren Datenschutzvorschriften nach, insbesondere jenen gemäss DSG und, soweit anwendbar, der DSGVO.

Die jeweils geltende Version wird online auf der Webseite publiziert. Insoweit aufgrund von übersetzen Versionen unterschiedliche sprachliche Fassungen vorliegen sollten, ist die deutsche Fassung relevant.

Diese Vereinbarung gilt als eigenständige Vereinbarung nebst dem Hauptvertrag. Im Falle von Widersprüchen zwischen Bestimmungen dieser Vereinbarung und jenen des Hauptvertrages haben die Bestimmungen dieser Vereinbarung **Vorrang**, wenn und soweit sie sich auf die Bearbeitung von Personendaten durch den Dienstleister im Rahmen des Hauptvertrages beziehen.

Die Bestimmungen dieser Vereinbarung gelten auch nach Beendigung des Hauptvertrages und bleiben so lange in Kraft, als der Dienstleister im Besitz der von dieser Vereinbarung erfassten Personendaten ist oder Zugriff auf diese hat.

Die Bestimmungen dieser Vereinbarung unterliegen schweizerischem Recht. Der Gerichtsstand ist im Rahmenvertrag festgelegt.

Anhang:
Technische & Organisatorische Massnahmen (TOM)

In der heutigen digitalen Welt sind der Datenschutz und die Informationssicherheit von höchster Bedeutung. Dies gilt insbesondere für Kommunikations- und EDI-Dienstleistungen wie iomarket. Um die Sicherheit und Vertraulichkeit der Nutzerdaten zu gewährleisten, ist die Anwendung effektiver technischer und organisatorischer Massnahmen (TOM) unerlässlich. In den folgenden Abschnitten werden die spezifischen Datenschutzmassnahmen dargelegt, die bei iomarket und der «gate2b-Plattform» implementiert sind, um die Einhaltung der Datenschutz- und Informationssicherheitsstandards sicherzustellen.

Die Massnahmen basieren auf dem Schweizer Bundesgesetz über den Datenschutz (DSG), welches eine solide Basis für die Sicherheit von Daten bietet. Gemäss DSG verpflichtet sich iomarket umfassende technische und organisatorische Massnahmen (TOM) zu ergreifen, um die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten zu gewährleisten.

Zusätzlich richtet sich iomarket nach der Datenschutzverordnung (DSV), um spezifische Sicherheitsbereiche detailliert abzudecken. Diese gesetzlichen Vorgaben sind der Leitfaden, um Daten sicher und geschützt zu halten.

1. Allgemeine Sicherheitsmassnahmen

Zutrittskontrolle

Regelt die Zutrittsberechtigungen der Organisation

- Klingelanlage mit Gegensprechanlage / Empfang
- Der Zutritt erfolgt mittels elektronischer Sicherheitsschlösser und zwei Sicherheitstüren
- Die Verwaltung der Zutrittsrechte erfolgt durch die Administration und wird protokolliert
- Die Verwaltung der Benutzerrechte erfolgt durch die Administratoren und wird protokolliert
- Besucher betreten die Geschäftsräume ausschliesslich in Begleitung der Mitarbeiter

- Sorgfalt bei Auswahl von Reinigungsdienst
- Schlüsselmanagement
- Besucherregistrierung

Zugangskontrolle

Stellt sicher, dass nur autorisierte Personen Zugang zu den Systemen haben

- Datenschutztresor
- Passwortvergabe
- Vergabe von Benutzerrechten
- Berechtigungs-/ Authentifizierung Konzepte mit auf das Nötigste (Need to Know?) beschränkten Zugriffsregulierungen
- Automatische Desktopstperre
- Zwei-Faktoren-Authentifizierung
- Verwendung von Hardware Firewalls
- Verwendung von Software Firewalls
- Verwendung von User Profilen

Zugriffskontrolle

Stellt sicher, dass die Datenverarbeitung gemäss den Berechtigungen erfolgt

- Benutzerberechtigungen
- Richtline Clean Desk
- Hardwareverschlüsselung
- Rechteverwaltung Systemadministratoren
- Sperrung von Zugriffsrechten bei Personalwechsel
- Passwort Richtlinien
- Sensibilisierung zur Verhinderung von Phishing

2. Spezifische Massnahmen

Übermittlungskontrolle

Massnahmen, um sicherzustellen, dass personenbezogene Daten während der Übermittlung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

- Verschlüsselung (z. B. TLS)
- Sicherung der Kommunikationskanäle
- Hardwareverschlüsselung

Auftragskontrolle

Sicherstellung, dass Daten im Auftrag nur gemäss den Anweisungen des Verantwortlichen verarbeitet werden.

- Abschluss von Auftragsverarbeitungsverträgen (AVV)
- Regelmässige Audits der Auftragsverarbeiter

3. Datenintegrität

Integritätskontrolle

Schutz der Daten vor zufälliger oder unberechtigter Veränderung. Sorgt für die Vollständigkeit und Unveränderlichkeit der Daten.

- Den Betrieb eines ISMS, dass die Datenintegrität sicherstellt und regelmässig auf den neuesten Stand gebracht wird.
- Schnelle und dokumentierte Reaktion auf Sicherheitsvorfälle durch unser CSIRT, um Integritätsverletzungen nachzuvollziehen und zu beheben.
- Kontinuierliche Überwachung aller Datenänderungen durch ein Monitoring-System.
- Ein umfassendes Identitäts- und Zugriffsmanagement, das den Zugang zu Daten streng regelt.
- Regelmässige Penetrationstests und ein aktives Bug Bounty Programm, um die Robustheit unserer Systeme zu testen und zu verbessern.
- Die Durchführung von OWASP Top 10-konformen Schulungen zur sicheren Software-Entwicklung, die die Qualität und Sicherheit unserer Produkte sicherstellt.
- Effektive Notfallpläne für den Fall von Integritätsverletzungen, die eine zügige Behebung garantieren

Verfügbarkeitskontrolle

Bezieht sich auf die ständige Zugänglichkeit und Funktionsfähigkeit von Systemen und Daten:

- Nutzung verschiedener Sicherheitstools, wie Malware-Scanner, Web Application
- Redundanter Cloud-Betrieb der iomarket-Applikationen: Gewährleistung einer hohen Verfügbarkeit.
- Regelmässige Durchführung von Backups: Sicherstellung der Datenverfügbarkeit und Wiederherstellbarkeit.
- Feuer und Rauchmeldeanlage
- Schaffung von Backup- & Wiederherstellungskonzepten
- Vorbereitung eines Emergency-Response-Plans
- Serverraum mit Klimaanlage

4. Organisatorische Massnahmen (Art. 26 DSG)

Beinhaltet Struktur und Prozesse innerhalb einer Organisation.

- Geeignete Organisationsstruktur für Informationssicherheit und Integration in organisationsweite Prozesse und Abläufe: Organisatorische Einbettung der Informationssicherheit.
- Konsequente Einbindung des ISO (Information Security Officer): Verantwortungszuweisung und Experten Einbindung.
- Schulung des gesamten Personals in Informationssicherheit und Datenschutz:

Wissensvermittlung und Bewusstseinsbildung.

- Regelmässige Informationen über Neuigkeiten zum Datenschutz und IT-Sicherheit: Informations- und Kommunikationspolitik.
- Unsere Informationssicherheits-Prinzipien sind fest in unsere Geschäftsprozesse integriert und werden durch regelmässige Schulungen und Prüfungen der Mitarbeiterkompetenz gestärkt.

5. Art und Zweck der Verarbeitung

Im Rahmen der Erfüllung des DL-Vertrages erhält der Auftragsbearbeiter Zugriff auf folgende Kategorien von Personendaten:

Art der personenbezogenen Daten

- Kundenstammdaten: Vor- und Nachname, Geburtsdatum, Adresse, Geburtstag, Nationalität, etc.
- Kunden-Daten des Kunden
- Betroffene Daten des Kunden
- Mitarbeiterstammdaten
- Adressdaten: Strasse, Hausnummer, PLZ, Ort, Land etc
- Meta- und Kommunikationsdaten (z.B. Telefon, E-Mail)
- Lieferdaten: Waren und Warenmengen, Lieferorte und – Zeitpunkte, Empfänger etc.
- Abrechnungsdaten: Kundenabrechnungen, Lieferantenabrechnungen etc.
- Inhaltdaten des Kunden

Kategorien der betroffenen Personen

Es sind Personendaten des folgenden Personenkreises betroffen:

- Kundendaten
- Lieferantendaten
- Mitarbeiter des Kunden
- Externe Mitarbeiter des Kunden
- Endkunden des Kunden
- Betroffene des Kunden
- Dienstleister des Kunden

Zweck der Datenverarbeitung

Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne des DSG. Die «Zwecke» sind zur Erbringung der vereinbarten Leistung erforderlichen Massnahmen.

Die Datenverarbeitung beinhaltet das Speichern von Daten, das Abrufen von Daten, das Schreiben und Auswerten von Aktivitätslog. Die Datenverarbeitung erfolgt ausschliesslich in einer geschützten Anwenderumgebung mit entsprechenden Zugriffsberechtigungen. Der

Auftragsverarbeiter ist berechtigt, auf seinen Systemen, im nötigen Ausmass zur Erfüllung seiner Aufgaben, seine personenbezogenen Daten zu verarbeiten.

Die Bearbeitung der Personendaten dient dem nachfolgenden Zweck:

- Automatisierung der Debitoren- und Kreditoren Prozesse des Verantwortlichen

Umfang und Zweck der Datenbearbeitung ergeben sich auch aus dem DL-Vertrag.

Die Parteien vereinbaren ausdrücklich, dass die in dieser Vereinbarung geregelten Pflichten im Umgang mit den Personendaten stets gilt, sobald und solange der Auftragsbearbeiter Personendaten des Verantwortlichen bearbeitet.

Ort der Datenverarbeitung

Die Bearbeitung erfolgt ausschliesslich in der Schweiz. Dem Auftragsbearbeiter ist untersagt, Personendaten ausserhalb der Schweiz zu bearbeiten.

Rückgabe und Löschung

Nach Abschluss der Erbringung der vereinbarten Dienstleistung verpflichtet sich der Dienstleister, alle Personendaten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, sofern nicht nach Datenschutzrecht oder sonstigem anwendbaren Recht eine Verpflichtung zur Speicherung der Personendaten besteht. Die Löschung der Daten erfolgt nach 30 Tagen nach Erbringung der Dienstleistung.

6. Sensibilisierung und Schulung

Mitarbeiterschulungen

Regelmässige Schulungen und Sensibilisierungsmassnahmen für den Datenschutz.

Beispiele:

- E-Learning-Programme
- Präsenzschulungen zu DSG-relevanten Themen

7. Kontinuierliche Verbesserung

Auditierung und Überprüfung

Regelmässige Prüfung der implementierten Massnahmen auf Wirksamkeit

Beispiele:

- interne und externe Audits
- Datenschutz-Folgeabschätzung