Allgemeine Geschäftsbedingungen (AGB)

Gültig ab: 01.05.2024

1. Anwendungsbereich, Geltung und Definitionen

1.1 Diese Allgemeinen Geschäftsbedingungen («AGB») regeln Abschluss, Inhalt und Abwicklung von Verträgen über Beschaffung und Nutzung der von Staffgenius GmbH entwickelten Plattformen und deren Wartung.

2. Angebot

2.1 Die Staffgenius GmbH entwickelt die Software inplan für die Personaleinsatzplanung (nachfolgend «Plattform»). Es handelt sich dabei um Standard-Software, die für den Einsatz bei einer Vielzahl von Kunden konzipiert ist. Diese kann auf die Verhältnisse des Kunden angepasst werden (Parametrisierung). Bei inplan handelt es sich um eine browserbasierte Plattform, welche es dem Kunden ermöglicht, die Dienstplanung und Auswertung durchzuführen. Die Mitarbeitenden können im eigenen Benutzerkonto Dienstwünsche und Präferenzen festlegen und sich selbst einplanen, sowie den veröffentlichten Dienstplan anschauen.

2.2 Das Recht auf Supportleistungen gilt lediglich so lange, wie inplan vom Anbieter angeboten wird.

3. Leistungen des Anbieters

3.1 Der Anbieter gewährleistet, dass die von ihr gelieferten Produkte und vertraglichen Leistungen die vereinbarten Eigenschaften aufweisen, ferner diejenigen Eigenschaften, welche dem Auftraggeber auch ohne besondere Vereinbarung nach dem jeweiligen Stand der Technik bei Vertragsabschluss (sofern sich aus dem Vertrag nicht etwas Anderes ergibt) und in guten Treuen voraussetzen darf.

3.2 Der Anbieter gewährt dem Kunden Zugang auf eine eigene Kundeninstanz, über welche der Kunde die Plattform nutzen kann. Der Zugang ist 24 Stunden an 365 Tagen pro Jahr gewährleistet unter Vorbehalt des in Ziff. 16 definierten Haftungsausschlusses.

3.3 Der Anbieter behält sich das Recht vor ihre Plattformen vorübergehend ganz oder teilweise nicht verfügbar zu machen. Eine eingeschränkte Verfügbarkeit oder Nichtverfügbarkeit der Plattform kann sich insbesondere dann ergeben, wenn Wartungsarbeiten ausgeführt werden. Der Anbieter unternimmt alle zumutbaren Anstrengungen, um die Unterbrüche auf ein Minimum zu beschränken und planmässige Wartungen im Voraus anzukündigen.

4. Art und Umfang der Nutzung

4.1 Der Anbieter gewährt dem Kunde ein nicht-exklusives, nicht übertragbares Recht zur Nutzung der Plattform gemäss den Bestimmungen des Vertrages.

4.2 Jede Zuwiderhandlung gegen dieses Nutzungsrecht stellt einen wichtigen Grund dar, der den Anbieter berechtigt, den Vertrag fristlos aufzulösen und überdies Schadenersatz zu verlangen.

5. Schutzrechte

5.1 Alle Rechte an der Plattform und an den darin enthaltenen Materialien, wie insbesondere das Eigentum und die Urheberrechte, bleiben bei der Staffgenius GmbH oder ihrer Lizenzgebern. bzw. den Urhebern, auch wenn daran Änderungen oder Erweiterungen vorgenommen werden.

6. Unterstützung und Mitwirkungspflichten des Kunden

6.1 Der Kunde schafft in seinem Betrieb alle Voraussetzungen für die erfolgreiche Einführung der Plattform und verpflichtet sich, dem Anbieter rechtzeitig alle notwendigen Informationen über Zielsetzungen und organisatorische Gegebenheiten zu liefern, welche für eine erfolgreiche Nutzung erforderlich sind. Insbesondere gilt dies auch in Bezug auf die Supportleistungen.

6.2 Der Kunde ist zudem für Auswahl, Gebrauch und Unterhalt der im Zusammenhang mit der Plattform eingesetzten Informatiksysteme, weiterer Programme und Datensysteme sowie die dafür erforderlichen Dienstleistungen zuständig und stellt die für den Einsatz der Plattform geeignete Aufbauund Ablauforganisation bereit.

6.3 Für die erfolgreiche Nutzung der Plattform wird folgendes vorausgesetzt:

- Zurverfügungstellung der notwendigen Daten für die Erstellung der Kundeninstanz
- Hardware (Computer, Tablet, Smartphone)
- Internetzugang
- Webbrowser: Microsoft Edge, Mozilla Firefox, Google Chrome oder Safari (jeweils aktuelle Version)

7. Fernzugriff

7.1 Erbringt die Anbieterin Leistungen via Fernzugriff, so trifft sie angemessene technische und organisatorische Vorkehrungen, dass der Datenverkehr vor unbefugtem Zugriff durch Dritte geschützt ist und dass die Verpflichtungen zur Geheimhaltung und dem Datenschutz eingehalten werden.

8. Weiterentwicklungen/Updates

8.1 Bei Modifikationen, Erweiterungen oder neu erstellten Versionen der Plattform erhält der Kunde automatisch die neuste Version. Allfällige Dokumentationen werden vom Anbieter entsprechend aktualisiert. Die Form der Dokumentation muss angemessen sein, kann vom Anbieter jedoch frei bestimmt werden.

9. Backup auf Verlangen

9.1 Werden Daten beim Kunden durch Bedienungsfehler oder Ereignisse höherer Gewalt gelöscht, so kann der Kunde beim Anbieter kostenpflichtig ein Backup der entsprechenden Daten verlangen und die Daten wiederherstellen lassen.

10. Gewährleistung

10.1 Der Anbieter garantiert die Funktionalität der Plattform. Die Garantie bezieht sich ausschliesslich auf den bestimmungsgemässen Gebrauch der Plattform. Der Anbieter übernimmt weder Garantie noch Haftung für Fehler oder Probleme von der Plattform, welche auf nicht von ihm zu vertretende Umstände zurückzuführen sind. Dazu gehören insbesondere:

- nicht autorisierte Eingriffe auf die Kundeninstanz durch den Kunden oder Dritte
- Bedienungsfehler von Kunden oder Dritt-Personal
- Einflüsse von durch Dritte gelieferten Systemen oder Programmen. Neben weiterer Plattformprovider gelten auch die Provider des Browsers und des Internetzugangs als Dritte;
- Hosting: Die Plattform wird vom Anbieter auf geeigneten Servern in der Schweiz betrieben. Der Anbieter kann nicht für allfällige Ausfälle der Serverinfrastruktur oder technische Probleme derselben verantwortlich gemacht werden und übernimmt keinerlei Haftung oder Schadensersatzansprüche.

10.2 Die Garantie des Anbieters beschränkt sich auf die kostenlose Korrektur von Problemen oder Fehlern innert nützlicher Frist nach seiner Wahl.

10.3 Erhebliche Mängel sind innerhalb von zehn Tagen nach Feststellung beim Anbieter schriftlich geltend zu machen.

11. Geheimhaltung

11.1 Die Parteien behandeln alle Tatsachen und Informationen vertraulich, die weder offenkundig noch allgemein zugänglich sind. Im Zweifelsfall sind Tatsachen und Informationen vertraulich zu behandeln. Die Parteien verpflichten sich, alle wirtschaftlich zumutbaren sowie technisch und organisatorisch möglichen Vorkehrungen zu treffen, damit vertrauliche Tatsachen und Informationen gegen den Zugang und die Kenntnisnahme durch Unbefugte wirksam geschützt sind.

11.2 Die Geheimhaltungspflicht besteht schon vor Vertragsabschluss und dauert nach Beendigung des Vertragsverhältnisses fort.

11.3 Die Parteien überbinden die Geheimhaltungspflicht auf ihre Mitarbeitenden, Subunternehmer, Unterlieferanten sowie weitere beigezogene Dritte.

11.4 Der Kunde stellt sicher, dass Dritte keinen unerlaubten Zugriff auf die Plattform erlangen, und gewährleistet die Geheimhaltung der Passwörter.

11.5 Verletzt der Kunde die vorstehenden Geheimhaltungspflichten, so schuldet sie dem Anbieter eine Konventionalstrafe, sofern sie nicht beweist, dass sie kein Verschulden trifft. Diese beträgt pro Verstoss CHF 50'000. Die Bezahlung der Konventionalstrafe befreit nicht von der Einhaltung vertraglicher Pflichten und wird an allfällige Schadenersatzforderungen angerechnet.

12. Datenschutz und Auftragsbearbeitung

12.1 Zum Zwecke der Vertragsabwicklung und des Marketings werden Personendaten des Kunden von uns und von uns beauftragten Dienstleistern unter Beachtung der geltenden Datenschutzbestimmungen erhoben und bearbeitet. Weitere Informationen zur Bearbeitung von Personendaten finden Sie in unserer Datenschutzerklärung auf den jeweiligen Websites.

12.2 Soweit wir Personendaten als Auftragsbearbeiter im Sinne des Datenschutzgesetzes bearbeiten, erfolgt dies auf der Grundlage der Auftragsbearbeitungsvereinbarung («ABV») Diese Vereinbarung ist integraler Bestandteil unserer AGB (siehe Anhang A).

12.3 Betreffend Plattformen verpflichtet sich der Anbieter, die Datensicherheit und den Datenschutz mit angemessenen zur Verfügung stehenden technischen und organisatorischen Möglichkeiten zu gewährleisten.

13. Haftung

13.1 Die Anbieterin lehnt jede Haftung, die im Zusammenhang mit der Erbringung ihrer Dienstleistungen beim Kunden entstehen kann, ab, sofern es sich um leichtoder mittelfahrlässige Sorgfaltspflichtverletzungen handelt. Für die Haftung ihrer Hilfspersonen lehnt die Auftragnehmerin jegliche Haftung für Schäden ab (insbesondere Beschädigungen von Installationen, Maschinen oder Computern, Datenverlust etc.).

13.2 Die Anbieterin haftet nur für absichtlich oder grobfahrlässig nachweisbar entstandenen Schaden beim Kunden. Haftung für Folgeschäden und mittelbare Schäden ist in jedem Fall ausgeschlossen.

14. Schlussbestimmungen

14.1 Änderungen und Ergänzungen des Vertrages sowie dessen Aufhebung bedürfen der Schriftform.

14.2 Auf das Vertragsverhältnis gilt schweizerisches Recht unter Ausschluss des UN-Kaufrechts.

14.3 Für alle Streitigkeiten ist, soweit nicht vertragliche oder gesetzlich zwingend etwas anderes bestimmt ist, der Gerichtsstand Winterthur vereinbart.

14.4 Erweisen sich einzelne Bestimmungen als ungültig oder rechtswidrig, so wird die Gültigkeit des Vertrages davon nicht berührt. Die betreffende Bestimmung soll in diesem Fall durch eine wirksame, wirtschaftlich möglichst gleichwertige Bestimmung ersetzt werden. Gleiches gilt im Falle einer Vertragslücke.

Anhang A – Auftragsbearbeitungsvereinbarung (ABV)

1. Gesetzliche Grundlagen und Anwendungsbereich der ABV

1.1 Der Auftragnehmer erbringt für den Auftraggeber Dienstleistungen, die auch die Bearbeitung von Personendaten (Art. 5 a, 5 d DSG) umfassen und eine Auftragsbearbeitung darstellen (Art. 9 DSG). Die nachfolgenden Hinweise gelten auch für Leistungen, bei denen die EU-DSGVO oder andere Datenschutzgesetze Anwendung finden.

1.2 Die ABV findet Anwendung auf alle Hauptverträge, die mit dem Auftragnehmer abgeschlossen werden und die eine Bearbeitung von Personendaten («Auftragsdaten») umfassen. Die Bestimmungen dieser ABV ergänzen diejenigen des Hauptvertrages und schränken die Rechte und Pflichten der Parteien hinsichtlich der Erbringung bzw. Inanspruchnahme der Leistungen nicht ein.

1.3 Die ABV regelt die Rollen, Verantwortlichkeiten und Pflichten zwischen dem Auftragnehmer und dem Auftraggeber («Parteien») bei der Auftragsbearbeitung.

1.4 Diese ABV gilt nicht für Bearbeitungen von Personendaten, bei denen der Auftragnehmer als selbständiger Verantwortlicher handelt und die Zwecke der Bearbeitung bestimmt.

2. Gegenstand und Zweck der Auftragsbearbeitung

2.1 Gegenstand und Zweck der Auftragsbearbeitung ist die Erfüllung der vertraglich vereinbarten Leistungen durch den Auftragnehmer für den Auftraggeber. Die Auftragsbearbeitung besteht in der Erhebung, Bearbeitung und dem Zugriff auf Auftragsdaten gemäss den Bestimmungen des Hauptvertrages.

2.2 Die Auftragsbearbeitung gilt für Auftragsdaten, die der Auftragnehmer im Rahmen des Betriebs, der Wartung und der Datensicherung von der Plattform wie inplan und der damit verbundenen Dienste und Funktionalitäten sowie der Erbringung von Service und Support bearbeitet oder auf die er Zugriff erhält. Die Kategorien der Betroffenen sind abhängig von den übermittelten Auftragsdaten die Kunden, Mitarbeiter, Lieferanten, Geschäftspartner etc. des Auftraggebers.

3. Rollen und Verantwortlichkeiten der Parteien

3.1 Der Auftraggeber hat in Bezug auf die Bearbeitung von Auftragsdaten die Rolle des Verantwortlichen (Art. 5 j DSG).

3.2 Der Auftragnehmer hat in Bezug auf die Bearbeitung von Auftragsdaten die Rolle des Auftragsbearbeiters (Art. 5 k DSG).

4. Pflichten des Auftragnehmers

4.1 Er verpflichtet sich, die Auftragsdaten nur zur Erbringung der vertraglich vereinbarten Leistungen und auf der Grundlage dieser ABV zu bearbeiten.

4.2 Weitergehende schriftliche Weisungen wird er nur annehmen, soweit diese nicht gegen offensichtliche datenschutzrechtliche Bestimmungen verstossen. Er kann sie dann ablehnen, wenn sie unzumutbar sind, durch Änderung der vertraglich vereinbarten Leistungen zu Mehrkosten führen oder durch sie gesetzliche oder behördliche Auflagen nicht erfüllt werden können.

4.3 Er verpflichtet sich, angemessene technische und organisatorische Massnahmen (TOM) zu treffen, um die Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Bearbeitung von Auftragsdaten zu gewährleisten. Da die TOM dem technischen Fortschritt unterliegen, ist er berechtigt, alternative und adäquate Massnahmen umzusetzen, sofern das Sicherheitsniveau der hier festgelegten Massnahmen nicht unterschritten wird. Die TOM sind in der Beilage 1 detailliert aufgeführt.

4.4 Er verpflichtet sich, unverzüglich schriftlich zu informieren, wenn ihm eine Verletzung der Datensicherheit bekannt wird, die Auftragsdaten betrifft. Er wird unverzüglich die erforderlichen Massnahmen treffen, um den Schutz der Auftragsdaten sicherzustellen und darüber informieren. Darüber hinaus verpflichtet er sich auf schriftliche Anforderung die erforderlichen Informationen zur Verfügung zu stellen, damit etwaige Meldeund Dokumentationspflichten im Zusammenhang mit der Datensicherheitsverletzung nachgekommen werden kann.

4.5 Er unterstützt auf schriftliche Anforderung und gegen angemessene zusätzliche Vergütung bei der Erfüllung von Betroffenenrechten und Datenschutz-Folgeabschätzungen in Bezug auf die Auftragsdaten.

4.6 Wendet sich ein Betroffener mit seinen Betroffenenrechten direkt an uns, wird er unverzüglich an den Auftraggeber verweisen.

4.7 Er stellt sicher, dass die bei Ihm mit der Auftragsbearbeitung befassten Personen die Datenschutzgrundsätze einhalten, und verpflichtet sie zur Vertraulichkeit, auch über die Dauer ihrer Tätigkeit hinaus.

4.8 Er wird die Auftragsdaten nach Beendigung der Zusammenarbeit auf Verlangen zurückgeben oder löschen, soweit dem keine gesetzlichen Aufbewahrungsfristen oder berechtigten Interessen entgegenstehen.

5. Nachweise und Überprüfungen des Auftragnehmers

5.1 Er stellt dem Auftraggeber auf schriftliches Verlangen Informationen zur Verfügung, um die Einhaltung dieser ABV nachzuweisen.

5.2 Er wird dem Auftraggeber oder einem von diesem beauftragten Auditor mit einer Vorankündigungsfrist von 15 Tagen, unter Wahrung der Verhältnismässigkeit und nach vorheriger Zusicherung der Vertraulichkeit gestatten, die Einhaltung dieser ABV auf Kosten des Auftraggebers zu überprüfen. Werden bei der Überprüfung relevante Abweichungen festgestellt, hat er diese unverzüglich und unentgeltlich zu beseitigen.

6. Datenübermittlung ins Ausland

6.1 Die Datenbearbeitungen erfolgen primär am Standort des Auftragnehmers in der Schweiz. Durch die Zusammenarbeit mit Sub-Auftragsbearbeitern können Daten auch von diesen und auch ausserhalb der Schweiz bearbeitet werden. Werden Datenbearbeitungen im Ausland durchgeführt, so erfolgt dies auf der Grundlage des Angemessenheitsbeschlusses gemäss Anhang zur Datenschutzverordnung (DSV), auf der Grundlage der vom Eidgenössischen Datenschutzund Öffentlichkeitsbeauftragten (EDÖB) genehmigten Standarddatenschutzklauseln (EU-SCC) oder auf der Grundlage verbindlicher interner Datenschutzvorschriften.

7. Einsatz von Sub-Auftragsbearbeitern

7.1 Der Auftragnehmer ist grundsätzlich berechtigt, im Sinne der allgemeinen Genehmigung (Art. 7 DSV) Sub-Auftragsbearbeiter zur Erfüllung seiner Verpflichtungen heranzuziehen. Von der Sub-Auftragsbearbeitung zu unterscheiden sind Fälle, in denen der Auftraggeber einen direkten Vertrag mit dem Drittdienstleister abschliesst.

7.2 Die gegenwärtig vom Auftragsbearbeiter eingesetzten Sub-Auftragsbearbeiter sind in Beilage 2 aufgeführt.

7.3 Der Auftragnehmer informiert den Auftraggeber vorab über Änderungen bei den Sub-Auftragsbearbeitern und räumt ihm das Recht ein, aus berechtigten Gründen innerhalb von 30 Tagen schriftlich zu widersprechen. Im Falle eines Widerspruchs ist die Vertragserfüllung möglicherweise nicht mehr im bisherigen Umfang möglich ist. Können sich die Parteien nicht innerhalb von 30 Tagen einigen, kann die betroffene Leistung ausserordentlich gekündigt werden, sofern der Auftraggeber nachweist, dass der Widerspruch datenschutzrechtlich notwendig ist.

Anhang A – Beilage 1: Technisch organisatorische Massnahmen

Im Rahmen der Auftragsbearbeitung werden dem Risiko angemessene technische und organisatorische Massnahmen (TOM) getroffen, um Verletzungen der Datensicherheit weitestgehend zu vermeiden (Art. 8 DSG). Die Massnahmen orientieren sich an den vom Bundesrat erlassenen Mindest-anforderungen an die Datensicherheit aus der Datenschutzverordnung (Art. 1-3 DSV).

Die Daten werden ihrem Schutzbedarf entsprechend:
- nur Berechtigten zugänglich gemacht (Vertraulichkeit)
- sind verfügbar, wenn sie benötigt werden (Verfügbarkeit)
- sollen nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität)
- und müssen nachvollziehbar bearbeitet werden (Nachvollziehbarkeit)

Die folgend dokumentierten Massnahmen gelten für die Bearbeitung von Auftragsdaten gemäss Anhang A.

Zugriffskontrolle
Zur Gewährleistung der Verfügbarkeit und Integrität haben Auftraggeber und Auftragnehmer geeignete Massnahmen zu treffen, damit berechtigte Personen nur Zugriff auf diejenigen Personendaten erhalten, die sie zur Erfüllung ihrer Aufgaben benötigen (Zugriffskontrolle DSV Art. 3, 1a).

Zugriffsrechte nach dem Need-to-know-Prinzip	Durch Zugriffsrechte wird sichergestellt, dass nur diejenigen Mitarbeiter Zugriff auf Personendaten haben, die diese zur Erfüllung ihrer auftragsspezifischen Aufgaben benötigen. Dies gilt sowohl für physische als auch für digitale Datenspeicher. Zugriffsrechte werden nach dem Need-to-know-Prinzip vergeben.
Protokollierung der Zugriffe	Die Zugriffe auf die im Rahmen der Auftragsabwicklung genutzten Systeme werden protokolliert.
Bildschirmsperre bei Inaktivität	Geräte zur Auftragsbearbeitung wie Notebooks und Computer sind mit einer automatischen Bildschirmsperre bei Inaktivität versehen.
Clean-Desk-Policy	In den Räumlichkeiten des Auftraggebers wird eine Clean-Desk-Policy eingehalten. Dies bedeutet, dass Schreibtische und andere Flächen frei von Auftragsdaten zu hinterlassen sind.
Test und Produktivsystem	Neben dem Produktivsystem können Testsysteme zur Verfügung stehen, in denen Änderungen getestet werden können, bevor sie in das Produktivsystem übernommen werden.
Separierte Datenbestände gemäss Trennungsprinzip	Werden Systeme für die gemeinsame Nutzung durch mehrere Kunden eingesetzt, so erfolgt dies mit getrennten logischen Datenbeständen und mandantenfähigen Systemen.
Authentifizierung und Autorisierung	Die Clientund Serversysteme, die der Auftragnehmer zur Durchführung des Auftrags verwendet, sind durch Authentifizierungsund Autorisierungssysteme geschützt.
Multi-Faktor-Authentifizierung	Die Multi-Faktor-Authentifizierung für Administratoren und Mitarbeitende ist wo technisch möglich aktiviert, insbesondere auch für externe Zugriffe.

Zugangskontrolle

Zur Gewährleistung der Verfügbarkeit und Integrität haben Auftraggeber und Auftragnehmer geeignete Massnahmen zu treffen, damit nur berechtigte Personen Zutritt zu den Räumlichkeiten und Einrichtungen haben, in denen Personendaten bearbeitet werden (Zugangskontrolle DSV Art. 3, 1b).

Physische Sicherheit	Der Zugang zu Räumen mit Auftragsdaten ist auf befugte Personen beschränkt.
Serverraum	Die Server befinden sich in einem externen Rechenzentrum in der Schweiz. Nur autorisierte Personen haben Zugang zum Rechenzentrum.
Segmentierung der Netzwerke	Die Netzwerke sind segmentiert und das Netzwerk mit Zugriff auf Auftragsdaten eingeschränkt.
VPN-Technologie für externe Zugriffe	Externe Zugriffe auf andere Systeme erfolgen nach Möglichkeit über VPNVerbindungen, die mit ausreichender Kryptographie gesichert sind.

Benutzerkontrolle

Zur Sicherstellung der Verfügbarkeit und Integrität haben Auftraggeber und Auftragnehmer durch geeignete Massnahmen zu verhindern, dass Unbefugte automatisierte Datenbearbeitungssysteme mittels Einrichtungen zur Datenübertragung benutzen können (Benutzerkontrolle DSV Art. 3, 1c).

Personenbezogene Accounts	Soweit möglich werden personenbezogene Zugänge und Kennungen («Accounts») vergeben.
Geregelter Austrittsprozess	Ein geregelter Austrittsprozess ist in Kraft, der verhindert, dass Mitarbeitende nach dem Ausscheiden aus dem Unternehmen auf Auftragsdaten zugreifen können.
Passwortrichtlinie	Es gilt eine Passwortrichtlinie, die besagt, dass Passwörter ausreichend komplex und sicher sein müssen.
PIN für Mobilgeräte	Mobile Geräte sind mit einem Passwort oder einer PIN geschützt.
Client-Zertifikate	Für den Zugriff auf die Systeme werden Client-Zertifikate verwendet, um die Sicherheit zusätzlich zu erhöhen.
Verschlüsselung und Geheimhaltung der Authentifizierungsdaten	Der Auftragnehmer stellt sicher, dass Authentifizierungsdaten, insbesondere Passwörter und kryptografische Schlüssel, gegenüber Unbefugten streng geheim gehalten werden. Diese Daten dürfen nicht im Klartext und nur mit geeigneter Verschlüsselung gespeichert werden.
Beschränkung der Administrationsrechte	Die Vergabe von Administratorrechten ist auf die unbedingt notwendigen Mitarbeiter des Auftragnehmers beschränkt.

Datenträgerkontrolle

Zur Gewährleistung der Verfügbarkeit und Integrität haben Auftraggeber und Auftragnehmer geeignete Massnahmen zu treffen, damit Datenträger nicht unbefugt gelesen, kopiert, verändert, verschoben, gelöscht oder vernichtet werden können (Datenträgerkontrolle DSV Art. 3, 2a).

Verschlüsselung von mobilen Datenträgern	Mobile Datenträger und Geräte werden mit ausreichend starker Kryptographie verschlüsselt.
Fachgerechte Entsorgung der Datenträger	Datenträger werden fachgerecht entsorgt, wenn sie nicht mehr benötigt werden, das gilt für Geräte wie Computer, Notebooks, Smartphones, Tablets und Drucker usw.
Fachgerechte Entsorgung von Papierunterlagen	Papierdokumente werden entsprechend ihrer Klassifizierung fachgerecht entsorgt oder geschreddert.

Speicherkontrolle

Um die Verfügbarkeit und Integrität zu gewährleisten, müssen der Auftraggeber und der Auftragnehmer geeignete Massnahmen treffen, um zu verhindern, dass unbefugte Personen Personendaten im Speicher ablegen, lesen, verändern, löschen oder vernichten können (Speicherkontrolle DSV Art. 3, 2b).

Virenschutz	Alle Clientgeräte sind mit einem Virenschutz ausgestattet.
Fernlöschmöglichkeiten	Es besteht die Möglichkeit, Daten auf mobilen Geräten per Fernzugriff zu löschen. Die Mitarbeiter sind angewiesen, den Verlust eines Gerätes unverzüglich zu melden.

Transportkontrolle

Zur Sicherstellung der Verfügbarkeit und Integrität haben der Auftraggeber und der Auftragnehmer geeignete Massnahmen zu treffen, damit bei der Bekanntgabe von Personendaten oder beim Transport von Datenträgern Personendaten nicht unbefugt gelesen, kopiert, verändert, gelöscht oder vernichtet werden können (Transportkontrolle DSV Art. 3, 2c).

Sicherer Datenaustausch Extern	Sensitive Auftragsdaten werden unter Einsatz geeigneter Verschlüsselungstechnologien und nicht via unverschlüsselte E-Mail an Kunden, Mitarbeiter oder Lieferanten versendet, es sei denn dieser Kanal wird von der Gegenstelle explizit gewählt.
Sicherer Datenaustausch intern	Anstatt eine E-Mail mit Anhang zu versenden, werden die Auftragsdaten intern über einen Link zugänglich gemacht, um eine Verteilung in unstrukturierten Postfächern zu vermeiden.
Einsatz von Verschlüsselung für mobile Datenträger	Auftragsdaten auf mobilen Datenträgern sind durch den Einsatz von Verschlüsselungstechnologien vor unberechtigten Auslesen geschützt.
Transportverschlüsselung	Es wird darauf geachtet, dass bei der Übermittlung von Auftragsdaten nur verschlüsselte Kanäle wie Webplattformen mit https verwendet werden.
Überwachung von ein- und ausgehendem Netzwerkverkehr	Es wird sichergestellt, dass der einund ausgehende Netzwerkverkehr überwacht wird.

Wiederherstellung

Zur Gewährleistung der Verfügbarkeit und Integrität haben Auftraggeber und Auftragnehmer geeignete Massnahmen zu treffen, damit bei einem physischen oder technischen Zwischenfall die Verfügbarkeit der Personendaten und der Zugriff auf diese rasch wiederhergestellt werden können (Wiederherstellung DSV Art. 3, 2d), alle Funktionen des automatisierten Datenbearbeitungssystems zur Verfügung stehen (Verfügbarkeit), Störungen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten durch Fehlfunktionen des Systems nicht beschädigt werden können (Datenintegrität DSV Art. 3, 2e).

Notfallplan	Es existiert ein Notfallplan, der bei Ausfällen/Desastern wie Ransomware Verschlüsselung, Brand oder Hardwareausfall angewendet werden kann.
Redundante Systeme und Hochverfügbarkeit	Wichtige Serversysteme und Netzwerkkomponenten, die Auftragsdaten enthalten, sind redundant ausgelegt, damit bei einem Ausfall der Zugriff schnellstmöglich wiederhergestellt werden kann.
Backupkonzept	Ein Backup-Konzept ist implementiert. Es ist sichergestellt, dass Auftragsdaten im Backup enthalten sind und Datenbanken konsistent gesichert werden. Ein Generationsprinzip mit einer angemessenen und definierten Aufbewahrungsfrist ist implementiert. Daten werden verschlüsselt übertragen und gespeichert.
Unterbrechungsfreie Stromversorgung	Unterbrechungsfreie Stromversorgungen stellen sicher, dass Serversysteme bei Stromausfall ohne Datenverlust heruntergefahren werden können. Zusätzlich dienen sie als Überspannungsschutz gegen Stromspitzen.

Überwachungssystem	Es ist ein zentrales Überwachungssystem im Einsatz, das kritische Komponenten der Infrastruktur überwacht und so ein proaktives Eingreifen bei Systemwarnungen ermöglicht.
Rasche Wiederherstellbarkeit	Backups sind so angelegt, dass nicht nur Auftragsdaten, sondern ganze Systeme schnell wiederhergestellt werden können. Es wird regelmässig getestet, ob die Daten wiederhergestellt werden können.

Systemsicherheit

Zur Gewährleistung der Verfügbarkeit und Integrität haben Auftraggeber und Auftragnehmer durch geeignete Massnahmen dafür zu sorgen, dass Betriebssysteme und Anwendungssoftware stets auf dem aktuellen Sicherheitsstand gehalten und bekannte kritische Schwachstellen geschlossen werden (Systemsicherheit DSG Art. 3, 2f).

Wartung und Aktualisierung von Servern und Anwendungen	Server und Anwendungen werden regelmässig, mindestens monatlich, mit Updates versorgt.
Aktualisierung von Clientgeräten	Es wird sichergestellt, dass Clientgeräte wie Computer, Notebooks und mobile Geräte regelmässig aktualisiert werden. Dies wird zentral überwacht.
Lifecycle der Hardund Plattform	Die Lifecycles von Hardund Software werden berücksichtigt und Systeme, die vom Hersteller nicht mehr mit Updates versorgt werden, werden rechtzeitig ersetzt.
Systemhärtung	Beim Einsatz von Servern wird darauf geachtet, dass eine Firewall aktiv ist, nicht benötigte Dienste deaktiviert sind und Best Practices zur Härtung der Betriebssysteme angewendet werden.

Eingabekontrolle

Zur Gewährleistung der Nachvollziehbarkeit müssen Auftraggeber und Auftragnehmer geeignete Massnahmen treffen, damit nachvollzogen werden kann, welche Personendaten zu welcher Zeit und von welcher Person in das automatisierte Datenverarbeitungssystem eingegeben oder verändert worden sind (Eingabekontrolle DSG Art. 3, 3a).

Individuelle Benutzerkonten	Die Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Auftragsdaten in den verwendeten Serversystemen wird, wo technisch möglich durch die Verwendung individueller Benutzerkonten gewährleistet.
Protokollierung der Zugriffe	Die Zugriffe auf die Systeme im Rahmen der Auftragsabwicklung werden überwacht und die Logs gespeichert.

Bekanntgabekontrolle

Zur Sicherstellung der Nachvollziehbarkeit haben der Auftraggeber und der Auftragnehmer geeignete Massnahmen zu treffen, damit überprüft werden kann, wem Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden (Bekanntgabekontrolle DSG Art. 3, 3b).

Beschränkung externer Freigaben	Die externe Freigabe von Auftragsdaten ist beschränkt, um die Freigabe vertraulicher Daten zu verhindern.
Mitarbeiterweisung für externe Freigaben	Die Mitarbeiter sind angewiesen, für vertrauliche Daten dem Risiko angemessene Übertragungskanäle zu verwenden. Dadurch wird verhindert, dass z.B. Zugangsdaten unverschlüsselt per E-Mail versendet werden.

Anhang A – Auftragsbearbeitungsvereinbarung (ABV)

Die Liste der genehmigten Sub-Auftragsbearbeiter ist nachstehend aufgeführt. Soweit möglich sind die Länder angegeben, in denen die Datenbearbeitung erfolgt. Für weitere Informationen über die Datenbearbeitung durch die Sub-Auftragsbearbeiter wird auf deren Datenschutzerklärung verwiesen, die über die Websites zugänglich ist.

Bearbeiter	Umfang und Zweck	Grundlage des Exports	Länder der Datenbearbeitung
Microsoft Ireland Operations, Ltd., Attn: Data Privacy, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	Kommunikation und Datenablage	Data Processing Agreement / EU-SCC	Die Daten werden je nach Anwendung in der Schweiz oder in der EU gespeichert, der Zugriff kann aber auch aus anderen Ländern, insbesondere den USA, erfolgen.
CodeTwo, ul. Wolności 16, 58-500 Jelenia Góra, Polen	Zentrale Verwaltung von E-Mail-Signaturen	Data Processing Agreement	Die Daten werden von CodeTwo in Polen, der EU und in der Microsoft Cloud bearbeitet.
Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L1855, Luxemburg	Transaktionelle SMS und E-Mails für Kommunikation und Authentifizierungszwecke	Data Processing Agreement / EU-SCC	Die Daten werden in der EU gespeichert, der Zugriff kann aber auch aus anderen Ländern, insbesondere den USA, erfolgen.
Digital Realty Switzerland GmbH, Bäulerwisenstrasse 6, 8152 Glattbrugg, Schweiz	Miete von Rackspace im Rechenzentrum in der Schweiz, der Rechenzentrumsanbieter hat keinen Zugriff auf Daten.	Kein Datenexport	Die Daten sind in einem Rechenzentrum in der Schweiz gespeichert.