BOS-ID Vertragswerk für Software-as-a-Service-Leistungen

bestehend aus:

- Allgemeine Geschäftsbedingungen (AGB)
- Leistungsbeschreibung und Nutzungsbedingungen
- Service Level Agreement (SLA)
- Auftragsverarbeitungsvertrag (AVV)
- Technische und organisatorische Maßnahmen (TOMs)
- Verzeichnis der Unterauftragsverarbeiter
- Informationssicherheitsrichtlinie

Vertragspartner sind die MP-BOS GmbH (nachfolgend „Anbieter") und der jeweilige Vertragspartner gemäß Angebot, Auftrag, Bestellformular oder sonstiger individueller Vereinbarung (nachfolgend „Kunde").

Allgemeine Geschäftsbedingungen (AGB)

§ 1 Geltungsbereich

(1) Diese Allgemeinen Geschäftsbedingungen („AGB") gelten für Verträge über die Bereitstellung und Nutzung der Software-as-a-Service-Lösung „BOS-ID" zwischen der MP-BOS GmbH („Anbieter") und dem jeweiligen Vertragspartner („Kunde"). Für gesondert beauftragte Zusatzleistungen, insbesondere Beratungs-, Schulungs-, Migrations-, Integrations-, Projekt- oder Entwicklungsleistungen, gelten diese AGB ergänzend, soweit keine spezielleren Vereinbarungen getroffen wurden.

(2) Das Angebot des Anbieters richtet sich ausschließlich an Unternehmer im Sinne des § 14 BGB, juristische Personen des öffentlichen Rechts sowie öffentlich-rechtliche Sondervermögen. Verträge mit Verbrauchern im Sinne des § 13 BGB werden nicht geschlossen.

(3) Diese AGB gelten für Kunden mit Sitz in der Bundesrepublik Deutschland sowie in anderen Mitgliedstaaten der Europäischen Union, soweit nicht zwingende gesetzliche Vorschriften des jeweiligen Staates entgegenstehen.

(4) Maßgeblich für den Vertragsinhalt sind in folgender Reihenfolge:
a) das individuelle Angebot bzw. der Einzelvertrag,
b) diese AGB,
c) die Leistungsbeschreibung und Nutzungsbedingungen (Anlage 1),
d) das Service Level Agreement (Anlage 2),
e) der Auftragsverarbeitungsvertrag einschließlich seiner Anlagen (Anlage 3),
f) die Informationssicherheitsrichtlinie (Anlage 4).

Bei Widersprüchen zwischen den Vertragsbestandteilen gilt die jeweils höherrangige Regelung. Soweit Regelungen dieses Vertrages die Verarbeitung personenbezogener Daten betreffen, gehen die Regelungen des Auftragsverarbeitungsvertrages sämtlichen übrigen Vertragsbestandteilen vor.

(5) Entgegenstehende, abweichende oder ergänzende Allgemeine Geschäftsbedingungen des Kunden finden keine Anwendung, auch wenn der Anbieter ihrer Geltung im Einzelfall nicht ausdrücklich widerspricht oder Leistungen vorbehaltlos erbringt.

(6) Individuelle Vereinbarungen zwischen den Vertragsparteien haben Vorrang vor diesen AGB. Die Vertragsparteien werden individuelle Vereinbarungen aus Beweisgründen in Textform dokumentieren.

(7) Unentgeltliche Test-, Demo- oder Evaluierungszugänge zu BOS-ID unterliegen ebenfalls diesen AGB, soweit nicht ausdrücklich abweichende Regelungen vereinbart wurden.

§ 2 Begriffsbestimmungen

Im Sinne dieser AGB gelten die folgenden Begriffsbestimmungen:

(1) **BOS-ID** ist die vom Anbieter bereitgestellte Software-as-a-Service-Lösung (SaaS) einschließlich aller zugehörigen Anwendungen, Module, Schnittstellen, Datenbanken, Updates und Dokumentationen.

© by MP-BOS GmbH

(2) **Kunde** ist die natürliche oder juristische Person oder rechtsfähige Personengesellschaft, die mit dem Anbieter einen Vertrag über die Nutzung von BOS-ID abgeschlossen hat.

(3) **Benutzer** ist jede vom Kunden autorisierte natürliche Person, die auf BOS-ID zugreift oder die Software nutzt.

(4) **Benutzerkonto** ist ein personalisierter Zugang zu BOS-ID, der einem bestimmten Benutzer zugeordnet wird.

(5) **Administrator** ist ein vom Kunden benannter Benutzer mit erweiterten Verwaltungs- und Berechtigungsrechten innerhalb von BOS-ID.

(6) **Mandant** ist ein organisatorisch und technisch abgegrenzter Daten- und Funktionsbereich innerhalb von BOS-ID, der einer bestimmten Organisation, Organisationseinheit oder sonstigen fachlichen Struktur des Kunden zugeordnet ist.

(7) **Leistungspaket** ist der gebuchte Funktionsumfang, Ausweiskontingent, inkl. aller Zusatzleistungen (Add-ons) und Integrationen.

(8) **Kundendaten** sind sämtliche Daten, Informationen, Dokumente, Dateien, Stammdaten, Bewegungsdaten, Kommunikationsdaten und sonstigen Inhalte, die durch den Kunden oder dessen Benutzer in BOS-ID gespeichert, verarbeitet, übermittelt oder erzeugt werden.

(9) **Vertragsdaten** sind alle Daten, die für die Durchführung des Vertragsverhältnisses zwischen Anbieter und Kunde erforderlich sind.

(10) **Integrationen** sind Schnittstellen und Drittanwendungen die mit BOS-ID verbunden oder integriert werden können.

(11) **Schnittstelle (API)** ist eine technische Programmierschnittstelle, über die BOS-ID mit anderen Systemen, Anwendungen oder Diensten Daten austauschen oder Funktionen bereitstellen kann.

(12) **Drittanwendungen** sind Anwendungen, Systeme oder Dienste, die nicht vom Anbieter bereitgestellt werden und mit BOS-ID verbunden oder integriert werden können.

(13) **Wartung** umfasst Maßnahmen zur Fehlerbehebung, Aktualisierung, Weiterentwicklung, Optimierung oder Absicherung von BOS-ID.

(14) **Störung** ist eine nicht nur unerhebliche Beeinträchtigung der vertragsgemäßen Nutzung von BOS-ID.

§ 3 Vertragsgegenstand

(1) Gegenstand des Vertrages ist die zeitlich befristete Bereitstellung der webbasierten Softwarelösung „BOS-ID" zur Nutzung über das Internet, sowie die Einräumung der hierfür erforderlichen Nutzungsrechte nach Maßgabe dieses Vertrages.

(2) BOS-ID wird ausschließlich als Software-as-a-Service-Lösung (SaaS) betrieben. Eine Überlassung des Quellcodes oder eine Bereitstellung zur Installation in der IT-Umgebung des Kunden (On-Premise-Betrieb) ist nicht geschuldet, sofern nicht ausdrücklich etwas anderes vereinbart wurde.

(3) BOS-ID ist eine standardisierte Softwarelösung. Der Anbieter schuldet die Bereitstellung der jeweils aktuellen Standardversion einschließlich der vereinbarten Funktionen des vom Kunden gebuchten Leistungspakets.

(4) Der Leistungsumfang richtet sich nach dem jeweils gebuchten Leistungspaket, sowie der jeweils gültigen Leistungsbeschreibung gemäß Anlage 1.

(5) Der Kunde ist berechtigt, BOS-ID ausschließlich für eigene betriebliche Zwecke zu nutzen. Eine Nutzung durch Dritte, die Überlassung an Dritte oder die Nutzung für andere rechtlich selbstständige Unternehmen ist nur zulässig, soweit dies ausdrücklich vereinbart wurde.

(6) Die Nutzung von BOS-ID ist auf den vertraglich vereinbarten Leistungsumfang sowie die jeweils gebuchten Ausweis-, Benutzer-, Organisations-, Mandanten- oder sonstigen Nutzungskontingente beschränkt.

© by MP-BOS GmbH

(7) Die Plattform dient der organisatorischen, administrativen und verwaltungstechnischen Unterstützung von BOS-Organisationen, Kommunen, Behörden, Verbänden und Vereinen. Sie ersetzt keine Leitstellen-, Alarmierungs-, Einsatzleit- oder sonstigen sicherheitskritischen Systeme.

(8) Der Anbieter ist berechtigt, zur Erbringung seiner Leistungen verbundene Unternehmen sowie geeignete Unterauftragnehmer einzusetzen. Die datenschutzrechtlichen Anforderungen des Auftragsverarbeitungsvertrages bleiben hiervon unberührt.

(9) Zusatzleistungen, insbesondere Beratungsleistungen, Schulungen, Datenmigrationen, Schnittstellen-anbindungen, individuelle Konfigurationen, Projektleistungen oder sonstige Professional Services, sind nur geschuldet, soweit diese ausdrücklich vereinbart wurden.

§ 4 Leistungsumfang

(1) Der Anbieter stellt dem Kunden während der Vertragslaufzeit die jeweils aktuelle Version von BOS-ID entsprechend dem gebuchten Leistungspaket zur Nutzung über das Internet bereit.

(2) Der konkrete Leistungsumfang ergibt sich aus dem jeweiligen Angebot, der Leistungsbeschreibung (Anlage 1), dem gebuchten Leistungspaket, sowie gegebenenfalls zusätzlich vereinbarten Leistungen.

§ 5 Bereitstellung der SaaS-Leistungen

(1) Der Anbieter stellt dem Kunden BOS-ID ab dem vertraglich vereinbarten Vertragsbeginn zur Nutzung über das Internet bereit.

(2) Die Bereitstellung erfolgt als zentral betriebene Software-as-a-Service-Lösung (SaaS). Der Zugriff erfolgt über die vom Anbieter bereitgestellten Zugangswege und Schnittstellen.

(3) Der Anbieter betreibt BOS-ID in Rechenzentren innerhalb der Europäischen Union. Der Anbieter ist berechtigt, die zur Leistungserbringung eingesetzte Infrastruktur, Rechenzentrumsstandorte oder Hosting-Dienstleister innerhalb der Europäischen Union zu wechseln, soweit hierdurch keine wesentliche Beeinträchtigung der vertraglich vereinbarten Leistungen entsteht.

(4) Der Kunde erhält die für die Nutzung erforderlichen Zugangsdaten und Berechtigungen in elektronischer Form.

(5) Test-, Staging- oder Sandbox-Umgebungen sind nicht Bestandteil der Standardleistungen. Der Anbieter kann solche Umgebungen für Kunden optional auf Anfrage bereitstellen, sofern dies ausdrücklich vereinbart wurde.

(6) Der Anbieter schuldet die Bereitstellung der Anwendung bis zum Übergabepunkt seines Rechenzentrums bzw. der von ihm eingesetzten Hosting-Infrastruktur.

(7) Die Herstellung und Aufrechterhaltung der Internetverbindung zwischen dem Kunden und dem Übergabepunkt sowie die Bereitstellung geeigneter Hard- und Software auf Kundenseite liegen ausschließlich im Verantwortungs-bereich des Kunden.

(8) Der Kunde ist verpflichtet, die technischen Mindestanforderungen gemäß Anlage 1 einzuhalten.

(9) Der Anbieter ist berechtigt, den Zugang des Kunden oder einzelner Benutzer vorübergehend ganz oder teilweise zu sperren, wenn konkrete Anhaltspunkte für Sicherheitsvorfälle bestehen oder der Verdacht einer missbräuchlichen Nutzung vorliegt oder erhebliche Verstöße gegen diese AGB vorliegen oder die Sperrung zur Abwehr erheblicher Gefahren für die Sicherheit, Integrität oder Verfügbarkeit von BOS-ID erforderlich ist.

(10) Der Anbieter wird den Kunden über eine Sperrung unverzüglich informieren, soweit gesetzliche, sicherheits-relevante oder technische Gründe dem nicht entgegenstehen.

(11) Nach Wegfall des Sperrgrundes wird der Zugang unverzüglich wieder freigeschaltet.

§ 6 Registrierung und Benutzerverwaltung

(1) Der Kunde ist berechtigt, Ausweise innerhalb des vertraglich vereinbarten Nutzungsumfangs selbst anzulegen, zu verwalten, zu ändern und zu löschen. Dies erfolgt über Benutzerzugänge im BOS-ID Webportal.

(2) Die Anzahl der nutzbaren Ausweise richtet sich nach dem jeweils gebuchten Leistungspaket, sowie den vertraglich vereinbarten Nutzungskontingenten.

© by MP-BOS GmbH

(3) Die Nutzung des BOS-ID Webportals erfolgt nach dem Prinzip der personenbezogenen Benutzerzugänge („Named user"). Jeder Zugang darf ausschließlich von der jeweils zugeordneten natürlichen Person genutzt werden.

(4) Die gemeinsame Nutzung eines Benutzerkontos durch mehrere Personen, sowie die Weitergabe persönlicher Zugangsdaten an Dritte ist unzulässig.

(5) Der Kunde ist für die Verwaltung seiner Benutzerkonten, Rollen, Berechtigungen und Organisationsstrukturen selbst verantwortlich.

(6) Der Kunde hat sicherzustellen, dass Benutzerkonten ausschließlich autorisierten Personen zugewiesen werden und die vergebenen Berechtigungen den jeweiligen Aufgabenbereichen entsprechen.

(7) Der Anbieter ist berechtigt, unterschiedliche Rollen- und Berechtigungskonzepte innerhalb von BOS-ID bereitzustellen. Der konkrete Funktionsumfang einzelner Rollen ist vom jeweiligen Leistungspaket abhängig.

(8) Soweit technisch verfügbar, kann der Anbieter Verfahren zur zentralen Authentifizierung, insbesondere Single-Sign-On (SSO), bereitstellen. Ein Anspruch auf bestimmte Authentifizierungsverfahren besteht nur, soweit dies ausdrücklich vereinbart wurde.

(9) Der Anbieter kann Funktionen zur Multi-Faktor-Authentifizierung (MFA) bereitstellen. Die Aktivierung und Nutzung solcher Funktionen obliegen dem Kunden, sofern keine abweichende Vereinbarung getroffen wurde.

(10) Der Kunde ist verpflichtet, Zugangsdaten vertraulich zu behandeln und vor dem Zugriff unberechtigter Dritter zu schützen.

(11) Werden dem Kunden Anhaltspunkte für einen Missbrauch von Benutzerkonten oder Zugangsdaten bekannt, hat er den Anbieter unverzüglich zu informieren.

(12) Der Anbieter ist berechtigt, Benutzerkonten vorübergehend zu sperren, soweit dies zur Gewährleistung der Informationssicherheit, zur Abwehr von Missbrauch oder zur Erfüllung gesetzlicher Verpflichtungen erforderlich ist.

§ 7 Nutzungsrechte

(1) Der Anbieter räumt dem Kunden für die Dauer des Vertrags ein einfaches, nicht ausschließliches, nicht übertragbares und nicht unterlizenzierbares Recht ein, BOS-ID im vertraglich vereinbarten Umfang zu nutzen.

(2) Das Nutzungsrecht ist auf die Laufzeit des jeweiligen Vertrags beschränkt und endet automatisch mit Beendigung des Vertragsverhältnisses.

(3) Die Nutzung ist ausschließlich für die eigenen geschäftlichen oder satzungsgemäßen Zwecke des Kunden zulässig.

(4) Der Kunde ist berechtigt, BOS-ID innerhalb seiner eigenen Organisation, sowie innerhalb vertraglich vereinbarter organisatorischer Untergliederungen, Verbände, Gliederungen, Kreisverbände, Landesverbände, Tochterorganisationen oder vergleichbarer organisatorischer Einheiten zu nutzen, soweit dies vom vereinbarten Leistungspaket oder einer gesonderten Vereinbarung umfasst ist.

(5) Eine Überlassung von BOS-ID an sonstige Dritte, die Einräumung von Unterlizenzen oder die Bereitstellung als Hosting-, Outsourcing-, Service-Bureau- oder Application-Service-Providing-Leistung zugunsten Dritter ist unzulässig und ausdrücklich untersagt.

(6) Der Kunde darf BOS-ID ausschließlich über die vom Anbieter bereitgestellten Benutzeroberflächen, Schnittstellen und Dokumentationen nutzen.

(7) Soweit vom Anbieter dokumentierte Programmierschnittstellen (APIs) bereitgestellt werden, ist der Kunde berechtigt, eigene Integrationen, Anbindungen und Erweiterungen zu entwickeln und zu betreiben. Die Nutzung hat ausschließlich im Rahmen der jeweils veröffentlichten technischen Dokumentation und der vorgesehenen Schnittstellen zu erfolgen.

(8) Der Kunde ist nicht berechtigt,
a) BOS-ID zu vervielfältigen, soweit dies nicht für die vertragsgemäße Nutzung erforderlich ist,
b) den Quellcode einzusehen oder zugänglich zu machen,
c) BOS-ID zurückzuentwickeln (Reverse Engineering),

© by MP-BOS GmbH

d) BOS-ID zu dekompilieren, disassemblieren oder anderweitig technisch zu analysieren,
e) technische Schutzmaßnahmen zu umgehen,
soweit dies nicht aufgrund zwingender gesetzlicher Vorschriften ausdrücklich zulässig ist.

(9) Sämtliche Rechte an BOS-ID, einschließlich aller Urheberrechte, Markenrechte, Datenbankrechte, Geschäftsgeheimnisse, sowie sonstiger gewerblicher Schutzrechte, verbleiben ausschließlich beim Anbieter oder dessen Lizenzgebern.

(10) Dies gilt auch für sämtliche Weiterentwicklungen, Updates, Upgrades, Anpassungen, Konfigurationen, Erweiterungen, Schnittstellen, Dokumentationen und sonstige Arbeitsergebnisse, die im Zusammenhang mit BOS-ID entstehen.

(11) Sofern im Rahmen von Individual-Projekten individuelle Erweiterungen, Anpassungen oder kundenspezifische Funktionen entwickelt werden, verbleiben sämtliche hieran entstehenden Rechte ebenfalls beim Anbieter, sofern nicht ausdrücklich eine abweichende schriftliche Vereinbarung getroffen wurde.

(12) Vorschläge, Ideen, Verbesserungshinweise oder Anregungen des Kunden dürfen vom Anbieter für die Weiterentwicklung von BOS-ID unentgeltlich genutzt werden, ohne dass hieraus Ansprüche des Kunden entstehen.

§ 8 Zulässige Nutzung und Nutzungsbeschränkungen

(1) Der Kunde darf BOS-ID ausschließlich im Rahmen der vertraglich vereinbarten Zwecke, sowie unter Beachtung der geltenden gesetzlichen Vorschriften nutzen.

(2) Der Kunde ist verpflichtet, insbesondere die Vorschriften des Datenschutzrechts, des Urheberrechts, des Wettbewerbsrechts, des Strafrechts, sowie sonstige einschlägige gesetzliche Bestimmungen einzuhalten.

(3) Die Nutzung der bereitgestellten Programmierschnittstellen (APIs) ist ausschließlich im Rahmen der vom Anbieter veröffentlichten technischen Dokumentation und der vorgesehenen Anwendungsfälle zulässig.

(4) Unzulässig ist insbesondere jede Nutzung, die geeignet ist, die Sicherheit, Integrität, Verfügbarkeit oder Leistungsfähigkeit von BOS-ID oder der zugrunde liegenden Infrastruktur zu beeinträchtigen.

(5) Der Kunde ist verpflichtet, erkannte Sicherheitslücken, Sicherheitsvorfälle oder Missbrauchsfälle unverzüglich dem Anbieter zu melden.

(6) Der Anbieter ist berechtigt, bei erheblichen Verstößen gegen diese Bestimmung den Zugriff auf BOS-ID ganz oder teilweise mit sofortiger Wirkung vorübergehend zu sperren, soweit dies zur Gefahrenabwehr, zur Sicherung des ordnungsgemäßen Betriebs oder zur Erfüllung gesetzlicher Verpflichtungen erforderlich ist.

(7) Weitergehende vertragliche oder gesetzliche Ansprüche des Anbieters bleiben unberührt.

§ 9 Mitwirkungs- und Handlungspflichten des Kunden

(1) Der Kunde ist verpflichtet, alle zur Durchführung des Vertrags erforderlichen Mitwirkungsleistungen rechtzeitig, vollständig und unentgeltlich zu erbringen.

(2) Der Kunde ist für sämtliche von ihm, den Ausweis-Inhabern oder seinen Benutzern in BOS-ID gespeicherten, verarbeiteten oder übermittelten Inhalte und Daten selbst verantwortlich.

(3) Der Kunde gewährleistet, dass die von ihm verarbeiteten Daten rechtmäßig erhoben, gespeichert, verarbeitet und genutzt werden und keine Rechte Dritter verletzen.

(4) Der Kunde ist verpflichtet, mindestens einen fachlichen Ansprechpartner, sowie mindestens einen administrativen Ansprechpartner für die Kommunikation mit dem Anbieter zu benennen und deren Kontaktdaten aktuell zu halten.

(5) Der Kunde ist für die Einrichtung, Verwaltung und Pflege seiner Organisationsstrukturen, Benutzerkonten, Rollen, Berechtigungen und Zugriffsrechte verantwortlich.

(6) Der Kunde hat sicherzustellen, dass ausschließlich berechtigte Personen Zugriff auf BOS-ID erhalten.

(7) Der Kunde ist verpflichtet, die vom Anbieter veröffentlichten technischen Mindestanforderungen einzuhalten und geeignete Hard- und Software, sowie aktuelle und unterstützte Browser-Versionen einzusetzen.

© by MP-BOS GmbH

(8) Der Kunde unterstützt den Anbieter bei der Analyse, Eingrenzung und Behebung von Störungen durch die Bereitstellung der hierfür erforderlichen Informationen, Protokolle, Screenshots, Fehlerbeschreibungen oder sonstigen relevanten Angaben.

(9) Der Kunde ist verpflichtet, dem Anbieter unverzüglich alle ihm bekanntwerdenden Sicherheitsvorfälle, Datenschutzverletzungen, unbefugten Zugriffe, missbräuchlichen Nutzungen oder sonstigen sicherheitsrelevanten Ereignisse mitzuteilen.

(10) Der Anbieter führt Datensicherungen gemäß den Regelungen des Service Level Agreements (Anlage 2) durch. Unabhängig hiervon bleibt der Kunde für die Einhaltung gesetzlicher Aufbewahrungsfristen sowie für die Sicherstellung seiner geschäftlichen Prozesse verantwortlich.

(11) Der Kunde hat die vom Anbieter bereitgestellten Dokumentationen, Nutzungshinweise, Sicherheitsinformationen und Bedienungsanleitungen zu beachten.

(12) Fehler, Störungen oder Beeinträchtigungen, die insbesondere zurückzuführen sind auf:
- fehlerhafte oder unvollständige Daten des Kunden
- Fehlbedienungen durch Benutzer (inkl. Ausweisinhaber)
- fehlerhafte Konfigurationen durch den Kunden
- Verstöße gegen die Dokumentation oder Nutzungsvorgaben
- technische Systeme des Kunden
- nicht unterstützte Hard- oder Software
- gelten nicht als Mangel der vertragsgegenständlichen Software

(13) Kommt der Kunde seinen Mitwirkungs- oder Handlungspflichten nicht nach und entstehen hierdurch Verzögerungen, Mehraufwände oder Einschränkungen der Leistungserbringung, gehen die daraus resultierenden Folgen nicht zu Lasten des Anbieters.

§ 10 Vergütung, Rechnungsstellung und Zahlungsbedingungen

(1) Die Vergütung für die Nutzung von BOS-ID richtet sich nach dem jeweils vereinbarten Angebot, sowie dem gebuchten Leistungspaket.

(2) Sämtliche Preise verstehen sich in Euro zuzüglich der jeweils geltenden gesetzlichen Umsatzsteuer.

(3) Die Vergütung für die SaaS-Leistungen wird jährlich im Voraus zum 01. Januar eines Kalenderjahres in Rechnung gestellt.

(4) Beginnt das Vertragsverhältnis unterjährig, erfolgt die erste Abrechnung ebenfalls als Jahresbeitrag für das gesamte aktuelle Jahr.

(5) Rechnungen werden ausschließlich in elektronischer Form als elektronische Rechnung (E-Rechnung) oder in einem gesetzlich zulässigen elektronischen Format bereitgestellt oder übermittelt.

(6) Rechnungen sind innerhalb von vierzehn (14) Kalendertagen ab Rechnungsdatum ohne Abzug zur Zahlung fällig.

(7) Maßgeblich für die Rechtzeitigkeit der Zahlung ist der Eingang des vollständigen Rechnungsbetrages auf dem vom Anbieter benannten Konto.

(8) Gerät der Kunde mit einer Zahlung in Verzug, gelten die gesetzlichen Verzugsregelungen. Der Anbieter ist berechtigt, Verzugszinsen in gesetzlicher Höhe geltend zu machen.

(9) Befindet sich der Kunde trotz Mahnung weiterhin im Zahlungsverzug und ist eine vom Anbieter gesetzte angemessene Nachfrist erfolglos abgelaufen, ist der Anbieter berechtigt, die Leistungen ganz oder teilweise bis zur vollständigen Begleichung sämtlicher fälliger Forderungen vorübergehend einzuschränken oder auszusetzen.

(10) Unabhängig von Absatz 9 ist der Anbieter berechtigt, Leistungen spätestens dann vorübergehend zu sperren, wenn sich der Kunde länger als dreißig (30) Kalendertage mit einer fälligen Zahlung im Verzug befindet.

(11) Die Zahlungspflicht des Kunden bleibt während einer berechtigten Sperrung unberührt.

© by MP-BOS GmbH

(12) Zusatzleistungen, insbesondere Beratungsleistungen, Schulungen, Projektleistungen, Datenmigrationen, individuelle Konfigurationen, Schnittstellenanbindungen, Professional Services oder sonstige gesondert beauftragte Leistungen, werden nach den jeweils vereinbarten Konditionen vergütet.

(13) Soweit keine abweichende Vergütungsvereinbarung getroffen wurde, erfolgt die Abrechnung von Zusatzleistungen nach tatsächlichem Aufwand auf Basis der jeweils vereinbarten Tagessätze, Stundensätze oder Festpreise.

(14) Aufrechnungs- und Zurückbehaltungsrechte des Kunden richten sich ausschließlich nach den Regelungen dieser AGB und den gesetzlichen Vorschriften.

§ 11 Preisanpassungen

(1) Der Anbieter ist berechtigt, die vertraglich vereinbarten Entgelte erstmals nach Ablauf von zwölf (12) Monaten ab Vertragsbeginn und danach höchstens einmal pro Kalenderjahr anzupassen.

(2) Die jährliche Preisanpassung darf pro Anpassungsvorgang höchstens fünf Prozent (5 %) der zuletzt vereinbarten Vergütung betragen.

(3) Der Anbieter wird dem Kunden eine Preisanpassung mindestens sechs (6) Wochen vor ihrem geplanten Inkrafttreten in Textform mitteilen.

(4) Unabhängig von Absatz 1 und 2 ist der Anbieter berechtigt, die Vergütung angemessen anzupassen, wenn sich für die Leistungserbringung maßgebliche Kostenfaktoren wesentlich verändern. Hierzu zählen insbesondere:

- Hosting- und Rechenzentrumskosten
- Lizenz- und Softwarekosten Dritter
- Energiekosten
- Telekommunikations- und Infrastrukturkosten
- gesetzliche oder regulatorische Anforderungen

(5) Eine Preisanpassung nach Absatz 4 darf nur insoweit erfolgen, als die Kostensteigerungen die Kalkulationsgrundlage der vertraglich vereinbarten Leistungen wesentlich beeinflussen. Die Anpassung darf nur in dem Umfang erfolgen, in dem sich die maßgeblichen Kosten tatsächlich verändert haben.

(6) Übersteigt die Summe einer angekündigten Preiserhöhung zehn Prozent (10 %) der zuletzt vereinbarten Vergütung, ist der Kunde berechtigt, den Vertrag innerhalb von vier (4) Wochen nach Zugang der Änderungsmitteilung außerordentlich zum Zeitpunkt des Wirksamwerdens der Preisanpassung in Textform zu kündigen.

(7) Macht der Kunde von seinem Sonderkündigungsrecht keinen Gebrauch, gelten die geänderten Preise mit dem angekündigten Wirksamkeitsdatum als vereinbart.

(8) Preisanpassungen aufgrund gesetzlicher Änderungen, insbesondere Änderungen von Steuern, Abgaben oder vergleichbaren staatlichen Belastungen, bleiben von den vorstehenden Regelungen unberührt.

§ 12 Vertragslaufzeit, Vertragsverlängerung und Kündigung

(1) Der Vertrag beginnt mit dem im jeweiligen Angebot oder Vertrag vereinbarten Vertragsbeginn.

(2) Die Mindestvertragslaufzeit beträgt zwölf (12) Monate.

(3) Der Vertrag verlängert sich nach Ablauf der jeweiligen Vertragslaufzeit automatisch um jeweils weitere zwölf (12) Monate, sofern er nicht von einer Vertragspartei mit einer Frist von sechs (6) Wochen zum Ende der jeweiligen Vertragslaufzeit gekündigt wird.

(4) Kündigungen bedürfen mindestens der Textform (§ 126b BGB). Die Übermittlung per E-Mail ist ausreichend.

(5) Das Recht beider Vertragsparteien zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

(6) Ein wichtiger Grund für den Anbieter liegt insbesondere vor, wenn:
a) der Kunde trotz Mahnung und angemessener Nachfrist mit fälligen Zahlungen in Verzug bleibt,
b) der Kunde schwerwiegend oder wiederholt gegen wesentliche Bestimmungen dieses Vertrages verstößt,
c) der Kunde BOS-ID rechtswidrig oder missbräuchlich nutzt,

© by MP-BOS GmbH

d) durch das Verhalten des Kunden die Sicherheit, Integrität oder Verfügbarkeit von BOS-ID erheblich gefährdet wird.

(7) Vor Ausspruch einer außerordentlichen Kündigung ist der kündigenden Partei grundsätzlich Gelegenheit zur Abhilfe zu geben, soweit dies nach Art des Verstoßes möglich und zumutbar ist.

(8) Mit Beendigung des Vertrages enden sämtliche dem Kunden eingeräumten Nutzungsrechte an BOS-ID.

(9) Der Kunde bleibt nach Vertragsende für einen Zeitraum von dreißig (30) Kalendertagen berechtigt, seine Daten gemäß den vom Anbieter bereitgestellten Exportmöglichkeiten zu exportieren oder herauszugeben zu lassen. Auf schriftlichen Antrag des Kunden kann die Frist einmalig verlängert werden.

(10) Nach Ablauf der Frist gemäß Absatz 9 ist der Anbieter berechtigt, sämtliche Kundendaten zu löschen, soweit keine gesetzlichen Aufbewahrungspflichten oder sonstigen gesetzlichen Verpflichtungen einer Löschung entgegenstehen.

(11) Der Anbieter wird den Kunden vor Durchführung der endgültigen Löschung in geeigneter Weise auf den Ablauf der Exportfrist hinweisen.

(12) Der Kunde kann nach Vertragsende zusätzliche Unterstützungsleistungen für Datenexporte, Datenmigrationen oder sonstige Übergabeleistungen beauftragen. Solche Leistungen sind gesondert zu vergüten.

(13) Gesetzliche Aufbewahrungs-, Nachweis- oder Dokumentationspflichten der Vertragsparteien bleiben von den vorstehenden Regelungen unberührt.

§ 13 Verfügbarkeit, Wartung und Leistungsunterbrechungen

(1) Der Anbieter bemüht sich, BOS-ID während der Vertragslaufzeit in einem vertragsgemäßen und funktionsfähigen Zustand bereitzustellen.

(2) Die Einzelheiten zu Verfügbarkeit, Servicezeiten, Wartungsfenstern, Reaktionszeiten, Wiederherstellungszeiten und sonstigen Serviceparametern ergeben sich ausschließlich aus der Anlage 2 Service Level Agreement (SLA).

(3) Gesetzliche Ansprüche des Kunden bleiben von den vorstehenden Regelungen unberührt.

§ 14 Produktänderungen und Weiterentwicklung

(1) Der Anbieter entwickelt BOS-ID kontinuierlich weiter, um Funktionalität, Sicherheit, Benutzerfreundlichkeit, Leistungsfähigkeit und Integrationsmöglichkeiten zu verbessern.

(2) Der Anbieter ist berechtigt, die Software, ihre technischen Komponenten, ihre Architektur, ihre Datenstrukturen, ihre Benutzeroberflächen sowie ihre Funktionalitäten zu ändern, anzupassen oder weiterzuentwickeln, soweit hierdurch der vertragsgemäße Nutzungszweck nicht wesentlich beeinträchtigt wird.

(3) Der Anbieter ist insbesondere berechtigt, bestehende Funktionen zu erweitern oder anzupassen, Funktionen zusammenzuführen oder neu zu strukturieren, technische Komponenten auszutauschen, Benutzeroberflächen und Bedienkonzepte zu verändern, Sicherheitsmaßnahmen zu erweitern, Integrationen und Schnittstellen anzupassen.

(4) Der Anbieter ist berechtigt, einzelne Funktionen einzustellen, sofern hierfür gleichwertige oder verbesserte Funktionen bereitgestellt werden oder die Änderung aus technischen, wirtschaftlichen, sicherheitsrelevanten oder regulatorischen Gründen erforderlich ist.

(5) Der Kunde hat keinen Anspruch auf die unveränderte Beibehaltung bestimmter Funktionen, Benutzeroberflächen, Workflows, Darstellungen, Datenstrukturen oder technischer Implementierungen.

(6) Der Anbieter ist berechtigt, Programmierschnittstellen (APIs) weiterzuentwickeln, zu ändern oder durch neue Versionen zu ersetzen.

(7) Werden bestehende API-Versionen eingestellt, wird der Anbieter dem Kunden eine angemessene Übergangsfrist zur Anpassung seiner Integrationen einräumen, soweit dies technisch und wirtschaftlich zumutbar ist.

(8) Der Anbieter ist berechtigt, neue Funktionen, Module oder Erweiterungen ausschließlich bestimmten Leistungspaketen oder Produktlinien zuzuordnen.

© by MP-BOS GmbH

(9) Der Kunde hat keinen Anspruch auf die Entwicklung, Bereitstellung oder Einführung bestimmter neuer Funktionen, Erweiterungen oder Integrationen.

(10) Der Anbieter ist berechtigt, technische, organisatorische oder regulatorische Änderungen vorzunehmen, soweit diese zur Aufrechterhaltung eines sicheren, wirtschaftlichen und ordnungsgemäßen Betriebs erforderlich sind.

(11) Vorschläge, Ideen, Anforderungen, Verbesserungshinweise oder sonstiges Feedback des Kunden dürfen vom Anbieter unentgeltlich und zeitlich unbeschränkt für die Weiterentwicklung von BOS-ID genutzt werden.

(12) Aus der Übermittlung von Verbesserungsvorschlägen oder Funktionswünschen entstehen dem Kunden keine Rechte auf Umsetzung, Vergütung, Beteiligung oder sonstige Ansprüche.

§ 15 Datensicherung und Datenverfügbarkeit

(1) Der Anbieter trifft angemessene technische und organisatorische Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Wiederherstellbarkeit der im Rahmen von BOS-ID verarbeiteten Daten.

(2) Die Einzelheiten der Datensicherung, insbesondere Sicherungsintervalle, Aufbewahrungsfristen, Wiederherstellungsziele, sowie sonstige Backup- und Recovery-Parameter, ergeben sich ausschließlich aus dem Service Level Agreement (Anlage 2).

(3) Der Anbieter ist berechtigt, Daten zu Zwecken der Ausfallsicherheit, Notfallvorsorge, Hochverfügbarkeit, Datensicherung oder Betriebsstabilität redundant innerhalb der Europäischen Union zu speichern oder zu verarbeiten.

(4) Der Anbieter gewährleistet die Wiederherstellbarkeit von Daten ausschließlich im Rahmen der im Service Level Agreement vereinbarten Leistungen.

(5) Der Kunde kann die Wiederherstellung bestimmter Datenstände aus vorhandenen Datensicherungen beantragen, soweit dies technisch möglich und wirtschaftlich zumutbar ist.

(6) Wiederherstellungen auf Wunsch des Kunden, die nicht auf einem vom Anbieter zu vertretenden Fehler beruhen, gelten als gesonderte Zusatzleistung und werden nach Aufwand oder gemäß der jeweils gültigen Vergütungsvereinbarung berechnet.

(7) Datensicherungen dienen ausschließlich der Sicherstellung des ordnungsgemäßen Betriebs, der Notfallwiederherstellung sowie der technischen Verfügbarkeit von BOS-ID.

(8) Datensicherungen stellen keinen Archivierungsdienst dar. Der Kunde bleibt für die Erfüllung gesetzlicher Aufbewahrungs-, Dokumentations- und Archivierungspflichten selbst verantwortlich.

(9) Soweit gesetzlich zulässig, besteht kein Anspruch auf Herausgabe von Backup-Medien, Sicherungskopien oder internen Wiederherstellungsständen.

(10) Die Verfügbarkeit einzelner historischer Datenstände kann insbesondere aufgrund technischer, organisatorischer oder datenschutzrechtlicher Anforderungen eingeschränkt sein.

§ 16 Datenexport und Datenherausgabe bei Vertragsende

(1) Der Kunde bleibt jederzeit Inhaber seiner Kundendaten.

(2) Der Anbieter stellt dem Kunden während der Vertragslaufzeit die in BOS-ID vorgesehenen Standardfunktionen zum Export von Kundendaten zur Verfügung.

(3) Nach Beendigung des Vertragsverhältnisses bleibt der Kunde für einen Zeitraum von dreißig (30) Kalendertagen berechtigt, seine Kundendaten zu exportieren oder deren Herausgabe zu verlangen.

(4) Die Herausgabe der Kundendaten erfolgt grundsätzlich in einem vom Anbieter unterstützten maschinenlesbaren Standardformat, insbesondere als SQL-Datenbank.

(5) Der Anbieter schuldet ausschließlich die Bereitstellung der jeweils standardmäßig verfügbaren Exportfunktion und des Exportformates.

© by MP-BOS GmbH

(6) Eine Anpassung, Aufbereitung, Konvertierung oder Migration von Daten in kundenspezifische Zielsysteme, Datenmodelle oder Sonderformate ist nicht Bestandteil der vertraglich geschuldeten Leistungen.

(7) Soweit der Kunde eine darüberhinausgehende Unterstützung bei Datenmigrationen, Datenübernahmen oder Systemwechseln wünscht, können entsprechende Leistungen gesondert beauftragt und vergütet werden.

(8) Die Datenherausgabe erfolgt ausschließlich in elektronischer Form.

(9) Nach Ablauf der in Absatz 3 genannten Frist ist der Anbieter berechtigt, sämtliche Kundendaten nach Maßgabe der vertraglichen und datenschutzrechtlichen Regelungen zu löschen, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

(10) Nach Durchführung der Löschung besteht kein Anspruch des Kunden auf Wiederherstellung oder Herausgabe der gelöschten Daten.

(11) Von der Herausgabepflicht ausgenommen sind insbesondere interne Systemdaten des Anbieters, Betriebs- und Konfigurationsdaten, Protokoll- und Logdaten, Audit- und Sicherheitsprotokolle, Monitoring-Daten, Sicherungskopien und Backups, technische Metadaten, Daten anderer Kunden, Geschäftsgeheimnisse des Anbieters.

(12) Gesetzliche Herausgabe-, Aufbewahrungs- oder Nachweispflichten bleiben von den vorstehenden Regelungen unberührt.

§ 17 Rechte an Kundendaten

(1) Sämtliche Rechte an den vom Kunden oder dessen Benutzern in BOS-ID gespeicherten, verarbeiteten oder erzeugten Kundendaten verbleiben ausschließlich beim Kunden.

(2) Durch die Nutzung von BOS-ID werden dem Anbieter keine Eigentums-, Nutzungs-, Verwertungs- oder sonstigen Rechte an den Kundendaten eingeräumt, soweit dies nicht zur Durchführung des Vertrags erforderlich ist.

(3) Der Kunde räumt dem Anbieter für die Dauer des Vertragsverhältnisses das erforderliche Recht ein, die Kundendaten zu speichern, zu verarbeiten, zu übertragen und zu nutzen, soweit dies zur Erbringung der vertraglich vereinbarten Leistungen erforderlich ist.

(4) Der Anbieter ist berechtigt, anonymisierte oder aggregierte Daten zu erstellen und zu nutzen, sofern hierbei kein Personenbezug und kein Rückschluss auf einzelne Kunden, Benutzer oder Organisationen möglich ist.

(5) Der Anbieter ist berechtigt, anonymisierte oder aggregierte Daten insbesondere zu folgenden Zwecken zu verwenden:

- Weiterentwicklung und Optimierung von BOS-ID
- Produkt- und Qualitätsverbesserung
- Kapazitätsplanung
- Sicherheitsanalysen
- Fehleranalyse
- statistische Auswertungen
- Forschung und Entwicklung

(6) Der Anbieter ist berechtigt, Betriebs-, Nutzungs-, Telemetrie-, Diagnose- und Protokolldaten zu verarbeiten, soweit dies erforderlich ist für den sicheren Betrieb von BOS-ID, die Fehleranalyse, die Störungsbehebung, die Überwachung der Systemstabilität, die Kapazitäts- und Ressourcenplanung, die Informationssicherheit, die Erfüllung gesetzlicher Verpflichtungen.

(7) Die Verarbeitung personenbezogener Daten erfolgt ausschließlich im Rahmen der geltenden Datenschutzgesetze, sowie des zwischen den Parteien geschlossenen Auftragsverarbeitungsvertrages.

(8) Der Anbieter ist nicht berechtigt, Kundendaten für eigene vertriebsbezogene, werbliche oder sonstige vertragsfremde Zwecke zu verwenden.

(9) Die vorstehenden Regelungen gelten auch nach Beendigung des Vertragsverhältnisses fort, soweit gesetzliche Aufbewahrungspflichten oder berechtigte Interessen dies erfordern.

§ 18 Referenznennung

© by MP-BOS GmbH

(1) Der Anbieter ist berechtigt, den Kunden während der Vertragslaufzeit, sowie nach deren Beendigung als Referenzkunden zu benennen.

(2) Die Referenznennung darf insbesondere durch die Nennung des Unternehmens-, Verbands-, Vereins- oder Organisationsnamens des Kunden erfolgen.

(3) Die Referenznennung darf in Vertriebsunterlagen, Präsentationen, Angebotsunterlagen, Referenzlisten, Ausschreibungen, auf Webseiten sowie in sonstigen Unternehmensdarstellungen des Anbieters erfolgen.

(4) Die Verwendung von Logos, Marken, Kennzeichen, Wappen oder sonstigen geschützten Zeichen des Kunden bedarf der vorherigen ausdrücklichen Zustimmung des Kunden.

(5) Die Veröffentlichung von Projektbeschreibungen, Fallstudien (Case Studies), Anwenderberichten, Erfolgsgeschichten oder vergleichbaren Darstellungen bedarf der vorherigen Freigabe durch den Kunden.

(6) Der Anbieter wird bei jeder Referenznennung die berechtigten Interessen des Kunden angemessen berücksichtigen.

(7) Der Kunde kann einer zukünftigen Referenznennung aus berechtigtem Grund widersprechen. Bereits veröffentlichte Unterlagen müssen in diesem Fall nicht rückwirkend geändert werden; der Anbieter wird die Referenznennung jedoch bei künftigen Veröffentlichungen angemessen berücksichtigen.

(8) Weitergehende Nutzungsrechte an Marken, Kennzeichen, Logos oder sonstigen Schutzrechten des Kunden werden dem Anbieter durch diese Vereinbarung nicht eingeräumt.

§ 19 Vertraulichkeit und Geheimhaltung

(1) Die Vertragsparteien verpflichten sich, sämtliche ihnen im Zusammenhang mit diesem Vertrag bekanntwerdenden vertraulichen Informationen der jeweils anderen Vertragspartei vertraulich zu behandeln und ausschließlich zur Durchführung dieses Vertrags zu verwenden.

(2) Als vertrauliche Informationen gelten insbesondere Geschäfts- und Betriebsgeheimnisse, technische Informationen, Sicherheitskonzepte, Systemarchitekturen, Dokumentationen, Quellcodeinformationen, Zugangsdaten, Vertragsinhalte, Preis- und Kalkulationsinformationen, organisatorische Informationen, personenbezogene Daten, sonstige nach den Umständen als vertraulich anzusehende Informationen.

(3) Die empfangende Vertragspartei darf vertrauliche Informationen ausschließlich solchen Mitarbeitern, Organmitgliedern, Beratern, Wirtschaftsprüfern, Rechtsanwälten, Unterauftragnehmern oder sonstigen Erfüllungsgehilfen zugänglich machen, die diese Informationen zur Erfüllung ihrer Aufgaben benötigen und ihrerseits zur Vertraulichkeit verpflichtet wurden.

(4) Die Vertragsparteien verpflichten sich, angemessene technische und organisatorische Maßnahmen zum Schutz vertraulicher Informationen zu treffen.

(5) Die Geheimhaltungspflicht gilt nicht für Informationen, die zum Zeitpunkt ihrer Offenlegung bereits öffentlich bekannt waren, die nach ihrer Offenlegung ohne Verstoß gegen diese Vereinbarung öffentlich bekannt werden, die der empfangenden Vertragspartei bereits rechtmäßig bekannt waren, die von einem berechtigten Dritten rechtmäßig offengelegt wurden oder die unabhängig und ohne Nutzung vertraulicher Informationen entwickelt wurden.

(6) Die Offenlegung vertraulicher Informationen ist zulässig, soweit hierzu eine gesetzliche Verpflichtung, eine behördliche Anordnung, eine gerichtliche Entscheidung oder eine sonstige zwingende rechtliche Verpflichtung besteht.

(7) Soweit rechtlich zulässig, wird die offenlegende Vertragspartei vor einer Offenlegung nach Absatz 6 vorab informiert.

(8) Die Vertragsparteien erkennen an, dass vertrauliche Informationen und Geschäftsgeheimnisse im Sinne des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) geschützt sind.

(9) Die Vertragsparteien werden alle angemessenen Maßnahmen ergreifen, um einen Verlust, eine unbefugte Offenlegung oder eine unbefugte Nutzung vertraulicher Informationen zu verhindern.

© by MP-BOS GmbH

(10) Die Verpflichtung zur Vertraulichkeit gilt während der gesamten Vertragslaufzeit sowie zeitlich unbeschränkt über die Beendigung des Vertragsverhältnisses hinaus.

(11) Die Verpflichtung gemäß Absatz 10 gilt insbesondere dauerhaft für Geschäftsgeheimnisse, Sicherheitsinformationen, technische Architekturen, Quellcodeinformationen, Zugangsinformationen, kryptographische Verfahren, Sicherheitsmaßnahmen oder sonstige besonders schutzwürdige Informationen.

(12) Gesetzliche Ansprüche, insbesondere aus dem GeschGehG, dem Urheberrecht, dem Datenschutzrecht sowie sonstigen Schutzvorschriften, bleiben unberührt.

§ 20 Datenschutz

(1) Die Vertragsparteien verpflichten sich zur Einhaltung der jeweils geltenden datenschutzrechtlichen Vorschriften, insbesondere der Datenschutz-Grundverordnung (DSGVO), sowie der ergänzend anwendbaren nationalen Datenschutzgesetze.

(2) Soweit der Anbieter im Auftrag des Kunden personenbezogene Daten verarbeitet, erfolgt die Verarbeitung ausschließlich auf Grundlage des zwischen den Parteien geschlossenen Auftragsverarbeitungsvertrages (Anlage 3).

(3) Der Auftragsverarbeitungsvertrag einschließlich seiner Anlagen ist integraler Bestandteil dieses Vertragsverhältnisses.

(4) Der Kunde ist für die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung der von ihm oder seinen Benutzern in BOS-ID verarbeiteten personenbezogenen Daten verantwortlich.

(5) Der Kunde stellt sicher, dass sämtliche für die Verarbeitung personenbezogener Daten erforderlichen Rechtsgrundlagen, Einwilligungen, Informationspflichten und sonstigen datenschutzrechtlichen Voraussetzungen vorliegen.

(6) Der Anbieter verarbeitet personenbezogene Daten ausschließlich im Rahmen der vertraglichen Vereinbarungen, der dokumentierten Weisungen des Kunden sowie der geltenden gesetzlichen Vorschriften.

(7) Ist der Anbieter der Auffassung, dass eine Weisung des Kunden gegen datenschutzrechtliche Vorschriften verstößt, ist er berechtigt, die Ausführung der betreffenden Weisung auszusetzen und den Kunden hierauf hinzuweisen.

(8) Die Vertragsparteien werden sich gegenseitig bei der Erfüllung datenschutzrechtlicher Verpflichtungen angemessen unterstützen, soweit dies gesetzlich vorgeschrieben oder vertraglich vereinbart ist.

(9) Der Anbieter setzt angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten ein. Die Einzelheiten ergeben sich aus dem Auftragsverarbeitungsvertrag, den dort beschriebenen technischen und organisatorischen Maßnahmen, sowie der Informationssicherheitsrichtlinie.

(10) Die Informationssicherheitsmaßnahmen des Anbieters orientieren sich an den Anforderungen eines Informationssicherheitsmanagementsystems nach ISO/IEC 27001 (einem gleichwertigen anerkannten Standard), sowie den jeweils implementierten technischen und organisatorischen Maßnahmen.

(11) Weitergehende Regelungen zum Datenschutz ergeben sich ausschließlich aus dem Auftragsverarbeitungsvertrag einschließlich seiner Anlagen.

§ 21 Schutzrechte Dritter und Freistellung

(1) Der Kunde gewährleistet, dass die von ihm oder seinen Benutzern in BOS-ID gespeicherten, verarbeiteten, übermittelten oder bereitgestellten Inhalte, Daten und Informationen keine Rechte Dritter verletzen und nicht gegen geltendes Recht verstoßen.

(2) Der Kunde stellt den Anbieter auf erstes Anfordern von sämtlichen Ansprüchen Dritter frei, die aufgrund einer vom Kunden zu vertretenden Verletzung gesetzlicher Vorschriften oder Rechte Dritter geltend gemacht werden.

(3) Die Freistellung umfasst insbesondere Ansprüche aufgrund von Urheberrechtsverletzungen, Markenrechtsverletzungen, Design- oder Schutzrechtsverletzungen, Persönlichkeitsrechtsverletzungen, Datenschutzverstößen, Wettbewerbsrechtsverstößen und sonstigen Rechtsverletzungen.

© by MP-BOS GmbH

(4) Die Freistellung umfasst ebenfalls die angemessenen Kosten der Rechtsverteidigung, Gerichts- und Verfahrenskosten, Anwaltskosten, Sachverständigenkosten, Vergleichskosten sowie sonstige zur Rechtsverteidigung erforderliche Aufwendungen.

(5) Die Freistellung umfasst, soweit rechtlich zulässig, Schäden, Aufwendungen und Kosten, die dem Anbieter aufgrund einer vom Kunden zu vertretenden Pflichtverletzung entstehen.

(6) Voraussetzung der Freistellung ist, dass der Anbieter
a) den Kunden unverzüglich über geltend gemachte Ansprüche informiert,
b) dem Kunden die Möglichkeit zur angemessenen Mitwirkung an der Rechtsverteidigung einräumt,
c) ohne Zustimmung des Kunden keine Ansprüche anerkennt oder Vergleiche abschließt, soweit dies dem Anbieter zumutbar ist.

(7) Der Kunde wird den Anbieter bei der Abwehr entsprechender Ansprüche angemessen unterstützen und die hierfür erforderlichen Informationen und Unterlagen unverzüglich bereitstellen.

(8) Die Freistellungsverpflichtung besteht nur, soweit die zugrunde liegende Rechtsverletzung oder Pflichtverletzung vom Kunden zu vertreten ist.

(9) Weitergehende gesetzliche oder vertragliche Ansprüche des Anbieters bleiben unberührt.

§ 22 Gewährleistung

(1) Der Anbieter gewährleistet, dass BOS-ID während der Vertragslaufzeit im Wesentlichen den vereinbarten Funktionen und Leistungsmerkmalen entspricht und für die vertraglich vorausgesetzte Nutzung geeignet ist.

(2) Der Anbieter schuldet keine vollständige Fehlerfreiheit der Software. Dem Kunden ist bekannt, dass Software nach dem Stand der Technik nicht vollständig frei von Fehlern bereitgestellt werden kann.

(3) Ein Mangel liegt nur vor, wenn die vertragsgemäße Nutzung von BOS-ID nicht nur unerheblich beeinträchtigt wird.

(4) Unerhebliche Abweichungen von der vereinbarten Beschaffenheit, geringfügige Funktionsbeeinträchtigungen oder lediglich optische Beeinträchtigungen begründen keine Gewährleistungsansprüche.

(5) Der Kunde hat auftretende Mängel unverzüglich nach Kenntniserlangung in nachvollziehbarer Form zu melden und alle zur Fehleranalyse erforderlichen Informationen bereitzustellen.

(6) Im Falle eines Mangels ist der Anbieter zunächst berechtigt, nach eigener Wahl den Mangel durch Nachbesserung, Fehlerkorrektur, Workaround oder Bereitstellung einer Ersatzlösung zu beseitigen.

(7) Schlägt die Nacherfüllung endgültig fehl oder ist sie dem Kunden unzumutbar, kann der Kunde nach den gesetzlichen Vorschriften die Vergütung angemessen mindern oder den Vertrag außerordentlich kündigen.

(8) Gewährleistungsansprüche bestehen nicht, soweit Mängel oder Beeinträchtigungen auf einer fehlerhaften Nutzung durch den Kunden, einer nicht bestimmungsgemäßen Verwendung, fehlerhaften Daten des Kunden, Änderungen oder Eingriffen des Kunden oder Dritter, kundenseitigen Integrationen oder Eigenentwicklungen, Drittanwendungen oder Drittservices oder nicht unterstützten Systemumgebungen beruhen.

(9) Der Anbieter übernimmt keine Gewähr für die dauerhafte Verfügbarkeit, Funktionsfähigkeit oder Kompatibilität von Drittanwendungen, Fremdsystemen oder Diensten Dritter.

(10) Soweit BOS-ID Schnittstellen zu Drittanwendungen bereitstellt, beschränkt sich die Gewährleistung auf die ordnungsgemäße Bereitstellung der jeweiligen Schnittstelle durch den Anbieter.

(11) Die verschuldensunabhängige Haftung des Anbieters für bereits bei Vertragsbeginn vorhandene Mängel gemäß § 536a Abs. 1 Alt. 1 BGB wird ausgeschlossen.

(12) Gesetzliche Rechte des Kunden wegen arglistig verschwiegener Mängel oder ausdrücklich übernommener Garantien bleiben unberührt.

§ 23 Haftung

© by MP-BOS GmbH

(1) Der Anbieter haftet unbeschränkt bei Vorsatz und grober Fahrlässigkeit, bei schuldhafter Verletzung des Lebens, des Körpers oder der Gesundheit, nach den Vorschriften des Produkthaftungsgesetzes, soweit der Anbieter ausdrücklich eine Garantie übernommen hat oder in sonstigen Fällen zwingender gesetzlicher Haftung.

(2) Bei einfacher Fahrlässigkeit haftet der Anbieter nur bei Verletzung einer wesentlichen Vertragspflicht (Kardinalpflicht).

(3) Wesentliche Vertragspflichten sind solche Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Kunde regelmäßig vertrauen darf.

(4) In den Fällen des Absatzes 2 ist die Haftung des Anbieters auf den vertragstypischen, vorhersehbaren Schaden begrenzt.

(5) Die Haftung des Anbieters bei einfacher Fahrlässigkeit ist der Höhe nach auf den Nettobetrag der vom Kunden im Zeitpunkt des Schadenseintritts für zwölf (12) Monate geschuldeten Jahresvergütung begrenzt.

(6) Die Haftungsbegrenzung nach Absatz 5 gilt je Schadensereignis, sowie insgesamt für alle Schadensereignisse innerhalb eines Vertragsjahres.

(7) Soweit gesetzlich zulässig, ist die Haftung des Anbieters für folgende Schäden ausgeschlossen:
- entgangenen Gewinn
- mittelbare Schäden
- Folgeschäden
- reine Vermögensschäden außerhalb wesentlicher Vertragspflichtverletzungen
- Betriebsunterbrechungen oder Organisationsausfälle
- ausgebliebene Einsparungen
- Datenverluste, soweit diese durch eine zumutbare Wiederherstellung aus vorhandenen Datensicherungen hätten vermieden werden können

(8) Der Anbieter haftet nicht für Schäden, die auf fehlerhaften oder unvollständigen Kundendaten, Fehlbedienungen durch den Kunden oder dessen Benutzer, kundenseitigen Konfigurationen, kundenseitigen Integrationen, Drittanwendungen oder Leistungen Dritter oder Verstößen des Kunden gegen gesetzliche oder vertragliche Pflichten beruhen.

(9) Soweit die Haftung des Anbieters ausgeschlossen oder beschränkt ist, gilt dies ebenfalls zugunsten seiner gesetzlichen Vertreter, Organe, Mitarbeiter, Erfüllungsgehilfen, Unterauftragnehmer und sonstigen Hilfspersonen.

(10) Eine weitergehende Haftung des Anbieters ist ausgeschlossen.

(11) Die vorstehenden Haftungsregelungen gelten auch für außervertragliche Ansprüche, soweit gesetzlich zulässig.

(12) Die gesetzlichen Beweislastregeln bleiben von den vorstehenden Regelungen unberührt.

§ 24 Höhere Gewalt

(1) Keine Vertragspartei haftet für die Nichterfüllung oder verspätete Erfüllung ihrer vertraglichen Verpflichtungen, soweit diese auf Ereignissen höherer Gewalt beruhen.

(2) Als höhere Gewalt gelten insbesondere Ereignisse, die außerhalb des zumutbaren Einflussbereichs der betroffenen Vertragspartei liegen und auch bei Anwendung äußerster Sorgfalt nicht verhindert werden konnten.

(3) Hierzu zählen insbesondere:
- Naturkatastrophen, insbesondere Überschwemmungen, Erdbeben, Sturmereignisse, Brände oder vergleichbare Ereignisse
- Krieg, kriegsähnliche Ereignisse, bewaffnete Konflikte oder Terroranschläge
- Pandemien, Epidemien oder sonstige Gesundheitsnotstände
- behördliche Maßnahmen, Anordnungen oder gesetzliche Beschränkungen
- Streiks, Aussperrungen oder sonstige Arbeitskampfmaßnahme
- Ausfälle oder Störungen öffentlicher Telekommunikationsnetze
- Ausfälle von Energieversorgungsnetzen
- Cyberangriffe auf Dritte oder kritische Infrastrukturen
- Ausfälle von Cloud-, Hosting-, Infrastruktur- oder Telekommunikationsdienstleistern, soweit diese nicht vom Anbieter zu vertreten sind

© by MP-BOS GmbH

- sonstige unvorhersehbare und unabwendbare Ereignisse vergleichbarer Art

(4) Für die Dauer des Ereignisses höherer Gewalt sowie für einen angemessenen Wiederanlaufzeitraum ruhen die hiervon betroffenen Leistungspflichten der jeweiligen Vertragspartei.

(5) Die betroffene Vertragspartei wird die andere Vertragspartei über das Vorliegen eines Ereignisses höherer Gewalt sowie dessen voraussichtliche Auswirkungen und Dauer unverzüglich informieren, soweit ihr dies möglich und zumutbar ist.

(6) Die Vertragsparteien werden sich nach Kräften bemühen, die Auswirkungen des Ereignisses zu begrenzen und die vertraglichen Leistungen schnellstmöglich wieder aufzunehmen.

(7) Dauert das Ereignis höherer Gewalt länger als drei (3) Monate ununterbrochen an und ist eine Fortsetzung des Vertragsverhältnisses für eine Vertragspartei unzumutbar, ist jede Vertragspartei berechtigt, den Vertrag mit Wirkung für die Zukunft außerordentlich zu kündigen.

(8) Bereits erbrachte Leistungen sowie bis zum Zeitpunkt der Kündigung entstandene Vergütungsansprüche bleiben von einer Kündigung nach Absatz 7 unberührt.

§ 25 Informationssicherheit

(1) Der Anbieter betreibt für BOS-ID ein Informationssicherheitsmanagementsystem (ISMS) auf Grundlage der Norm ISO/IEC 27001 (einem gleichwertigen anerkannten Standard) in ihrer jeweils gültigen Fassung.

(2) Der Anbieter ist berechtigt, sein Informationssicherheitsmanagementsystem fortlaufend weiterzuentwickeln, anzupassen oder durch gleichwertige Sicherheitsstandards zu ersetzen, sofern das Sicherheitsniveau nicht wesentlich abgesenkt wird.

(3) Die Informationssicherheitsmaßnahmen dienen insbesondere dem Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der von BOS-ID verarbeiteten Informationen und Systeme.

(4) Der Anbieter setzt angemessene technische und organisatorische Maßnahmen ein, um Sicherheitsrisiken zu minimieren und die Sicherheit der bereitgestellten Leistungen zu gewährleisten.

(5) Zu den eingesetzten Sicherheitsmaßnahmen können insbesondere rollenbasierte Berechtigungskonzepte, Authentifizierungs- und Autorisierungsverfahren, Multi-Faktor-Authentifizierung, Verschlüsselungsverfahren, Sicherheitsüberwachung und Monitoring, Datensicherungs- und Wiederherstellungsverfahren, Schwachstellenmanagement, Patch- und Änderungsmanagement und Sicherheits- und Notfallprozesse gehören.

(6) BOS-ID unterstützt rollenbasierte Berechtigungskonzepte, Multi-Faktor-Authentifizierung, sowie verschlüsselte Datenübertragungen unter Verwendung aktueller und anerkannter Verschlüsselungsverfahren.

(7) Audit- und Protokollierungsfunktionen können abhängig vom jeweils gebuchten Leistungspaket bereitgestellt werden. Erweiterte Audit- und Protokollierungsfunktionen sind insbesondere Bestandteil des Enterprise-Pakets, soweit dies in der Leistungsbeschreibung vorgesehen ist.

(8) Der Anbieter betreibt ein dokumentiertes Verfahren zur Erkennung, Bewertung, Behandlung und Nachverfolgung von Sicherheitsvorfällen.

(9) Sicherheitsvorfälle werden nach einem dokumentierten Incident-Management-Prozess behandelt und nach den jeweils geltenden internen Sicherheitsrichtlinien bearbeitet.

(10) Die Einzelheiten der Informationssicherheitsmaßnahmen ergeben sich aus der Informationssicherheitsrichtlinie (Anlage 4), den technischen und organisatorischen Maßnahmen gemäß Auftragsverarbeitungsvertrag sowie den jeweils implementierten Sicherheitsprozessen des Anbieters.

(11) Der Anbieter ist berechtigt, Sicherheitsmaßnahmen jederzeit anzupassen, zu erweitern oder zu ändern, soweit hierdurch das bestehende Sicherheitsniveau nicht wesentlich abgesenkt wird.

(12) Aus Gründen der Informationssicherheit, des Schutzes von Geschäftsgeheimnissen, sowie zum Schutz der Systeme, Kunden und Infrastruktur ist der Anbieter nicht verpflichtet, sämtliche technischen, organisatorischen oder sicherheitsrelevanten Einzelheiten seiner Sicherheitsarchitektur, Sicherheitsmaßnahmen oder Sicherheitsprozesse offenzulegen.

© by MP-BOS GmbH

(13) Der Anbieter kann auf Anfrage geeignete Nachweise über implementierte Sicherheitsmaßnahmen oder bestehende Zertifizierungen bereitstellen, soweit dem keine gesetzlichen, vertraglichen oder sicherheitsrelevanten Gründe entgegenstehen.

(14) Weitergehende Regelungen zur Informationssicherheit ergeben sich aus Anlage 4 dieses Vertrages.

§ 26 Compliance

(1) Die Vertragsparteien verpflichten sich, die im Zusammenhang mit diesem Vertrag anwendbaren gesetzlichen Vorschriften einzuhalten.

(2) Der Kunde darf BOS-ID nicht in einer Weise nutzen, die gegen geltende Gesetze, behördliche Anordnungen, Exportkontrollvorschriften, Embargobestimmungen oder sonstige verbindliche Compliance-Anforderungen verstößt.

(3) Insbesondere ist es dem Kunden untersagt,
a) BOS-ID in Staaten, Regionen oder Gebieten einzusetzen, gegen die umfassende Embargo- oder Sanktionsmaßnahmen bestehen, soweit dies nach anwendbarem Recht unzulässig ist,
b) BOS-ID Personen, Organisationen oder Einrichtungen zugänglich zu machen, die auf einschlägigen Sanktions- oder Terrorlisten geführt werden oder deren Nutzung nach geltendem Recht untersagt ist,
c) BOS-ID für rechtswidrige Zwecke zu verwenden.

(4) Die Vertragsparteien verpflichten sich zur Einhaltung der jeweils geltenden Vorschriften zur Korruptionsbekämpfung, Betrugsprävention und Integrität im Geschäftsverkehr.

(5) Keine Vertragspartei wird im Zusammenhang mit diesem Vertrag unzulässige Vorteile anbieten, versprechen, gewähren oder annehmen.

(6) Der Kunde wird den Anbieter unverzüglich informieren, wenn ihm Umstände bekannt werden, die auf einen erheblichen Compliance-Verstoß im Zusammenhang mit der Nutzung von BOS-ID hindeuten.

(7) Der Anbieter ist berechtigt, den Zugriff auf BOS-ID ganz oder teilweise vorübergehend auszusetzen, soweit konkrete Anhaltspunkte für schwerwiegende Verstöße gegen gesetzliche Vorschriften, Exportkontrollbestimmungen, Sanktionsregelungen oder sonstige Compliance-Anforderungen bestehen.

(8) Besteht ein schwerwiegender Compliance-Verstoß fort oder ist eine Fortsetzung des Vertragsverhältnisses für den Anbieter unzumutbar, ist der Anbieter berechtigt, den Vertrag aus wichtigem Grund außerordentlich zu kündigen.

(9) Weitergehende gesetzliche oder vertragliche Rechte des Anbieters bleiben unberührt.

§ 27 Audit- und Nachweisrechte

(1) Der Kunde ist berechtigt, angemessene Nachweise über die Einhaltung der vertraglich vereinbarten Datenschutz-, Qualitäts- und Informationssicherheitsanforderungen anzufordern.

(2) Der Anbieter kann auf Nachfrage geeignete Nachweise insbesondere durch die Bereitstellung folgender Dokumente oder Informationen erbringen:

- Zertifikate nach DIN EN ISO 9001
- Zertifikate nach DIN EN ISO/IEC 27001
- Beschreibungen der technischen und organisatorischen Maßnahmen (TOM)
- Unterlagen des Auftragsverarbeitungsvertrages
- sonstige geeignete Nachweise zur Informationssicherheit oder Qualitätssicherung

(3) Der Anbieter kann die Form und den Umfang der Nachweiserbringung nach pflichtgemäßem Ermessen festlegen, soweit hierdurch die berechtigten Interessen des Kunden angemessen berücksichtigt werden. Der Anbieter wird hierbei die berechtigten Prüf-, Nachweis- und Kontrollinteressen des Kunden angemessen berücksichtigen.

(4) Vor-Ort-Audits beim Anbieter sind nur zulässig, soweit
a) sie gesetzlich zwingend vorgeschrieben sind,
b) sie datenschutzrechtlich erforderlich sind,
c) andere geeignete Nachweise nicht ausreichen.

© by MP-BOS GmbH

(5) Vor-Ort-Audits bedürfen einer vorherigen schriftlichen Ankündigung mit einer angemessenen Vorlaufzeit, regelmäßig mindestens vier (4) Wochen.

(6) Audits sind auf die für den jeweiligen Prüfungszweck erforderlichen Bereiche zu beschränken und dürfen den Geschäftsbetrieb des Anbieters nicht unangemessen beeinträchtigen.

(7) Der Anbieter ist berechtigt, angemessene Sicherheits-, Vertraulichkeits- und Zugangsregelungen für Audits vorzugeben.

(8) Soweit ein Audit nicht auf gesetzlichen, datenschutzrechtlichen oder vertraglich vereinbarten Kontrollrechten beruht, trägt der Kunde die hierdurch entstehenden angemessenen Kosten des Anbieters.

(9) Von Audit-, Einsichts- oder Nachweisrechten ausdrücklich ausgenommen sind insbesondere Quellcodes, Entwicklungsumgebungen, interne Managementsysteme, interne Sicherheitsarchitekturen, interne Sicherheitskonzepte, Ergebnisse von Penetrationstests, Schwachstellenanalysen, interne Auditberichte, Informationen über andere Kunden, Geschäftsgeheimnisse des Anbieters und sonstige sicherheitskritische Informationen.

(10) Der Anbieter kann die Herausgabe oder Offenlegung von Informationen verweigern, soweit gesetzliche Vorschriften, Geheimhaltungspflichten, Sicherheitsinteressen oder berechtigte Geschäftsinteressen entgegenstehen.

(11) Die Regelungen des Auftragsverarbeitungsvertrages zu Kontroll- und Auditrechten bleiben unberührt.

§ 28 Vertragsübertragung und Rechtsnachfolge

(1) Der Anbieter ist berechtigt, diesen Vertrag sowie die sich hieraus ergebenden Rechte und Pflichten ganz oder teilweise auf ein verbundenes Unternehmen im Sinne der §§ 15 ff. AktG, einen Rechtsnachfolger oder einen Erwerber des betreffenden Geschäftsbereichs zu übertragen.

(2) Eine Zustimmung des Kunden ist hierfür nicht erforderlich. Der Kunde kann aber aus wichtigem Grund widersprechen.

(3) Der Anbieter wird den Kunden über eine Vertragsübertragung in angemessener Form informieren.

(4) Die Übertragung darf nicht zu einer wesentlichen Verschlechterung der vertraglich geschuldeten Leistungen, sowie des Datenschutz-, Geheimhaltungs- oder Sicherheitsniveaus führen.

(5) Der Kunde ist nicht berechtigt, diesen Vertrag oder einzelne Rechte und Pflichten aus diesem Vertrag ohne vorherige schriftliche Zustimmung des Anbieters ganz oder teilweise auf Dritte zu übertragen.

(6) Die Zustimmung darf nicht unbillig verweigert werden, sofern die berechtigten Interessen des Anbieters nicht beeinträchtigt werden.

(7) Die vorstehenden Regelungen gelten entsprechend für Umwandlungen, Verschmelzungen, Spaltungen, Einbringungen, Betriebsübergänge sowie sonstige gesellschaftsrechtliche oder wirtschaftliche Rechtsnachfolgen.

(8) Gesetzliche Regelungen zur Gesamtrechtsnachfolge bleiben unberührt.

§ 29 Änderungen dieser AGB

(1) Der Anbieter ist berechtigt, diese AGB mit Wirkung für die Zukunft zu ändern, soweit hierfür ein sachlicher Grund besteht und die Änderungen für den Kunden zumutbar sind.

(2) Ein sachlicher Grund liegt insbesondere vor bei Änderungen gesetzlicher oder behördlicher Anforderungen, Änderungen der höchstrichterlichen Rechtsprechung, Änderungen datenschutzrechtlicher Anforderungen, Änderungen von Informationssicherheitsanforderungen, technischen Weiterentwicklungen von BOS-ID, Änderungen der organisatorischen oder betrieblichen Abläufe des Anbieters, Schließung von Regelungslücken oder Anpassungen zur Verbesserung der Vertragsdurchführung.

(3) Der Anbieter wird den Kunden über Änderungen dieser AGB mindestens vier (4) Wochen vor ihrem geplanten Inkrafttreten in Textform informieren.

(4) Der Kunde kann den Änderungen innerhalb von vier (4) Wochen nach Zugang der Änderungsmitteilung in Textform widersprechen.

© by MP-BOS GmbH

(5) Widerspricht der Kunde den Änderungen nicht innerhalb der Frist gemäß Absatz 4, gelten die Änderungen mit Ablauf der Widerspruchsfrist als angenommen.

(6) Der Anbieter wird den Kunden in der Änderungsmitteilung ausdrücklich auf die Widerspruchsfrist, die Folgen eines unterlassenen Widerspruchs sowie ein gegebenenfalls bestehendes Sonderkündigungsrecht hinweisen.

(7) Änderungen, die den Leistungsumfang, die Vergütung, die Haftung, die Laufzeit, die Kündigungsregelungen oder sonstige wesentliche Vertragspflichten betreffen, bedürfen der ausdrücklichen Zustimmung des Kunden.

(8) Betrifft die Änderung wesentliche vertragliche Rechte oder Pflichten des Kunden und führt sie zu einer nicht nur unerheblichen Verschlechterung seiner Rechtsposition, ist der Kunde berechtigt, den Vertrag innerhalb der Widerspruchsfrist mit Wirkung zum Zeitpunkt des Inkrafttretens der Änderung außerordentlich zu kündigen.

(9) Diese Änderungsregelung gilt ausschließlich für Verträge mit Unternehmern im Sinne des § 14 BGB, juristischen Personen des öffentlichen Rechts und öffentlich-rechtlichen Sondervermögen.

(10) Individuelle Vereinbarungen zwischen den Vertragsparteien bleiben von Änderungen dieser AGB unberührt.

§ 30 Aufrechnung, Zurückbehaltung und Abtretung

(1) Der Kunde ist zur Aufrechnung nur berechtigt, soweit seine Gegenansprüche rechtskräftig festgestellt, entscheidungsreif, unbestritten oder vom Anbieter ausdrücklich anerkannt sind.

(2) Ein Zurückbehaltungsrecht kann der Kunde nur geltend machen, soweit sein Gegenanspruch auf demselben Vertragsverhältnis beruht und rechtskräftig festgestellt, unbestritten oder vom Anbieter anerkannt ist.

(3) Die Abtretung von Rechten oder Ansprüchen des Kunden aus diesem Vertrag an Dritte ist nur mit vorheriger schriftlicher Zustimmung des Anbieters zulässig.

(4) § 354a HGB bleibt unberührt.

(5) Der Anbieter ist berechtigt, Forderungen aus diesem Vertragsverhältnis an verbundene Unternehmen, Finanzierungspartner, Factoring-Unternehmen oder Inkassodienstleister abzutreten oder zu übertragen.

(6) Die Übertragung von Forderungen gemäß Absatz 5 berührt die Rechte und Pflichten des Kunden aus diesem Vertrag nicht.

§ 31 Anwendbares Recht und Gerichtsstand

(1) Für sämtliche Rechtsbeziehungen zwischen den Vertragsparteien gilt ausschließlich das Recht der Bundesrepublik Deutschland.

(2) Die Anwendung des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf (UN-Kaufrecht/CISG) ist ausgeschlossen.

(3) Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist der Sitz des Anbieters, sofern der Kunde Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

(4) Der Anbieter ist darüber hinaus berechtigt, Ansprüche gegen den Kunden auch an dessen allgemeinem Gerichtsstand geltend zu machen.

(5) Zwingende gesetzliche Gerichtsstände bleiben unberührt.

§ 32 Schlussbestimmungen

(1) Änderungen, Ergänzungen oder Nebenabreden zu diesem Vertrag bedürfen mindestens der Textform, soweit gesetzlich keine strengere Form vorgeschrieben ist.

(2) Dies gilt auch für die Änderung oder Aufhebung dieses Formerfordernisses.

© by MP-BOS GmbH

(3) Sämtliche Anlagen, Leistungsbeschreibungen, Service Level Agreements, Auftragsverarbeitungsverträge, Informationssicherheitsrichtlinien, sowie sonstige ausdrücklich in Bezug genommene Dokumente sind Bestandteil dieses Vertrags.

(4) Vertragssprache ist Deutsch. Soweit Übersetzungen dieses Vertrags oder einzelner Vertragsbestandteile erstellt werden, ist ausschließlich die deutschsprachige Fassung maßgeblich.

(5) Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise unwirksam, undurchführbar oder nicht durchsetzbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

(6) Anstelle der unwirksamen, undurchführbaren oder nicht durchsetzbaren Bestimmung gilt diejenige wirksame Regelung als vereinbart, die dem wirtschaftlichen Zweck der ursprünglichen Regelung rechtlich zulässig am nächsten kommt. Entsprechendes gilt für etwaige Vertragslücken.

(7) Die Vertragsparteien verpflichten sich, im Falle einer Regelungslücke oder der Unwirksamkeit einzelner Bestimmungen an einer rechtlich wirksamen und wirtschaftlich möglichst gleichwertigen Ersatzregelung mitzuwirken.

(8) Gesetzliche Bestimmungen, von denen vertraglich nicht wirksam abgewichen werden kann, bleiben unberührt.

© by MP-BOS GmbH

■ Anlage 1

Leistungsbeschreibung und Nutzungsbedingungen

§ 1 Gegenstand der Leistungsbeschreibung

(1) Diese Leistungsbeschreibung konkretisiert die von der MP-BOS GmbH im Rahmen der SaaS-Lösung BOS-ID bereitgestellten Leistungen.

(2) BOS-ID ist eine webbasierte Plattform inkl. App für Behörden und Organisationen mit Sicherheitsaufgaben (BOS), sowie sonstige Hilfsorganisationen, Verbände, Einsatzorganisationen, Organisationseinheiten, Verbände, Vereine, Hersteller und vergleichbare Einrichtungen.

(3) Die Plattform dient der digitalen Verwaltung und Anzeige von Ausweisen jeglicher Art, so z.B. Dienstausweise, Mitgliedsausweise und Mitarbeiterausweise.

(4) BOS-ID wird als Standardsoftware bereitgestellt und besteht aus den Modulen Administrationsportal und Ausweis-App für Smartphones.

(5) Der konkrete Leistungsumfang ergibt sich aus dem jeweils gebuchten Leistungspaket, den aktivierten Integrationen, dem Angebot, sowie den jeweils bereitgestellten Produktinformationen.

(6) BOS-ID unterstützt unterschiedliche Organisations- und Mandantenstrukturen und kann insbesondere für Verbände, Kreisverbände, Landesverbände, Organisationseinheiten, Vereine, Hersteller, sowie vergleichbare mehrstufige Organisationsformen eingesetzt werden.

(7) Maßgeblich für die vertraglich geschuldeten Leistungen ist jeweils die zum Zeitpunkt der Nutzung bereitgestellte Version von BOS-ID im Rahmen des gebuchten Leistungspakets.

§ 2 Zweckbestimmung von BOS-ID

(1) BOS-ID dient der digitalen Unterstützung von Organisations-, Verwaltungs-, Dokumentations- und Ressourcenprozessen im Bereich Ausweis-Management innerhalb von Behörden, Organisationen, Verbänden und sonstigen Einrichtungen.

(2) Zweck der Plattform ist die zentrale Erfassung, Verwaltung, Strukturierung und Bereitstellung von digitalen Ausweisen in einer einheitlichen Systemumgebung.

(3) Die Verantwortung für Entscheidungen, Maßnahmen, Freigaben, Genehmigungen und sonstige organisatorische oder operative Handlungen verbleibt ausschließlich beim Kunden beziehungsweise den von ihm autorisierten Nutzern.

(4) Der Kunde trägt die alleinige Verantwortung für die Ausstellung, Vergabe und Zuweisung von Ausweisen über BOS-ID. Dies umfasst insbesondere die Entscheidung, welche Ausweise mit welchen Inhalten, Berechtigungen und Gültigkeiten an welche Personen ausgegeben werden. Der Anbieter übernimmt keine Prüfung der Identität, Berechtigung oder Eignung der Ausweisempfänger, sowie der Rechtmäßigkeit der jeweiligen Ausweisausstellung.

(5) Die innerhalb von BOS-ID gespeicherten oder erzeugten Ausweise dienen der Unterstützung von Arbeits- und Entscheidungsprozessen und ersetzen keine eigenständige fachliche Prüfung durch den Kunden.

(6) Der Kunde darf BOS-ID ausschließlich für rechtmäßige und dem vorgesehenen Organisationszweck entsprechende Zwecke einsetzen.

(7) Eine Nutzung der Plattform außerhalb des vorgesehenen Anwendungsbereichs oder entgegen den vertraglichen Vereinbarungen ist unzulässig.

§ 3 Funktionsumfang

(1) Der konkrete Funktionsumfang von BOS-ID richtet sich nach dem jeweils gebuchten Leistungspaket, der Anzahl der gebuchten Ausweise, sowie den darin enthaltenen Funktionen und Modulen.

(2) Der jeweilige Funktionsumfang der Leistungspakete ergibt sich aus der zum Zeitpunkt des Vertragsschlusses gültigen Funktionsumfangs- und Preisübersicht, sowie dem individuellen Angebot.

© by MP-BOS GmbH

(3) Der Anbieter ist berechtigt, die Leistungs- und Preisübersicht fortlaufend weiterzuentwickeln und anzupassen. Für bestehende Vertragsverhältnisse gilt jeweils der vertraglich vereinbarte Leistungsumfang, soweit keine wirksame Änderung vereinbart wurde.

(4) Ein Anspruch auf die Bereitstellung bestimmter Funktionen, Module oder Integrationen besteht ausschließlich im Umfang der jeweils vertraglich vereinbarten Leistungen.

(5) Der Anbieter ist berechtigt, neue Module, Erweiterungen, Schnittstellen, Integrationen oder Produktbereiche einzuführen und diese einzelnen Leistungspaketen zuzuordnen oder als kostenpflichtige Zusatzmodule anzubieten.

(6) Funktionen, Module oder Erweiterungen können ausschließlich bestimmten Leistungspaketen vorbehalten werden.

(7) Der Anbieter ist berechtigt, weitere Module, Funktionen, Erweiterungen, Integrationen oder Produktbereiche bereitzustellen, zu ändern, zu erweitern, einzuschränken oder einzustellen, soweit hierdurch der vertragsgemäße Nutzungszweck nicht wesentlich beeinträchtigt wird. Ebenso kann er technische Komponenten austauschen, Datenstrukturen anpassen, Sicherheitsmaßnahmen erweitern und Benutzeroberflächen bzw. Bedienkonzepte ändern.

(8) Der Kunde hat keinen Anspruch auf die unveränderte Beibehaltung bestimmter Funktionen, Darstellungen, Benutzeroberflächen, Bedienabläufe oder technischer Implementierungen, sofern die wesentlichen vertraglichen Funktionen erhalten bleiben.

(9) Ein Anspruch auf die Bereitstellung bestimmter zukünftiger Funktionen, Module, Integrationen oder Produktentwicklungen besteht nicht, soweit diese nicht ausdrücklich vertraglich vereinbart wurden.

(10) Das Leistungspaket Enterprise kann zusätzliche kundenspezifische Konfigurationen, erweiterte Funktionalitäten, individuelle Organisationsstrukturen, erweiterte Integrationen sowie gesondert vereinbarte Sonderfunktionen umfassen.

(11) Individuelle Konfigurationen oder Sonderfunktionen im Enterprise-Paket begründen keinen Anspruch auf Übertragung von Urheberrechten, Quellcode oder sonstigen Schutzrechten.

(12) Maßgeblich für den vertraglich geschuldeten Funktionsumfang ist ausschließlich die jeweils zum Zeitpunkt der Nutzung bereitgestellte Version von BOS-ID im Rahmen des gebuchten Leistungspakets.

§ 4 Nutzer- und Rollenmodelle

(1) BOS-ID verfügt über ein rollenbasiertes Berechtigungsmodell zur Steuerung von Zugriffsrechten und Funktionen innerhalb der Plattform.

(2) Die Plattform kann unterschiedliche Rollen und Berechtigungsstufen bereitstellen. Zum Zeitpunkt des Vertragsschlusses sind insbesondere die Standardrollen Tenant-Administrator und Benutzer vorgesehen. Ausweisinhaber haben keinen Zugriff ins Webportal.

(3) Tenant-Administratoren verfügen über erweiterte Verwaltungsrechte und sind insbesondere berechtigt, Benutzer zu verwalten, Berechtigungen zu vergeben, sowie organisatorische Einstellungen vorzunehmen.

(4) Benutzer verfügen über die im jeweiligen Leistungspaket vorgesehenen Standardfunktionen entsprechend ihren zugewiesenen Berechtigungen.

(5) Die konkreten Berechtigungen einzelner Rollen können abhängig vom jeweiligen Leistungspaket, den aktivierten Modulen sowie den organisatorischen Einstellungen des Kunden variieren.

(6) Berechtigungen können modulbezogen vergeben werden.

(7) Das Rollen- und Berechtigungskonzept kann mandantenbezogen ausgestaltet werden, sodass unterschiedliche Rollen und Berechtigungen innerhalb verschiedener Mandanten oder Organisationseinheiten bestehen können.

(8) Der Anbieter ist berechtigt, das Rollen- und Berechtigungssystem technisch, organisatorisch oder funktional weiterzuentwickeln, zu erweitern oder anzupassen, soweit hierdurch die vertragsgemäße Nutzung nicht wesentlich beeinträchtigt wird.

© by MP-BOS GmbH

(9) Der Kunde ist für die ordnungsgemäße Vergabe, Verwaltung und regelmäßige Überprüfung der ihm zugewiesenen Rollen und Berechtigungen verantwortlich.

(10) Der Anbieter übernimmt keine Verantwortung für Berechtigungsvergaben, die durch den Kunden oder dessen Benutzer vorgenommen werden.

§ 5 Mandantenfähigkeit

(1) BOS-ID unterstützt den Betrieb mehrerer Mandanten innerhalb einer gemeinsamen Systemumgebung.

(2) Ein Mandant bildet eine organisatorisch und technisch abgegrenzte Einheit innerhalb der Plattform und kann eigenständige Datenbestände, Benutzer, Rollen, Berechtigungen, Einstellungen und Prozesse enthalten.

(3) Die Plattform ermöglicht die Abbildung mehrstufiger Organisationsstrukturen innerhalb einer oder mehrerer Organisationen.

(4) Hierzu können insbesondere Bundes-, Landes-, Bezirks-, Kreis-, Orts- oder sonstige Organisationsebenen innerhalb einer gemeinsamen Mandantenstruktur abgebildet werden.

(5) Mandanten können hierarchisch organisiert werden und organisatorische Beziehungen zueinander aufweisen.

(6) Die Trennung von Mandanten stellt ein wesentliches Sicherheits- und Organisationsmerkmal der Plattform dar.

(7) Daten eines Mandanten sind grundsätzlich von den Daten anderer Mandanten getrennt.

(8) Ein Datenaustausch zwischen Mandanten erfolgt ausschließlich, soweit dies durch entsprechende Freigaben, Berechtigungen oder technische Konfigurationen ausdrücklich vorgesehen ist.

(9) Der Kunde kann mandantenübergreifende Freigaben und Datenzugriffe nur im Rahmen der jeweils bereitgestellten Funktionen und Berechtigungskonzepte konfigurieren.

(10) Der Anbieter übernimmt keine Verantwortung für mandantenübergreifende Freigaben oder Zugriffsrechte, die durch den Kunden eingerichtet oder freigegeben wurden.

(11) Der Anbieter ist berechtigt, die technische Umsetzung der Mandantenfähigkeit, sowie die zugrunde liegenden Daten- und Organisationsstrukturen weiterzuentwickeln, soweit hierdurch die vertragsgemäße Nutzung nicht wesentlich beeinträchtigt wird.

(12) Ein Anspruch auf eine bestimmte technische Implementierung der Mandantentrennung besteht nicht.

§ 6 Technische Voraussetzungen

(1) Die Nutzung von BOS-ID erfolgt über einen aktuellen und unterstützten Webbrowser.

(2) Für die Nutzung der Plattform ist eine funktionierende Internetverbindung erforderlich.

(3) Der Kunde ist für die Bereitstellung und den Betrieb der für die Nutzung erforderlichen Hard- und Software, Netzwerkinfrastruktur, Endgeräte sowie Internetzugänge selbst verantwortlich.

(4) BOS-ID unterstützt die jeweils aktuellen Versionen marktüblicher Webbrowser. Hierzu können insbesondere aktuelle Versionen von Google Chrome, Microsoft Edge, Mozilla Firefox und Apple Safari gehören.

(5) Der Anbieter ist berechtigt, die Unterstützung einzelner Browser, Browserversionen, Betriebssysteme oder technischer Standards einzustellen, soweit diese technisch veraltet, sicherheitsrelevant oder wirtschaftlich nicht mehr sinnvoll unterstützbar sind.

(6) Der Kunde ist verpflichtet, unterstützte und aktuelle Browserversionen, sowie aktuelle Sicherheitsupdates für die von ihm eingesetzten Systeme einzusetzen.

(7) Die Nutzung von BOS-ID kann durch kundenseitige Sicherheitseinstellungen, Firewalls, Netzwerkkonfigurationen, Browsererweiterungen oder sonstige technische Einschränkungen beeinflusst werden. Hierfür übernimmt der Anbieter keine Verantwortung.

© by MP-BOS GmbH

(8) Der Anbieter ist berechtigt, technische Mindestanforderungen für die Nutzung von BOS-ID festzulegen und diese unter Berücksichtigung technischer Weiterentwicklungen anzupassen.

(9) Soweit der Anbieter Programmierschnittstellen (APIs) bereitstellt, gelten die jeweils veröffentlichten technischen Spezifikationen und Dokumentationen.

(10) Ein Anspruch auf Unterstützung bestimmter Browser, Betriebssysteme, Geräteklassen, technischer Standards oder Schnittstellenversionen besteht nur, soweit dies ausdrücklich vereinbart wurde.

(11) Der Anbieter ist berechtigt, technische Maßnahmen zu ergreifen, die zur Aufrechterhaltung von Sicherheit, Stabilität, Leistungsfähigkeit oder Kompatibilität der Plattform erforderlich sind.

§ 7 Hosting und Betriebsumgebung

(1) BOS-ID wird als zentral betriebene Software-as-a-Service-Lösung in einer durch den Anbieter betriebenen oder beauftragten Hosting- und Betriebsumgebung bereitgestellt.

(2) Die Verarbeitung und Speicherung von Kundendaten erfolgen ausschließlich innerhalb der Europäischen Union (EU) beziehungsweise des Europäischen Wirtschaftsraums (EWR).

(3) Der Anbieter ist berechtigt, geeignete Hosting-, Infrastruktur-, Plattform- oder Rechenzentrumsdienstleister zur Erbringung der Leistungen einzusetzen.

(4) Der Anbieter ist berechtigt, eingesetzte Hosting- oder Infrastrukturpartner jederzeit zu wechseln, soweit hierdurch die vertraglich geschuldeten Leistungen nicht wesentlich beeinträchtigt werden und die datenschutzrechtlichen Anforderungen weiterhin eingehalten werden.

(5) Die jeweils eingesetzte Betriebsumgebung kann physische, virtuelle, containerisierte oder sonstige technische Infrastrukturkomponenten umfassen.

(6) Der Anbieter ist berechtigt, die technische Architektur, Infrastruktur, Betriebsumgebung sowie eingesetzte Plattform- und Systemkomponenten weiterzuentwickeln, anzupassen oder auszutauschen.

(7) Die Bereitstellung der Betriebsumgebung erfolgt unter Berücksichtigung angemessener technischer und organisatorischer Maßnahmen zur Gewährleistung von Informationssicherheit, Datenschutz und Betriebssicherheit.

(8) Die Einzelheiten zu Verfügbarkeit, Wartung, Datensicherung, Wiederherstellung, Redundanz und sonstigen Betriebsparametern ergeben sich ausschließlich aus dem Service Level Agreement (Anlage 2).

(9) Der Anbieter ist berechtigt, Unterauftragnehmer und sonstige technische Dienstleister einzusetzen, soweit dies für den Betrieb, die Wartung, die Sicherheit oder die Weiterentwicklung von BOS-ID erforderlich ist.

(10) Die jeweils eingesetzten Unterauftragnehmer werden im Rahmen der datenschutzrechtlichen und vertraglichen Anforderungen eingebunden.

(11) Ein Anspruch des Kunden auf die Nutzung bestimmter Rechenzentren, bestimmter Hosting-Anbieter, bestimmter Infrastrukturtechnologien oder bestimmter technischer Betriebsmodelle besteht nicht.

§ 8 Datenspeicherung und Datenhaltung

(1) BOS-ID speichert die vom Kunden innerhalb der Plattform erfassten, verarbeiteten oder bereitgestellten Daten im Rahmen der vertraglich vereinbarten Leistungen.

(2) Die Datenspeicherung kann insbesondere Stammdaten, Bewegungsdaten, Organisationsdaten, Dokumente, Dateien, Bilder, Protokolle, Konfigurationsdaten, sowie sonstige vom Kunden bereitgestellte Inhalte umfassen.

(3) Der jeweils verfügbare Speicherumfang richtet sich nach dem gebuchten Leistungspaket, sowie den vertraglich vereinbarten Leistungen.

(4) Bereits gespeicherte Daten bleiben von einer Sperrung gemäß Absatz 7 grundsätzlich unberührt, soweit technische, rechtliche oder sicherheitsrelevante Gründe nicht entgegenstehen.

© by MP-BOS GmbH

(5) Der Anbieter ist berechtigt, Datenbestände technisch zu optimieren, zu komprimieren, zu konsolidieren, zu archivieren oder vergleichbare Maßnahmen zur Verbesserung von Sicherheit, Performance, Speicherbedarf oder Betriebsstabilität durchzuführen.

(6) Solche Maßnahmen dürfen die vertragsgemäße Nutzung der Kundendaten nicht unangemessen beeinträchtigen.

(7) Der Kunde bleibt für Inhalt, Richtigkeit, Vollständigkeit, Aktualität, Rechtmäßigkeit und Qualität seiner Daten allein verantwortlich.

(8) Der Anbieter ist nicht verpflichtet, die inhaltliche Richtigkeit, Vollständigkeit oder Plausibilität der vom Kunden gespeicherten Daten zu prüfen.

(9) Gesetzliche Aufbewahrungs-, Dokumentations- oder Nachweispflichten des Kunden bleiben von der Speicherung innerhalb von BOS-ID unberührt und liegen ausschließlich im Verantwortungsbereich des Kunden.

(10) Die Einzelheiten zu Datensicherung, Backup, Wiederherstellung und Datenverfügbarkeit ergeben sich aus dem Service Level Agreement (Anlage 2).

§ 9 Schnittstellen und Integrationen

(1) BOS-ID kann standardisierte Programmierschnittstellen (APIs) optional zur Verfügung stellen, über die Daten und Funktionen mit anderen Systemen ausgetauscht oder integriert werden können.

(2) Die technischen Spezifikationen, Funktionsumfänge, Authentifizierungsverfahren und Nutzungsvoraussetzungen ergeben sich aus der jeweils aktuellen API-Dokumentation.

(3) Der Anbieter ist berechtigt, für die Nutzung von APIs technische Nutzungslimits, Transaktionsgrenzen, Rate-Limits, Datenvolumenbeschränkungen oder vergleichbare Nutzungsbeschränkungen festzulegen.

(4) Umfang und Höhe solcher Nutzungslimits können abhängig vom jeweils gebuchten Leistungspaket ausgestaltet werden.

(5) Der Anbieter ist berechtigt, zusätzliche API-Kontingente, erweiterte Nutzungsrechte oder erhöhte Nutzungslimits als kostenpflichtige Zusatzleistung anzubieten.

(6) Der Anbieter ist berechtigt, bestehende API-Versionen weiterzuentwickeln, anzupassen oder durch neue Versionen zu ersetzen.

(7) Werden API-Versionen eingestellt, wird dem Kunden eine angemessene Übergangsfrist zur Anpassung seiner Integrationen eingeräumt.

(8) Der Anbieter kann zusätzliche Integrations- und Authentifizierungsverfahren bereitstellen, insbesondere Single-Sign-On (SSO), OAuth, Webhooks, SCIM oder vergleichbare Technologien.

(9) Ein Anspruch auf bestimmte Integrationsverfahren oder technische Standards besteht nur, soweit diese ausdrücklich Bestandteil des gebuchten Leistungspakets oder einer gesonderten Vereinbarung sind.

(10) Individuelle Integrationen, kundenspezifische Schnittstellenentwicklungen oder besondere Integrationsleistungen sind grundsätzlich gesondert zu vereinbaren.

(11) Soweit Integrationen durch den Anbieter entwickelt, eingerichtet oder kostenpflichtig bereitgestellt werden, umfasst der Support auch die vereinbarte Integration im vertraglich geschuldeten Umfang.

(12) Die Funktionsfähigkeit und Kompatibilität von Drittanwendungen selbst bleibt außerhalb des Verantwortungsbereichs des Anbieters, soweit die Störung nicht durch die vom Anbieter bereitgestellte Integration verursacht wurde. Der Anbieter schuldet bei einer Integration lediglich die Bereitstellung der Schnittstelle.

(13) Der Anbieter ist berechtigt, Integrationen oder Schnittstellen vorübergehend einzuschränken oder auszusetzen, soweit dies aus Sicherheitsgründen, zur Fehlerbehebung oder zur Aufrechterhaltung der Systemstabilität erforderlich ist.

§ 10 Benutzerkonten und Authentifizierung

© by MP-BOS GmbH

(1) Der Zugriff auf das BOS-ID Webportal erfolgt über personalisierte Benutzerkonten.

(2) Benutzerkonten werden grundsätzlich einer natürlichen Person zugeordnet und dürfen ausschließlich von dieser Person genutzt werden.

(3) Die Authentifizierung erfolgt grundsätzlich über die zentrale Identitätsplattform BOS-ID oder ein vom Anbieter bereitgestelltes Nachfolgesystem.

(4) Die Anmeldung erfolgt regelmäßig mittels E-Mail-Adresse und Passwort.

(5) Der Anbieter ist berechtigt, zusätzliche Authentifizierungsverfahren, Sicherheitsmechanismen oder Identitätsnachweise einzuführen oder bestehende Verfahren anzupassen.

(6) Die Plattform unterstützt Single-Sign-On-Verfahren (SSO) über die BOS-ID im Rahmen der jeweils bereitgestellten technischen Möglichkeiten.

(7) Der Anbieter kann die Anbindung externer Identitätsprovider ermöglichen. Hierzu können insbesondere Microsoft Entra ID (Azure AD), Keycloak oder vergleichbare Systeme gehören.

(8) Die Nutzung externer Identitätsprovider setzt die technische Kompatibilität, sowie die jeweilige Freischaltung durch den Anbieter voraus.

(9) Benutzer können ihre Zugangsdaten (Passwort) im Rahmen der bereitgestellten Funktionen eigenständig zurücksetzen oder ändern.

(10) Der Kunde ist verpflichtet, die Vertraulichkeit von Zugangsdaten sicherzustellen und eine Weitergabe an Dritte zu verhindern.

(11) Der Anbieter ist berechtigt, die Anzahl gleichzeitiger Sitzungen, Anmeldungen oder aktiver Verbindungen je Benutzerkonto technisch zu begrenzen.

(12) Der Anbieter kann Sitzungen automatisch beenden, wenn dies aus Sicherheitsgründen, zur Vermeidung von Missbrauch oder zur Wahrung der Systemstabilität erforderlich ist.

(13) Der Anbieter ist berechtigt, verdächtige Anmeldeversuche, ungewöhnliche Zugriffsmuster oder sicherheitsrelevante Aktivitäten automatisiert zu erkennen, einzuschränken oder vorübergehend zu blockieren.

(14) Der Anbieter kann zusätzliche Sicherheitsmaßnahmen wie Multi-Faktor-Authentifizierung, Gerätevalidierung, IP-basierte Schutzmechanismen oder vergleichbare Verfahren bereitstellen.

(15) Ein Anspruch auf bestimmte Authentifizierungsverfahren, Identitätsprovider oder Sicherheitsfunktionen besteht nur, soweit diese ausdrücklich Bestandteil des jeweiligen Leistungspakets oder einer gesonderten Vereinbarung sind.

§ 11 Passwort- und Sicherheitsanforderungen

(1) Die Authentifizierung von Benutzern erfolgt grundsätzlich über den BOS-ID-Account oder ein vom Anbieter bereitgestelltes Nachfolgesystem.

(2) Die Anforderungen an Passwörter, Passwortkomplexität, Passwortwechsel, Passwortschutz sowie weitere Authentifizierungsmerkmale werden grundsätzlich durch den BOS-ID-Account beziehungsweise die jeweils eingesetzten Authentifizierungssysteme vorgegeben.

(3) Benutzer sind verpflichtet, ihre Zugangsdaten vertraulich zu behandeln und vor dem Zugriff unberechtigter Dritter zu schützen.

(4) Zugangsdaten dürfen nicht weitergegeben, gemeinsam genutzt oder anderen Personen zugänglich gemacht werden.

(5) Der Kunde hat sicherzustellen, dass Benutzer ausschließlich über die ihnen persönlich zugeordneten Benutzerkonten auf BOS-ID zugreifen.

(6) Die Nutzung von Multi-Faktor-Authentifizierung (MFA) ist optional über den BOS-ID-Account kostenfrei möglich und wird ausdrücklich empfohlen.

© by MP-BOS GmbH

(7) Der Anbieter ist berechtigt, zusätzliche Sicherheitsanforderungen einzuführen oder bestehende Sicherheitsanforderungen anzupassen, soweit dies zur Aufrechterhaltung eines angemessenen Sicherheitsniveaus erforderlich ist.

(8) Der Anbieter kann Benutzerkonten, Sitzungen oder Zugriffe vorübergehend sperren, einschränken oder beenden, wenn konkrete Anhaltspunkte für eine Kompromittierung, missbräuchliche Nutzung oder sonstige sicherheitsrelevante Risiken bestehen.

(9) Der Kunde ist verpflichtet, dem Anbieter unverzüglich bekannt gewordene Sicherheitsvorfälle, unbefugte Zugriffe, kompromittierte Zugangsdaten oder sonstige sicherheitsrelevante Ereignisse mitzuteilen.

(10) Der Anbieter ist berechtigt, zur Abwehr von Sicherheitsrisiken angemessene technische und organisatorische Maßnahmen zu ergreifen, auch wenn hierdurch einzelne Funktionen oder Zugriffe vorübergehend eingeschränkt werden.

(11) Weitergehende Sicherheitsanforderungen können sich aus der Informationssicherheitsrichtlinie (Anlage 4), den technischen Dokumentationen oder den jeweils eingesetzten Authentifizierungssystemen ergeben.

§ 12 Zulässige Nutzung

(1) BOS-ID darf ausschließlich im Rahmen der vertraglich vereinbarten Zwecke sowie entsprechend der bereitgestellten Funktionen und Leistungspakete genutzt werden.

(2) Die Nutzung der Plattform hat unter Beachtung aller anwendbaren gesetzlichen Vorschriften, behördlichen Anforderungen sowie der vertraglichen Regelungen zu erfolgen.

(3) Der Kunde darf BOS-ID ausschließlich für die im jeweiligen Vertragsverhältnis vorgesehenen organisatorischen, administrativen, fachlichen und betrieblichen Zwecke einsetzen.

(4) Eine Bereitstellung von BOS-ID als eigenständige Software-as-a-Service-Leistung zugunsten Dritter ist unzulässig, soweit hierfür keine ausdrückliche vertragliche Vereinbarung, insbesondere im Rahmen eines White-Label-Vertrags, besteht.

(5) Die Nutzung der Plattform zur Speicherung, Verarbeitung, Verbreitung oder Bereitstellung rechtswidriger Inhalte ist unzulässig.

(6) Unzulässig sind insbesondere Inhalte oder Nutzungen, die gegen Strafgesetze, Datenschutzvorschriften, Urheberrechte, Markenrechte, Persönlichkeitsrechte oder sonstige Rechte Dritter verstoßen.

(7) Lasttests, Penetrationstests, Schwachstellenanalysen, Sicherheitstests oder vergleichbare technische Prüfungen dürfen ausschließlich nach vorheriger schriftlicher Freigabe durch den Anbieter durchgeführt werden.

(8) Automatisierte Datenabfragen, automatisierte Datenerfassung, Crawling, Scraping oder vergleichbare Verfahren sind ausschließlich über die hierfür vorgesehenen und freigegebenen Schnittstellen zulässig.

(9) Die Nutzung automatisierter Verfahren außerhalb der bereitgestellten APIs oder sonstigen vorgesehenen Integrationsmechanismen ist unzulässig.

(10) Die Plattform darf nicht genutzt werden, um gesetzliche, behördliche, regulatorische oder vertragliche Verpflichtungen zu umgehen oder zu verletzen.

(11) Der Anbieter ist berechtigt, bei Verstößen gegen die zulässige Nutzung angemessene technische, organisatorische oder vertragliche Maßnahmen zu ergreifen, einschließlich der vorübergehenden Einschränkung oder Sperrung von Funktionen oder Benutzerkonten.

(12) Weitergehende Regelungen zur zulässigen Nutzung ergeben sich aus den AGB, der Informationssicherheits-richtlinie sowie den jeweils bereitgestellten technischen Dokumentationen.

§ 13 Unzulässige Nutzung

(1) Jede Nutzung von BOS-ID, die gegen gesetzliche Vorschriften, behördliche Anordnungen, vertragliche Vereinbarungen oder berechtigte Sicherheitsinteressen verstößt, ist unzulässig.

© by MP-BOS GmbH

(2) Dem Kunden sowie dessen Benutzern ist insbesondere untersagt:

- Schadsoftware, Viren, Trojaner, Ransomware oder sonstige schädliche Programme zu speichern, zu verbreiten oder auszuführen
- Sicherheitsmechanismen, Zugriffskontrollen oder technische Schutzmaßnahmen zu umgehen
- bekannte oder vermutete Sicherheitslücken auszunutzen
- unberechtigte Zugriffe auf Daten, Benutzerkonten, Mandanten oder Systeme vorzunehmen
- die Plattform oder einzelne Komponenten zu manipulieren oder zu beeinträchtigen
- automatisierte Verfahren außerhalb der bereitgestellten und freigegebenen Schnittstellen einzusetzen
- unzulässige Lasttests, Penetrationstests, Sicherheitstests oder Schwachstellenanalysen durchzuführen
- Spam-Nachrichten, Massenmailings oder vergleichbare Kommunikationsmaßnahmen über die Plattform zu versenden
- die Plattform für Kryptowährungs-Mining oder vergleichbare ressourcenintensive Berechnungen zu verwenden
- die Plattform als Hosting-, Speicher-, Content- oder Bereitstellungsdienst für nicht vertragsgemäße Inhalte Dritter zu nutzen
- rechtswidrige Inhalte bereitzustellen, zu speichern oder zu verbreiten
- Schutzrechte, Datenschutzrechte oder sonstige Rechte Dritter zu verletzen

(3) Es ist untersagt, technische oder organisatorische Maßnahmen zu umgehen, die der Begrenzung von Nutzungsumfängen, Benutzerzahlen, Speicherkontingenten, API-Limits, Lizenzmodellen oder Leistungspaketen dienen.

(4) Eine Nutzung, die geeignet ist, andere Mandanten, Kunden, Benutzer oder die technische Infrastruktur von BOS-ID zu beeinträchtigen, zu stören oder unverhältnismäßig zu belasten, ist unzulässig.

(5) Insbesondere dürfen keine Handlungen vorgenommen werden, die die Verfügbarkeit, Integrität, Vertraulichkeit oder Stabilität der Plattform gefährden.

(6) Der Anbieter ist berechtigt, Verstöße gegen diese Bestimmungen zu dokumentieren, auszuwerten und als Nachweis für vertragliche, gesetzliche oder gerichtliche Verfahren zu verwenden.

(7) Bei schwerwiegenden oder wiederholten Verstößen ist der Anbieter berechtigt, Benutzerkonten, Funktionen, Mandanten oder Zugänge mit sofortiger Wirkung vorübergehend oder dauerhaft zu sperren.

(8) Weitergehende vertragliche oder gesetzliche Rechte des Anbieters bleiben unberührt.

§ 14 Speicher- und Nutzungslimits

(1) Die Nutzung von BOS-ID kann abhängig vom jeweils gebuchten Leistungspaket technischen oder organisatorischen Nutzungslimits unterliegen.

(2) Nutzungslimits können insbesondere für folgende Bereiche festgelegt werden:

- Ausweiskontingent
- Speicherplatz
- API-Nutzung bzw. API-Transaktionen

(3) Die jeweils geltenden Nutzungslimits ergeben sich aus der zum Zeitpunkt des Vertragsschlusses gültigen Leistungs- und Preisübersicht oder dem individuellen Angebot.

(4) Der Anbieter ist berechtigt, die Einhaltung vereinbarter Nutzungslimits technisch zu überwachen und hierfür geeignete Mess- und Auswertungsverfahren einzusetzen.

(5) Soweit technisch vorgesehen, kann der Anbieter den Kunden über das Erreichen oder Überschreiten bestimmter Nutzungsschwellen informieren.

(6) Die Benachrichtigung über die Erreichung oder Überschreitung von Nutzungslimits begründet keine Verpflichtung des Anbieters zur fortlaufenden Überwachung oder Warnung.

(7) Wird ein vereinbartes Nutzungslimit überschritten, kann der Anbieter dem Kunden zusätzliche Nutzungs-kontingente oder Leistungserweiterungen anbieten.

© by MP-BOS GmbH

(8) Eine Erweiterung von Nutzungskontingenten erfolgt ausschließlich auf Grundlage einer gesonderten Beauftragung oder Vereinbarung.

(9) Der Kunde hat keinen Anspruch auf eine automatische Erweiterung von Speicher- oder Nutzungskontingenten.

(10) Bei fortdauernder oder erheblicher Überschreitung vereinbarter Nutzungslimits ist der Anbieter berechtigt, die betroffenen Funktionen angemessen einzuschränken, bis ein vertragskonformer Zustand wiederhergestellt wurde oder eine entsprechende Erweiterung beauftragt wurde.

(11) Die Einschränkung von Funktionen nach Absatz 10 lässt die sonstigen Rechte und Pflichten der Vertragsparteien unberührt.

(12) Der Anbieter ist berechtigt, technische Verfahren zur Vermeidung einer Beeinträchtigung der Systemstabilität, Sicherheit oder Leistungsfähigkeit einzusetzen, sofern Nutzungslimits überschritten werden.

§ 15 Datenimporte

(1) BOS-ID kann Funktionen zum Import von Daten aus externen Quellen bereitstellen.

(2) Soweit Importfunktionen bereitgestellt werden, erfolgt der Datenimport grundsätzlich über die vom Anbieter unterstützten Excel-Formate und die hierfür vorgesehenen Importmechanismen.

(3) Der Umfang der verfügbaren Importfunktionen kann abhängig vom jeweils gebuchten Leistungspaket variieren.

(4) Der Kunde ist für die Richtigkeit, Vollständigkeit, Aktualität, Qualität und Rechtmäßigkeit der importierten Daten allein verantwortlich.

(5) Der Kunde hat vor einem Import sicherzustellen, dass die bereitgestellten Daten den technischen Vorgaben und Formatanforderungen des Anbieters entsprechen.

(6) Fehlerhafte, unvollständige, widersprüchliche oder technisch ungeeignete Importdaten können zu Einschränkungen, Fehlfunktionen, fehlerhaften Verarbeitungsergebnissen oder Dateninkonsistenzen führen.

(7) Der Anbieter übernimmt keine Verantwortung für Fehler oder Beeinträchtigungen, die auf die Qualität oder Beschaffenheit der vom Kunden bereitgestellten Importdaten zurückzuführen sind.

(8) Der Anbieter ist berechtigt, Importvorgänge ganz oder teilweise abzulehnen, zu unterbrechen oder einzuschränken, wenn technische Risiken bestehen, Sicherheitsrisiken bestehen, die Integrität der Plattform gefährdet werden könnte, die bereitgestellten Daten den technischen Anforderungen nicht entsprechen.

(9) Der Anbieter kann für bestimmte Importvorgänge Vorlagen, technische Spezifikationen oder Prüfmechanismen bereitstellen.

(10) Unterstützungsleistungen, Datenmigrationen, Massenimporte, Datenbereinigungen oder sonstige Importdienstleistungen können als gesonderte kostenpflichtige Leistungen beauftragt werden.

(11) Der Anbieter ist berechtigt, Importfunktionen technisch weiterzuentwickeln, anzupassen oder zu erweitern, soweit hierdurch die vertragsgemäße Nutzung nicht wesentlich beeinträchtigt wird.

§ 16 Datenexporte

(1) Die Herausgabe von Kundendaten erfolgt ausschließlich nach Maßgabe der AGB, sowie der dort geregelten Export- und Löschfristen.

(2) Ein Anspruch auf Datenexporte während der Vertragslaufzeit besteht nur, soweit dies ausdrücklich vereinbart wurde.

(3) Die Daten werden in einem vom Anbieter unterstützten maschinenlesbaren Standardformat als SQL-Datenbank bereitgestellt.

(4) Individuelle Exportformate, Sonderauswertungen oder migrationsspezifische Datenaufbereitungen sind nicht Bestandteil der vertraglichen Leistungen und können gesondert beauftragt werden.

© by MP-BOS GmbH

(5) Der Anbieter ist berechtigt, Exportvorgänge aus technischen, sicherheitsrelevanten oder rechtlichen Gründen einzuschränken oder auszusetzen.

(6) Weitergehende Regelungen zur Datenherausgabe ergeben sich aus den AGB, sowie dem Auftragsverarbeitungsvertrag.

§ 17 Archivierung und Aufbewahrung

(1) BOS-ID kann Funktionen zur Archivierung von Daten, Datensätzen, Dokumenten oder sonstigen Informationen bereitstellen.

(2) Archivierte Daten bleiben grundsätzlich innerhalb des Systems gespeichert, werden jedoch entsprechend ihrer Archivierungseigenschaften von aktiven Arbeitsprozessen getrennt oder eingeschränkt dargestellt.

(3) Die Archivierung dient der organisatorischen Trennung, Strukturierung und Verwaltung von Datenbeständen und ist nicht mit einer Löschung gleichzusetzen.

(4) Zwischen archivierten und gelöschten Daten ist technisch und organisatorisch zu unterscheiden.

(5) Archivierte Daten können im Rahmen der jeweils bereitgestellten Funktionen weiterhin eingesehen, ausgewertet oder wiederhergestellt werden, soweit dies technisch vorgesehen ist.

(6) Die Bereitstellung von Archivierungsfunktionen begründet keine Übernahme gesetzlicher Aufbewahrungs-, Nachweis-, Dokumentations- oder Archivierungspflichten des Kunden.

(7) Der Kunde bleibt allein verantwortlich für die Einhaltung sämtlicher ihn betreffender gesetzlichen Aufbewahrungsfristen und Dokumentationspflichten.

(8) Der Anbieter ist berechtigt, Archivierungsfunktionen technisch weiterzuentwickeln, anzupassen oder zu erweitern, soweit hierdurch die vertragsgemäße Nutzung nicht wesentlich beeinträchtigt wird.

(9) Die Archivierung von Daten begründet keinen Anspruch auf eine dauerhafte Speicherung über die vertraglich vereinbarte Laufzeit hinaus.

(10) Nach Beendigung des Vertragsverhältnisses gelten die Regelungen der AGB zur Datenherausgabe, Exportfrist und Datenlöschung.

(11) Archivierte Daten können daher nach Ablauf der vertraglich vereinbarten Exportfrist gelöscht werden, soweit keine gesetzlichen Verpflichtungen oder zwingenden rechtlichen Gründe entgegenstehen.

(12) Die Einzelheiten der Archivierungsfunktionen ergeben sich aus den jeweils bereitgestellten Funktionen und Modulen von BOS-ID.

§ 18 Test- und Demo-Umgebungen

(1) Test-, Demo-, Schulungs-, Staging- oder vergleichbare Nicht-Produktivumgebungen sind nicht Bestandteil der Standardleistungen von BOS-ID.

(2) Der Anbieter kann solche Umgebungen ausschließlich im Rahmen gesonderter Vereinbarungen bereitstellen.

(3) Test- und Demoumgebungen dienen ausschließlich Evaluierungs-, Schulungs-, Integrations-, Entwicklungs-, Konfigurations- oder Testzwecken.

(4) Der Kunde ist für die in Test- oder Demoumgebungen gespeicherten Daten selbst verantwortlich.

(5) Soweit der Kunde produktionsnahe oder produktive Daten in Testumgebungen verwendet, erfolgt dies ausschließlich in seiner eigenen Verantwortung.

(6) Der Anbieter empfiehlt, in Test- und Demoumgebungen ausschließlich anonymisierte, pseudonymisierte oder anderweitig geeignete Testdaten zu verwenden.

(7) Der Anbieter ist berechtigt, Test- und Demoumgebungen jederzeit ganz oder teilweise zurückzusetzen, neu aufzubauen, zu aktualisieren, zu löschen oder technisch zu verändern.

© by MP-BOS GmbH

(8) Der Kunde hat keinen Anspruch auf die dauerhafte Speicherung von Daten innerhalb von Test- oder Demoumgebungen.

(9) Für Test- und Demoumgebungen gelten keine mit Produktivsystemen vergleichbaren Verfügbarkeits-, Leistungs-, Wiederherstellungs- oder Servicezusagen.

(10) Soweit nicht ausdrücklich anders vereinbart, finden die Regelungen des Service Level Agreements auf Test- und Demoumgebungen keine Anwendung.

(11) Der Anbieter ist berechtigt, Test- und Demoumgebungen jederzeit einzuschränken, auszusetzen oder einzustellen, soweit hierfür technische, organisatorische, wirtschaftliche oder sicherheitsrelevante Gründe bestehen.

(12) Hieraus entstehen dem Kunden keine Ansprüche auf Entschädigung, Schadensersatz oder sonstige Ausgleichsleistungen.

(13) Test- und Demoumgebungen sind nicht für den produktiven Geschäftsbetrieb bestimmt.

(14) Der Kunde hat geeignete organisatorische Maßnahmen zu treffen, um eine versehentliche Nutzung von Test- oder Demoumgebungen als Produktivsystem zu vermeiden.

§ 19 Release-, Update- und Upgrade-Management

(1) Der Anbieter entwickelt BOS-ID fortlaufend weiter und stellt Updates, Upgrades, Fehlerkorrekturen, Sicherheitsupdates, sowie sonstige Weiterentwicklungen nach eigenem Ermessen bereit.

(2) Releases, Updates und Upgrades werden grundsätzlich zentral durch den Anbieter bereitgestellt und automatisch in die Produktivumgebung eingespielt bzw. als neue App in den beiden App-Stores zur Verfügung gestellt.

(3) BOS-ID wird als Software-as-a-Service ausschließlich in der jeweils aktuellen Version betrieben und bereitgestellt.

(4) Der Kunde hat keinen Anspruch auf die Nutzung bestimmter Softwareversionen, Releases, technischen Implementierungen oder früherer Systemzustände.

(5) Insbesondere besteht kein Anspruch auf die Bereitstellung, Wiederherstellung oder den Weiterbetrieb älterer Versionen, Funktionen oder Systemstände.

(6) Der Anbieter kann unterschiedliche Release-Kanäle bereitstellen.

(7) Hierzu können insbesondere gehören Standard-Releases und Beta-Releases.

(8) Beta-Releases, Testfunktionen, Vorschaufunktionen oder vergleichbare Vorabversionen können unvollständig sein und ausschließlich zu Test- oder Evaluierungszwecken bereitgestellt werden.

(9) Für Beta-Releases gelten keine Zusagen hinsichtlich Verfügbarkeit, Fehlerfreiheit, Funktionsumfang, Stabilität oder Kompatibilität.

(10) Der Anbieter ist berechtigt, Beta-Funktionen jederzeit zu ändern, einzuschränken oder einzustellen.

(11) Der Anbieter kann Funktionen, Schnittstellen, Module oder technische Komponenten als veraltet („deprecated“) kennzeichnen. Diese können nach angemessener Übergangsfrist geändert, ersetzt oder entfernt werden.

(12) Der Anbieter wird den Kunden über wesentliche Änderungen, soweit für die Nutzung relevant, in geeigneter Weise informieren. Die Information kann insbesondere über Release Notes, Produktinformationen, Systemhinweise, E-Mail-Mitteilungen oder vergleichbare Kommunikationswege erfolgen.

(13) Der Anbieter ist berechtigt, Updates und Änderungen auch dann durchzuführen, wenn hierdurch Anpassungen von Prozessen, Benutzeroberflächen, Datenstrukturen oder Integrationen erforderlich werden, soweit die vertragsgemäße Nutzung insgesamt erhalten bleibt.

(14) Der Kunde ist verpflichtet, seine organisatorischen Prozesse sowie gegebenenfalls eingesetzte Integrationen und Schnittstellen an notwendige Änderungen anzupassen.

© by MP-BOS GmbH

(15) Ein Anspruch auf die Entwicklung, Einführung oder Beibehaltung bestimmter Funktionen oder Produktbestandteile besteht nicht.

§ 20 Sicherheitsmaßnahmen des Kunden

(1) Der Kunde ist verpflichtet, angemessene technische und organisatorische Maßnahmen zu treffen, um die sichere Nutzung von BOS-ID innerhalb seines Verantwortungsbereichs sicherzustellen.

(2) Der Kunde hat sicherzustellen, dass für die Nutzung von BOS-ID ausschließlich aktuelle und unterstützte Browser, Betriebssysteme und sonstige technische Komponenten verwendet werden.

(3) Der Kunde ist verpflichtet, verfügbare Sicherheitsupdates, Fehlerkorrekturen und sonstige sicherheitsrelevante Aktualisierungen für die von ihm eingesetzten Systeme zeitnah einzuspielen.

(4) Der Kunde ist für die Sicherheit seiner Endgeräte, Netzwerke, Internetzugänge, Arbeitsplatzsysteme sowie sonstiger technischer Infrastruktur selbst verantwortlich.

(5) Der Kunde hat geeignete Maßnahmen zum Schutz vor Schadsoftware, unbefugten Zugriffen, Datenverlusten und sonstigen Sicherheitsrisiken zu treffen.

(6) Der Kunde ist verpflichtet, seine Benutzer angemessen über Informationssicherheit, Datenschutz, Zugangsschutz und die sichere Nutzung der Plattform zu sensibilisieren.

(7) Dem Kunden bekannt gewordene Sicherheitsvorfälle, Sicherheitsmängel, unbefugte Zugriffe oder Kompromittierungen von Benutzerkonten sind dem Anbieter unverzüglich mitzuteilen.

(8) Der Kunde wird den Anbieter bei der Untersuchung und Behebung sicherheitsrelevanter Vorfälle angemessen unterstützen.

(9) Verstößt der Kunde erheblich gegen Sicherheitsanforderungen oder bestehen konkrete Sicherheitsrisiken für die Plattform, andere Kunden oder die Betriebsumgebung, ist der Anbieter berechtigt, angemessene Schutzmaßnahmen zu ergreifen.

(10) Solche Maßnahmen können insbesondere die vorübergehende Einschränkung von Funktionen, Benutzerkonten, Zugriffsrechten oder sonstigen Nutzungsmöglichkeiten umfassen.

(11) Weitergehende vertragliche oder gesetzliche Rechte des Anbieters bleiben unberührt.

§ 21 Dokumentation und Benutzerinformationen

(1) Der Anbieter kann für BOS-ID Dokumentationen, Benutzerinformationen, Online-Hilfen, Wissensdatenbanken, Help-Center-Inhalte, Release Notes, technische Beschreibungen oder vergleichbare Informationsmaterialien bereitstellen.

(2) Die Bereitstellung der Dokumentation erfolgt grundsätzlich in elektronischer Form. Ein Anspruch auf die Bereitstellung gedruckter Dokumentationen, Handbücher oder sonstiger physischer Unterlagen besteht nicht.

(3) Der Anbieter ist berechtigt, Dokumentationen und Benutzerinformationen jederzeit zu aktualisieren, anzupassen, zu ergänzen oder zu ersetzen. Er übernimmt keine Gewähr dafür, dass Dokumentationen jederzeit vollständig, fehlerfrei oder für jeden individuellen Anwendungsfall geeignet sind.

(4) Die Dokumentation dient ausschließlich der Beschreibung und Unterstützung der Nutzung von BOS-ID.

(5) Aus Dokumentationen, Benutzerinformationen, Hilfetexten, Wissensdatenbanken oder vergleichbaren Informationsquellen ergeben sich keine über den Vertrag hinausgehenden Leistungs-, Beschaffenheits- oder Garantiezusagen.

(6) Maßgeblich für den geschuldeten Leistungsumfang sind ausschließlich die vertraglichen Vereinbarungen, die Leistungsbeschreibung, das jeweils gebuchte Leistungspaket sowie die AGB.

(7) Der Anbieter kann zusätzlich eine öffentliche oder zugangsbeschränkte Wissensdatenbank, ein Help Center oder vergleichbare Informationsplattformen betreiben. Inhalte solcher Informationsplattformen können insbesondere

© by MP-BOS GmbH

Anleitungen, Hilfestellungen, technische Informationen, Release Notes, Best Practices und häufig gestellte Fragen umfassen.

(8) Schulungen, Workshops, Einweisungen, Trainings, individuelle Beratungen oder sonstige Unterstützungsleistungen sind nicht Bestandteil der Standardleistungen und können als gesonderte kostenpflichtige Leistungen beauftragt werden.

§ 22 Supportleistungen

(1) Der Anbieter kann für BOS-ID Supportleistungen zur Unterstützung bei der Nutzung der Plattform bereitstellen.

(2) Der Umfang der Supportleistungen richtet sich nach dem jeweils gebuchten Leistungspaket, dem Service Level Agreement (SLA), sowie den vertraglichen Vereinbarungen.

§ 23 Wartungsfenster

(1) Der Anbieter ist berechtigt, Wartungs-, Aktualisierungs-, Sicherheits-, Optimierungs- oder sonstige technische Arbeiten an BOS-ID durchzuführen.

(2) Die Einzelheiten zu regulären Wartungsfenstern, Wartungszeiten und Wartungsverfahren ergeben sich aus der Anlage 2 Service Level Agreement (SLA).

§ 24 Leistungsänderungen

(1) Der Anbieter entwickelt BOS-ID kontinuierlich weiter und ist berechtigt, Funktionen, Module, Prozesse, Schnittstellen, Benutzeroberflächen, sowie sonstige Bestandteile der Plattform zu ändern, zu erweitern, zu optimieren oder zu ersetzen.

(2) Der Anbieter ist berechtigt, neue Funktionen, Module oder Produktbereiche einzuführen und bestehende Funktionen weiterzuentwickeln.

(3) Funktionen, Module oder Bestandteile der Plattform können insbesondere geändert, ersetzt oder eingestellt werden, wenn
a) ein gleichwertiger oder verbesserter Ersatz bereitgestellt wird,
b) die Nutzung der betreffenden Funktion nur noch in geringem Umfang erfolgt,
c) technische, sicherheitsrelevante, wirtschaftliche oder regulatorische Gründe dies erforderlich machen,
d) die Wartung oder Weiterentwicklung unverhältnismäßig erschwert wird.

(4) Der Anbieter ist berechtigt, Benutzeroberflächen, Designkonzepte, Bedienabläufe, Navigationsstrukturen und sonstige Elemente der Benutzerführung jederzeit anzupassen oder weiterzuentwickeln.

(5) Der Kunde hat keinen Anspruch auf die unveränderte Beibehaltung bestimmter Benutzeroberflächen, Designs, Workflows, Darstellungen oder Bedienkonzepte.

(6) Leistungsänderungen dürfen die vertragsgemäße Nutzbarkeit der Plattform insgesamt nicht wesentlich beeinträchtigen.

(7) Der Anbieter wird den Kunden über wesentliche Änderungen in angemessener Weise informieren.

(8) Die Information kann insbesondere über Release Notes, Produktinformationen, Systemmitteilungen, Kundenportale oder vergleichbare Kommunikationswege erfolgen.

(9) Soweit Leistungsänderungen Anpassungen von Integrationen, Schnittstellen oder organisatorischen Prozessen des Kunden erforderlich machen, ist der Kunde für die Umsetzung dieser Anpassungen verantwortlich.

(10) Die vorstehenden Regelungen gelten entsprechend für White-Label-Installationen sowie sonstige kundenspezifische Bereitstellungsformen von BOS-ID.

(11) Weitergehende Regelungen zu Vertragsänderungen und Änderungen der AGB bleiben unberührt.

© by MP-BOS GmbH

■ Anlage 2

Service Level Agreement (SLA)

§ 1 Gegenstand des SLA

(1) Dieses Service Level Agreement (SLA) konkretisiert die Service-, Support-, Verfügbarkeits- und Betriebsleistungen des Anbieters für die SaaS-Plattform BOS-ID.

(2) Das SLA ist Bestandteil des zwischen den Vertragsparteien geschlossenen Vertrags über die Nutzung von BOS-ID.

(3) Die Regelungen dieses SLA gelten für sämtliche Leistungspakete von BOS-ID.

(4) Jedes Leistungspaket beinhaltet grundsätzlich den SLA-Level „Basic", soweit nicht ausdrücklich ein anderer SLA-Level vereinbart wurde.

(5) Der Kunde kann gegen gesonderte Vergütung einen erweiterten SLA-Level buchen.

(6) Zum Zeitpunkt des Vertragsschlusses können folgende SLA-Level angeboten werden:
- Basic
- Standard
- Premium

(7) Die jeweils geltenden Serviceleistungen, Reaktionszeiten, Wiederherstellungszeiten, Verfügbarkeiten und sonstigen Serviceparameter richten sich ausschließlich nach dem vertraglich vereinbarten SLA-Level.

(8) Die einzelnen SLA-Level bauen aufeinander auf und können unterschiedliche Leistungsumfänge, Servicezeiten, Supportkanäle, Prioritäten und Reaktionszeiten enthalten.

(9) Dieses SLA gilt ausschließlich für Produktivsysteme von BOS-ID.

(10) Test-, Demo-, Schulungs-, Staging- oder sonstige Nicht-Produktivumgebungen unterliegen nicht den Regelungen dieses SLA, soweit nicht ausdrücklich etwas anderes vereinbart wurde.

(11) Die Regelungen dieses SLA gelten entsprechend für White-Label-Installationen von BOS-ID, soweit nicht abweichende Vereinbarungen getroffen wurden.

(12) Maßgeblich für die jeweils geschuldeten Leistungen sind die Regelungen dieses SLA in Verbindung mit dem gebuchten Leistungspaket, dem vereinbarten SLA-Level, den AGB sowie der Leistungsbeschreibung.

§ 2 Leistungsumfang

(1) Supportleistungen können insbesondere über folgende Kommunikationswege erbracht werden:
- Ticketsystem
- E-Mail
- Supportportal (Wissensdatenbank / Erklärvideo)
- Telefon

(2) Der Anbieter ist berechtigt, einzelne Supportkanäle abhängig vom gebuchten SLA-Level bereitzustellen oder einzuschränken.

(3) Telefonsupport ist ausschließlich dem SLA-Level „Standard" und „Premium" vorbehalten. Telefonsupport für Hotline-Fragen ist dabei unbegrenzt. Telefonsupport für Anwenderfragen ist im SLA-Level „Standard" auf 15 Minuten und im SLA-Level „Premium" auf 30 Minuten summiert pro Monat begrenzt. Zusätzlich Minuten werden je angefangene Zeiteinheit (15 Minuten zu 25,- € netto) kostenpflichtig abgerechnet. Nicht verbrauchte Minutenkontingente können nicht auf andere Monate übertragen werden.

(4) Supportleistungen werden grundsätzlich ausschließlich gegenüber den vom Kunden benannten und autorisierten Ansprechpartnern erbracht. Die Anzahl der berechtigten Ansprechpartner ist abhängig vom gebuchten SLA-Level begrenzt. Im Level „Basic" auf 1 Ansprechpartner, im Level „Standard" auf 3 Ansprechpartner und im Level „Premium" auf 5 Ansprechpartner.

© by MP-BOS GmbH

(5) Der Kunde hat sicherzustellen, dass Supportanfragen nach Möglichkeit zunächst intern geprüft und qualifiziert werden.

(6) Der Support umfasst insbesondere Unterstützung bei Fragen zur Nutzung, Bedienung und Konfiguration der bereitgestellten Funktionen von BOS-ID.

(7) Nicht Bestandteil der Standard-Supportleistungen sind insbesondere:
- individuelle Beratungsleistungen
- kundenspezifische Entwicklungen
- Datenmigrationen
- individuelle Integrationen
- Schulungen
- Prozessberatung
- Anpassungen außerhalb des Standardfunktionsumfangs

(8) Leistungen gemäß Absatz 7 können als gesonderte kostenpflichtige Leistungen beauftragt werden.

(9) Der Anbieter ist berechtigt, Supportanfragen nach Art, Umfang, Priorität und Komplexität zu klassifizieren und zu bearbeiten.

(10) Ein Anspruch auf bestimmte Reaktionszeiten, Bearbeitungszeiten oder Lösungszeiten besteht nur im Rahmen des jeweils vereinbarten SLA-Levels.

§ 3 Servicezeiten

(1) Servicezeiten im Sinne dieses SLA sind die Zeiträume, innerhalb derer Supportleistungen erbracht sowie SLA-relevante Reaktions- und Bearbeitungszeiten gemessen werden.

(2) Soweit nicht ausdrücklich etwas anderes vereinbart wurde, gelten für die SLA-Level „Basic", „Standard" und „Premium" dieselben Servicezeiten. Die regulären Servicezeiten sind Montag bis Freitag von 08:00 Uhr bis 16:00 Uhr (MEZ/MESZ).

(3) Samstage, Sonntage sowie gesetzliche Feiertage am Sitz des Anbieters gelten nicht als Servicezeiten.

(4) Außerhalb der Servicezeiten besteht kein Anspruch auf die Erbringung von Supportleistungen, Reaktionszeiten oder sonstigen Serviceleistungen, soweit nicht ausdrücklich etwas anderes vereinbart wurde.

(5) Geht eine Supportanfrage, Störungsmeldung oder sonstige SLA-relevante Meldung außerhalb der Servicezeiten ein, beginnt die Berechnung der jeweiligen Reaktions- oder Bearbeitungszeit mit Beginn der nächsten Servicezeit.

(6) Maßgeblich für den Beginn der Servicezeitberechnung ist der Eingang der Meldung über die vom Anbieter vorgesehenen Supportkanäle.

(7) Der Anbieter ist berechtigt, Servicezeiten im Rahmen zukünftiger SLA-Level oder gesonderter Vereinbarungen zu erweitern.

(8) Abweichende Servicezeiten können insbesondere für individuelle Enterprise-Vereinbarungen gesondert vereinbart werden.

§ 4 Verfügbarkeit

(1) Der Anbieter gewährleistet für die Produktivumgebung von BOS-ID eine monatliche Verfügbarkeit von 99,0 % im Kalendermonat für die SLA-Level Basic und Standard, sowie eine monatliche Verfügbarkeit von 99,9 % für den SLA-Level Professional.

(2) Die Verfügbarkeit wird auf Basis des jeweiligen Kalendermonats berechnet.

(3) Verfügbarkeit im Sinne dieses SLA liegt vor, wenn die wesentlichen Funktionen von BOS-ID für den Kunden nutzbar sind.

© by MP-BOS GmbH

(4) Die Verfügbarkeit wird auf Grundlage der durch den Anbieter eingesetzten Monitoring- und Messsysteme ermittelt.

(5) Maßgeblich sind ausschließlich die vom Anbieter erhobenen Messdaten, soweit der Kunde keine abweichenden Nachweise erbringt.

(6) Nicht als Nichtverfügbarkeit gelten insbesondere:
- angekündigte Wartungsfenster
- Notfallwartungen
- vom Kunden verursachte Störungen
- Störungen innerhalb der IT-Infrastruktur des Kunden
- Ausfälle von Internetzugängen, Netzwerken oder Telekommunikationsdiensten des Kunden
- Fehlkonfigurationen oder Fehlbedienungen durch den Kunden oder dessen Benutzer
- Störungen durch Drittanwendungen, Drittanbieter oder Fremdsysteme außerhalb des Verantwortungsbereichs des Anbieters
- Ereignisse höherer Gewalt
- behördliche Maßnahmen
- Sicherheitsmaßnahmen, die zur Abwehr akuter Gefahren für die Plattform oder deren Nutzer erforderlich sind

(7) Zeiten geplanter Wartungsarbeiten, sowie im SLA definierte Wartungsfenster bleiben bei der Berechnung der Verfügbarkeit unberücksichtigt.

(8) Gleiches gilt für Notfallwartungen, soweit diese zur Aufrechterhaltung der Sicherheit, Stabilität oder Integrität der Plattform erforderlich sind.

(9) Die Verfügbarkeitszusage gilt ausschließlich für die Produktivumgebung von BOS-ID.

(10) Test-, Demo-, Schulungs-, Staging- oder sonstige Nicht-Produktivumgebungen sind von der Verfügbarkeitszusage ausgenommen.

(11) Weitergehende Ansprüche aufgrund von Verfügbarkeitsabweichungen bestehen ausschließlich im Rahmen der vertraglich vereinbarten Haftungsregelungen.

§ 5 Wartungsfenster

(1) Der Anbieter ist berechtigt, Wartungs-, Aktualisierungs-, Sicherheits-, Optimierungs- oder sonstige technische Arbeiten an BOS-ID durchzuführen.

(2) Für Wartungsarbeiten besteht kein fest definiertes Wartungsfenster.

(3) Soweit Wartungsarbeiten planbar sind und voraussichtlich Auswirkungen auf die Verfügbarkeit oder Nutzbarkeit von BOS-ID haben, wird der Anbieter den Kunden mindestens 48 Stunden vor Beginn der Wartungsarbeiten informieren.

(4) Die Information kann insbesondere über E-Mail, Kundenportal, Systemmitteilungen oder vergleichbare Kommunikationswege erfolgen.

(5) Während angekündigter Wartungsarbeiten kann die Verfügbarkeit einzelner Funktionen oder der gesamten Plattform vorübergehend eingeschränkt oder vollständig unterbrochen sein. Dies stellt keinen Mangel der Leistung dar.

(6) Der Anbieter ist berechtigt, Notfallwartungen jederzeit durchzuführen, soweit dies zur Aufrechterhaltung von Sicherheit, Stabilität, Verfügbarkeit, Integrität oder Datenschutz erforderlich ist.

(7) Notfallwartungen können insbesondere durchgeführt werden bei Sicherheitsvorfällen, kritischen Sicherheitslücken, schwerwiegenden Systemstörungen, Ausfällen technischer Infrastruktur oder sonstigen erheblichen Betriebsrisiken.

(8) Soweit möglich und zumutbar, wird der Anbieter den Kunden über Notfallwartungen vorab informieren. Ist dies nicht möglich, erfolgt die Information unverzüglich nach Durchführung der Maßnahmen.

(9) Wartungszeiten und Notfallwartungen gelten nicht als Nichtverfügbarkeit im Sinne dieses SLA.

© by MP-BOS GmbH

(10) Wartungszeiten bleiben bei der Berechnung der vertraglich vereinbarten Verfügbarkeitswerte unberücksichtigt.

(11) Der Anbieter wird Wartungsarbeiten nach Möglichkeit so planen und durchführen, dass Beeinträchtigungen für den Kunden auf das notwendige Maß beschränkt werden.

§ 6 Störungsklassen

(1) Störungen werden entsprechend ihrer Auswirkungen auf die Nutzbarkeit von BOS-ID in die Störungsklassen I, II und III eingeteilt.

(2) Die Einstufung einer Störung erfolgt durch den Anbieter nach pflichtgemäßem Ermessen unter Berücksichtigung der tatsächlichen Auswirkungen auf die Nutzung der Plattform.

(3) Klasse I (leichte Störung)
Eine leichte Störung liegt vor, wenn lediglich geringfügige oder kosmetische Beeinträchtigungen bestehen, die die vertragsgemäße Nutzung von BOS-ID nicht wesentlich beeinträchtigen.
Hierzu können insbesondere Darstellungsfehler, Layoutfehler, geringfügige Funktionseinschränkungen oder sonstige Fehler ohne wesentliche Auswirkungen auf die Betriebsabläufe gehören.

(4) Klasse II (betriebsbehindernde Störung)
Eine betriebsbehindernde Störung liegt vor, wenn wesentliche Funktionen eingeschränkt nutzbar sind oder einzelne Geschäftsprozesse beeinträchtigt werden, die Nutzung von BOS-ID insgesamt jedoch weiterhin möglich bleibt.

(5) Klasse III (betriebsverhindernde Störung)
Eine betriebsverhindernde Störung liegt vor, wenn BOS-ID insgesamt nicht nutzbar ist oder eine wesentliche Kernfunktion vollständig ausfällt und dadurch eine vertragsgemäße Nutzung nicht mehr möglich ist.

(6) Maßgeblich für die Einstufung ist die tatsächliche Auswirkung auf die Nutzung des Systems und nicht allein die technische Ursache einer Störung.

(7) Der Anbieter ist berechtigt, die Einstufung einer Störung im Verlauf der Bearbeitung anzupassen, sofern neue Erkenntnisse oder veränderte Auswirkungen dies erforderlich machen.

§ 8 Service-Level-Beschreibung und Vergütung

(1) Die nachfolgenden Reaktions- und Wiederherstellungszeiten gelten für die jeweils vereinbarten SLA-Level.

(2) Sämtliche Zeitangaben beziehen sich auf die vereinbarten Servicezeiten gemäß §3 dieses SLA.

Störungsklasse	**Basic**	**Standard**	**Professional**
Klasse III Reaktionszeit	16 Stunden	8 Stunden	4 Stunden
Klasse III Wiederherstellungszeit	32 Stunden	16 Stunden	8 Stunden
Klasse II Reaktionszeit	24 Stunden	16 Stunden	8 Stunden
Klasse II Wiederherstellungszeit	48 Stunden	32 Stunden	16 Stunden
Klasse I Reaktionszeit	48 Stunden	24 Stunden	12 Stunden
Klasse I Wiederherstellungszeit	96 Stunden	48 Stunden	24 Stunden

(3) Die Wiederherstellung kann durch eine dauerhafte Fehlerbehebung oder durch einen zumutbaren Workaround erfolgen.

(4) Die vereinbarten Zeiten stellen Zielwerte dar und gelten vorbehaltlich der Mitwirkungspflichten des Kunden.

(5) Zeiten, in denen der Anbieter aufgrund fehlender Mitwirkung des Kunden, fehlender Informationen oder fehlender Zugänge nicht tätig werden kann, werden bei der Berechnung der Reaktions- und Wiederherstellungszeiten nicht berücksichtigt.

(6) Die Vergütung der jeweiligen SLA-Level ergibt sich aus dem Angebot, der Preisübersicht oder einer gesonderten Vereinbarung.

© by MP-BOS GmbH

(7) Der SLA-Level Basic ist Bestandteil jedes Vertrages.

(8) Die SLA-Level Standard und Professional können als kostenpflichtige Zusatzleistungen vereinbart werden.

§ 9 Datensicherung und Wiederherstellung

(1) Der Anbieter führt regelmäßige Datensicherungen der Produktivumgebung von BOS-ID durch.

(2) Die Datensicherung erfolgt grundsätzlich täglich.

(3) Der Anbieter bewahrt Datensicherungen für einen Zeitraum von dreißig (30) Kalendertagen auf, soweit keine gesetzlichen, technischen oder sicherheitsrelevanten Gründe eine abweichende Aufbewahrung erfordern.

(4) Die Datensicherungsstrategie gilt grundsätzlich unabhängig vom jeweils gebuchten SLA-Level.

(5) Datensicherungen dienen der Wiederherstellung von Systemen, Datenbeständen und Betriebsumgebungen im Rahmen der Notfallvorsorge und Betriebssicherheit.

(6) Ein Anspruch des Kunden auf die Wiederherstellung einzelner Datensätze, Dokumente, Dateien, Objekte oder sonstiger Einzelinformationen besteht nicht.

(7) Soweit technisch möglich und wirtschaftlich vertretbar, kann der Anbieter Wiederherstellungen einzelner Datenbestände als gesonderte kostenpflichtige Leistung durchführen.

(8) Wiederherstellungen aus Datensicherungen, die nicht auf einem vom Anbieter zu vertretenden Fehler beruhen, gelten als gesonderte kostenpflichtige Leistungen.

(9) Der Anbieter entscheidet nach pflichtgemäßem Ermessen über Art, Umfang und technische Durchführung von Wiederherstellungsmaßnahmen.

(10) Die Durchführung von Datensicherungen begründet keine Garantie für die vollständige Wiederherstellbarkeit sämtlicher Daten in jedem Einzelfall.

(11) Der Kunde bleibt unabhängig von den Datensicherungsmaßnahmen des Anbieters für die Einhaltung eigener gesetzlicher Aufbewahrungs-, Dokumentations- und Nachweispflichten verantwortlich.

(12) Weitergehende Regelungen zur Datenherausgabe, Archivierung und Datenlöschung ergeben sich aus den AGB, der Leistungsbeschreibung, sowie dem Auftragsverarbeitungsvertrag.

§ 10 Monitoring und Incident Management

(1) Der Anbieter betreibt für BOS-ID technische Überwachungs- und Monitoringverfahren zur Sicherstellung von Verfügbarkeit, Stabilität, Sicherheit und Leistungsfähigkeit der Plattform.

(2) Die technische Überwachung der Produktivumgebung erfolgt grundsätzlich rund um die Uhr (24 Stunden täglich an sieben Tagen pro Woche).

(3) Der Anbieter ist berechtigt, automatisierte Monitoring-, Analyse-, Alarmierungs- und Auswertungsverfahren einzusetzen.

(4) Das Monitoring kann insbesondere der Erkennung von Systemstörungen, Performanceproblemen, Sicherheitsereignissen, Infrastrukturstörungen, Kapazitätsengpässen, Integritätsverletzungen oder sonstigen Betriebsrisiken dienen.

(5) Der Anbieter betreibt ein dokumentiertes Incident-Management-Verfahren zur Erkennung, Bewertung, Bearbeitung und Nachverfolgung von Störungen und Betriebsereignissen.

(6) Störungen und Incidents werden entsprechend ihrer Auswirkungen auf Betrieb, Sicherheit und Nutzbarkeit klassifiziert und priorisiert.

(7) Der Anbieter ist berechtigt, angemessene technische und organisatorische Maßnahmen zur Eingrenzung, Behebung oder Vermeidung von Incidents zu ergreifen.

© by MP-BOS GmbH

(8) Der Kunde wird den Anbieter bei der Analyse und Bearbeitung von Incidents angemessen unterstützen und die hierfür erforderlichen Informationen bereitstellen.

(9) Maßnahmen des Incident Managements können vorübergehende Einschränkungen einzelner Funktionen oder Systeme umfassen, soweit dies zur Aufrechterhaltung von Sicherheit, Stabilität oder Integrität erforderlich ist.

(10) Weitergehende Regelungen zu Sicherheitsvorfällen ergeben sich aus §11 dieses SLA.

§ 11 Sicherheitsvorfälle

(1) Sicherheitsvorfälle werden im Rahmen des Informationssicherheitsmanagementsystems des Anbieters nach dokumentierten Verfahren behandelt.

(2) Als Sicherheitsvorfälle gelten insbesondere Ereignisse, die geeignet sind, die Vertraulichkeit, Integrität, Verfügbarkeit oder Authentizität von Informationen, Systemen oder Diensten zu beeinträchtigen.

(3) Hierzu können insbesondere unbefugte Zugriffsversuche, Sicherheitsverletzungen, Schadsoftware-Ereignisse, Angriffe auf Systeme oder Infrastruktur, Datenverlustereignisse, Sicherheitslücken oder sonstige informationssicherheitsrelevante Vorfälle gehören.

(4) Der Anbieter ist berechtigt, zur Abwehr oder Eindämmung von Sicherheitsvorfällen unverzüglich angemessene technische und organisatorische Maßnahmen zu ergreifen.

(5) Solche Maßnahmen können insbesondere die Einschränkung von Funktionen, Benutzerkonten, Schnittstellen, Integrationen oder Systemzugängen umfassen.

(6) Der Kunde ist verpflichtet, dem Anbieter bekannt gewordene sicherheitsrelevante Ereignisse unverzüglich mitzuteilen.

(7) Der Kunde wird den Anbieter bei der Untersuchung und Behandlung von Sicherheitsvorfällen angemessen unterstützen.

(8) Soweit gesetzlich erforderlich oder vertraglich vereinbart, informiert der Anbieter den Kunden über sicherheitsrelevante Vorfälle im Zusammenhang mit dessen Daten oder Nutzung von BOS-ID.

(9) Weitergehende Meldepflichten nach Datenschutzrecht, Informationssicherheitsrecht oder sonstigen gesetzlichen Vorschriften bleiben unberührt.

(10) Die Einzelheiten der Sicherheitsorganisation ergeben sich aus den AGB, der Informationssicherheitsrichtlinie sowie dem Informationssicherheitsmanagementsystem des Anbieters.

§ 12 SLA-Ausschlüsse

(1) Die in diesem SLA vereinbarten Verfügbarkeits-, Reaktions-, Wiederherstellungs- und Serviceleistungen gelten ausschließlich für Umstände innerhalb des Verantwortungsbereichs des Anbieters.

(2) Bei Ereignissen außerhalb des Verantwortungsbereichs des Anbieters ruhen die SLA-Verpflichtungen für die Dauer der jeweiligen Beeinträchtigung.

(3) Nicht als SLA-relevante Störungen oder Nichtverfügbarkeiten gelten insbesondere:

- Ereignisse höherer Gewalt
- Naturereignisse
- behördliche Maßnahmen
- Krieg, Terrorismus, Sabotage oder vergleichbare Ereignisse
- Ausfälle von Telekommunikations- oder Internetdiensten außerhalb des Verantwortungsbereichs des Anbieters
- Störungen der technischen Infrastruktur des Kunden
- Störungen von Endgeräten, Netzwerken oder Systemen des Kunden
- Fehlkonfigurationen oder Fehlbedienungen durch den Kunden oder dessen Benutzer
- Verstöße des Kunden gegen techn. Voraussetzungen, Sicherheitsanforderungen oder Nutzungsvorgaben
- Störungen durch Drittsoftware, Drittanbieter oder Fremdsysteme außerhalb des Verantwortungsbereichs des Anbieters
- Browser-, Betriebssystem- oder Geräteprobleme auf Kundenseite

© by MP-BOS GmbH

- Sicherheitsmaßnahmen, die zur Abwehr akuter Gefahren oder Sicherheitsrisiken erforderlich sind
- angekündigte Wartungsarbeiten
- Notfallwartungen
- geplante Updates, Upgrades oder Systemänderungen
- Verzögerungen aufgrund fehlender Mitwirkung des Kunden
- unvollständige oder fehlerhafte Störungsmeldungen
- fehlende Zugänge, Informationen oder Freigaben, die zur Fehleranalyse oder Fehlerbehebung erforderlich sind

(4) Zeiten, in denen der Anbieter aufgrund der in Absatz 3 genannten Umstände an der Leistungserbringung gehindert ist, werden bei der Berechnung von Verfügbarkeiten, Reaktionszeiten und Wiederherstellungszeiten nicht berücksichtigt.

(5) Die Beweislast für das Vorliegen eines SLA-relevanten Verstoßes trägt der Kunde.

(6) Weitergehende Haftungs- oder Schadensersatzansprüche richten sich ausschließlich nach den vertraglich vereinbarten Haftungsregelungen.

§ 13 Reporting und Nachweise

(1) Der Anbieter ist nicht verpflichtet, regelmäßige SLA-, Verfügbarkeits-, Monitoring- oder Leistungsberichte bereitzustellen, soweit nicht ausdrücklich etwas anderes vereinbart wurde.

(2) Ein Anspruch auf die Bereitstellung von Verfügbarkeits-, Monitoring- oder Leistungsnachweisen besteht ausschließlich, soweit dies individuell vertraglich vereinbart wurde.

(3) Soweit entsprechende Nachweise bereitgestellt werden, erfolgen diese auf Grundlage der vom Anbieter eingesetzten Monitoring-, Protokollierungs- und Auswertungssysteme.

(4) Maßgeblich für die Bewertung von Verfügbarkeiten, Störungen, Reaktionszeiten und Wiederherstellungszeiten sind grundsätzlich die durch den Anbieter erhobenen Mess- und Protokolldaten.

(5) Der Anbieter ist berechtigt, Form, Umfang, Inhalt und Bereitstellungsweg von Reports und Nachweisen festzulegen, soweit keine abweichende Vereinbarung besteht.

§ 14 Schlussbestimmungen

(1) Soweit Widersprüche zwischen diesem SLA und individuellen Vereinbarungen bestehen, gehen die individuellen Vereinbarungen vor.

(2) Die in diesem SLA beschriebenen Verfügbarkeiten, Reaktionszeiten, Wiederherstellungszeiten und sonstigen Servicewerte stellen Leistungsziele des Anbieters dar.

(3) Soweit gesetzlich zulässig und nicht ausdrücklich anders vereinbart, begründen die in diesem SLA genannten Werte keine selbstständigen Garantien, Beschaffenheitsvereinbarungen oder verschuldensunabhängigen Leistungspflichten.

(4) Weitergehende Ansprüche des Kunden richten sich ausschließlich nach den vertraglich vereinbarten Haftungsregelungen.

(5) Im Übrigen gelten die Regelungen der AGB und der Leistungsbeschreibung in ihrer jeweils vereinbarten Fassung.

© by MP-BOS GmbH

■ Anlage 3

Auftragsverarbeitungsvertrag (AVV)

§ 1 Gegenstand und Geltungsbereich

(1) Dieser Auftragsverarbeitungsvertrag („AVV") konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Vertragsparteien im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Verantwortlichen.

(2) Der Auftragnehmer erbringt seine Leistungen im Zusammenhang mit der SaaS-Plattform BOS-ID und verarbeitet hierbei personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Verantwortlichen im Sinne von Art. 28 DSGVO.

(3) Dieser AVV ist Bestandteil des zwischen den Vertragsparteien geschlossenen Hauptvertrages über die Nutzung von BOS-ID.

(4) Der Auftragnehmer hat seinen Sitz in der Bundesrepublik Deutschland.

(5) Die Verarbeitung personenbezogener Daten erfolgt ausschließlich innerhalb der Europäischen Union (EU) beziehungsweise des Europäischen Wirtschaftsraums (EWR), soweit nicht ausdrücklich etwas anderes vereinbart oder gesetzlich vorgeschrieben ist.

(6) Die Regelungen dieses AVV gelten für sämtliche Tätigkeiten, bei denen Beschäftigte, Beauftragte oder Unterauftragnehmer des Auftragnehmers personenbezogene Daten des Verantwortlichen verarbeiten.

(7) Soweit in diesem AVV keine abweichenden Regelungen getroffen werden, gelten die Bestimmungen der DSGVO, des BDSG sowie sonstiger anwendbarer Datenschutzvorschriften.

§ 2 Art und Zweck der Verarbeitung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen im Zusammenhang mit der SaaS-Plattform BOS-ID.

(2) Die Verarbeitung erfolgt insbesondere zur Bereitstellung, Nutzung, Wartung, Administration, Unterstützung, Sicherung, Fehleranalyse und technischen Weiterentwicklung der Plattform, soweit hierfür eine Verarbeitung personenbezogener Daten erforderlich ist.

(3) Die Verarbeitung kann insbesondere folgende Zwecke umfassen:
- Ausweisverwaltung
- Verwaltung von Organisationseinheiten
- Adress- und Kontaktdatenverwaltung
- Dokumenten- und Nachweisverwaltung
- Kommunikations- und Benachrichtigungsprozesse
- Verwaltung von Berechtigungen, Rollen und Benutzerkonten
- Protokollierung und Nachvollziehbarkeit von Systemvorgängen
- sonstige organisatorische und administrative Prozesse des Verantwortlichen

(4) Die konkrete Verarbeitung richtet sich nach den vom Verantwortlichen genutzten Modulen, Funktionen und Konfigurationen von BOS-ID.

(5) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der dokumentierten Weisungen des Verantwortlichen.

(6) Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers erfolgt nicht, soweit dies nicht aufgrund gesetzlicher Verpflichtungen zulässig oder erforderlich ist.

§ 3 Kategorien betroffener Personen

(1) Von der Auftragsverarbeitung können insbesondere folgende Kategorien betroffener Personen erfasst sein:
- Ausweisinhaber
- Benutzer der Plattform
- Ansprechpartner

© by MP-BOS GmbH

- Rechnungsempfänger
- sonstige Personen, deren Daten durch den Verantwortlichen im Rahmen der Nutzung von BOS-ID verarbeitet werden.

(2) Die tatsächlich betroffenen Personengruppen richten sich nach den vom Verantwortlichen genutzten Modulen, Funktionen, Organisationsstrukturen und Verarbeitungszwecken.

(3) Der Verantwortliche ist dafür verantwortlich, dass die Verarbeitung der jeweiligen personenbezogenen Daten auf einer geeigneten datenschutzrechtlichen Rechtsgrundlage beruht.

(4) Der Auftragnehmer übernimmt keine Prüfung der datenschutzrechtlichen Zulässigkeit der durch den Verantwortlichen veranlassten Verarbeitungsvorgänge, soweit hierzu keine gesetzliche Verpflichtung besteht.

§ 4 Arten personenbezogener Daten

(1) Im Rahmen der Nutzung von BOS-ID können insbesondere folgende Arten personenbezogener Daten verarbeitet werden:
- Namen
- Kontaktdaten
- Kommunikationsdaten
- Organisations- und Funktionsdaten
- Dokumente, Nachweise und Bescheinigungen
- Benutzer-, Rollen- und Berechtigungsdaten
- Authentifizierungsdaten
- Protokoll-, Audit- und Logdaten
- Bilddaten und Fotos

(2) Die tatsächlich verarbeiteten Datenarten richten sich nach den vom Verantwortlichen genutzten Modulen, Funktionen, Organisationsstrukturen und Verarbeitungszwecken.

(3) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO richtet sich ergänzend nach § 5 dieses Auftragsverarbeitungsvertrages.

(4) Der Verantwortliche entscheidet über Art, Umfang, Inhalt und Zweck der im Rahmen der Nutzung von BOS-ID verarbeiteten personenbezogenen Daten.

(5) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der vertraglich vereinbarten Leistungen sowie der dokumentierten Weisungen des Verantwortlichen.

§ 5 Besondere Kategorien personenbezogener Daten

(1) Soweit der Verantwortliche dies veranlasst, kann die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO Gegenstand der Auftragsverarbeitung sein.

(2) Hierzu können insbesondere gehören:
- gesundheitliche Eignungs- und Tauglichkeitsnachweise
- gesundheitsbezogene Qualifikationen und Befähigungen
- sonstige gesundheitsbezogene Angaben, die durch den Verantwortlichen im Rahmen der Nutzung von BOS-ID verarbeitet werden

(3) Der Verantwortliche ist allein dafür verantwortlich, dass für die Verarbeitung besonderer Kategorien personenbezogener Daten eine geeignete Rechtsgrundlage nach Art. 9 DSGVO sowie gegebenenfalls weiteren anwendbaren Datenschutzvorschriften besteht.

(4) Der Auftragnehmer verarbeitet besondere Kategorien personenbezogener Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen und im Rahmen der vertraglich vereinbarten Leistungen.

(5) Der Auftragnehmer trifft für die Verarbeitung besonderer Kategorien personenbezogener Daten angemessene technische und organisatorische Maßnahmen unter Berücksichtigung des Risikos für die Rechte und Freiheiten der betroffenen Personen.

© by MP-BOS GmbH

(6) Die Verarbeitung besonderer Kategorien personenbezogener Daten erfolgt unter Berücksichtigung erhöhter Anforderungen an Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der eingesetzten Systeme und Prozesse.

(7) Die technischen und organisatorischen Maßnahmen orientieren sich insbesondere an den Anforderungen der DSGVO, den anerkannten Standards der Informationssicherheit sowie dem durch den Auftragnehmer betriebenen Informationssicherheitsmanagementsystem.

(8) Der Auftragnehmer unterhält ein Informationssicherheitsmanagementsystem auf Grundlage der ISO/IEC 27001 oder eines gleichwertigen anerkannten Standards.

(9) Die Einzelheiten der technischen und organisatorischen Maßnahmen ergeben sich aus der Anlage „Technische und organisatorische Maßnahmen (TOMs)", die Bestandteil dieses Auftragsverarbeitungsvertrages ist.

(10) Die Verarbeitung besonderer Kategorien personenbezogener Daten erfolgt ausschließlich innerhalb der Europäischen Union (EU) beziehungsweise des Europäischen Wirtschaftsraums (EWR), soweit keine gesetzliche Verpflichtung oder ausdrückliche schriftliche Vereinbarung etwas anderes vorsieht.

§ 6 Weisungsrecht des Verantwortlichen

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf Grundlage der dokumentierten Weisungen des Verantwortlichen, soweit nicht eine gesetzliche Verpflichtung zur Verarbeitung besteht.

(2) Weisungen des Verantwortlichen sind grundsätzlich in Textform zu erteilen. Die Textform umfasst insbesondere E-Mail, Kundenportal, Ticketsystem oder vergleichbare elektronische Kommunikationswege.

(3) Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(4) Der Auftragnehmer wird den Verantwortlichen unverzüglich informieren, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften, sonstige gesetzliche Bestimmungen oder die Regelungen dieses Auftragsverarbeitungsvertrages verstößt.

(5) In diesem Fall ist der Auftragnehmer berechtigt, die Durchführung der betreffenden Weisung bis zur Bestätigung oder Anpassung durch den Verantwortlichen auszusetzen.

(6) Der Auftragnehmer ist nicht verpflichtet, Weisungen umzusetzen, die offensichtlich rechtswidrig sind oder gegen zwingende gesetzliche Vorschriften verstoßen.

(7) Der Verantwortliche ist berechtigt, im Rahmen dieses Auftragsverarbeitungsvertrages Weisungen hinsichtlich Art, Umfang, Verfahren und Zweck der Datenverarbeitung zu erteilen.

(8) Im Rahmen der SaaS-Leistung erfolgt die Datenverarbeitung im Wesentlichen automatisiert innerhalb der vom Auftragnehmer bereitgestellten Plattform BOS-ID und der BOS-ID App. Weisungen des Verantwortlichen werden daher regelmäßig durch die Nutzung der bereitgestellten Funktionen, Konfigurationen und Einstellungen innerhalb der Plattform umgesetzt.

(9) Individuelle Weisungen außerhalb der standardisierten Funktionen der SaaS-Plattform sind nur insoweit zulässig, als sie technisch umsetzbar sind und den sicheren, stabilen und mandantenfähigen Betrieb der Plattform nicht beeinträchtigen.

(10) Weisungen, die den vertraglich vereinbarten Leistungsumfang, die bereitgestellten Funktionen oder die vereinbarten technischen Rahmenbedingungen überschreiten, gelten als zusätzliche Leistungen. Dies gilt insbesondere für individuelle Auswertungen, Sonderentwicklungen, manuelle Datenmigrationen oder sonstige Leistungen außerhalb des vereinbarten Funktionsumfangs.

(11) Soweit die Umsetzung solcher Weisungen zusätzlichen Aufwand verursacht, kann der Auftragnehmer hierfür eine gesonderte Vergütung verlangen.

(12) Der Auftragnehmer dokumentiert Weisungen des Verantwortlichen sowie deren Umsetzung in angemessenem Umfang.

© by MP-BOS GmbH

(13) Gesetzliche Pflichten des Auftragnehmers zur Verarbeitung personenbezogener Daten bleiben unberührt. In solchen Fällen wird der Auftragnehmer den Verantwortlichen vor der Verarbeitung informieren, soweit dies gesetzlich zulässig ist.

§ 7 Vertraulichkeit und Verpflichtung der Beschäftigten

(1) Der Auftragnehmer stellt sicher, dass alle Personen, die Zugang zu personenbezogenen Daten des Verantwortlichen erhalten oder an deren Verarbeitung beteiligt sind, zur Vertraulichkeit verpflichtet werden.

(2) Dies gilt insbesondere für Beschäftigte, freie Mitarbeiter, Berater, Leiharbeitnehmer, Unterauftragnehmer sowie sonstige Personen, die im Auftrag des Auftragnehmers personenbezogene Daten verarbeiten.

(3) Die Verpflichtung zur Vertraulichkeit erfolgt vor Aufnahme der jeweiligen Tätigkeit und besteht auch nach deren Beendigung fort.

(4) Der Auftragnehmer stellt sicher, dass die zur Verarbeitung personenbezogener Daten befugten Personen ausschließlich auf Weisung handeln, soweit keine gesetzliche Verpflichtung zur Verarbeitung besteht.

(5) Zugriffe auf personenbezogene Daten werden nach dem Need-to-Know-Prinzip sowie dem Prinzip der minimal erforderlichen Berechtigung vergeben.

(6) Der Zugriff auf personenbezogene Daten wird auf diejenigen Personen beschränkt, die diesen Zugriff zur Erfüllung ihrer jeweiligen Aufgaben benötigen.

(7) Der Auftragnehmer unterhält organisatorische Regelungen, Prozesse und Richtlinien zur Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen.

(8) Der Auftragnehmer betreibt ein Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001 oder einem gleichwertigen anerkannten Standard.

(9) Die Beschäftigten und sonstigen berechtigten Personen werden regelmäßig zu Datenschutz, Informationssicherheit, Vertraulichkeit und den einschlägigen Sicherheitsanforderungen geschult und sensibilisiert.

(10) Der Auftragnehmer dokumentiert die Verpflichtung zur Vertraulichkeit sowie die Durchführung geeigneter Sensibilisierungs- und Schulungsmaßnahmen in angemessenem Umfang.

(11) Weitergehende Verpflichtungen zur Vertraulichkeit, Geheimhaltung oder Informationssicherheit aus gesetzlichen Vorschriften, vertraglichen Vereinbarungen oder internen Richtlinien des Auftragnehmers bleiben unberührt.

§ 8 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau für die Verarbeitung personenbezogener Daten sicherzustellen.

(2) Die technischen und organisatorischen Maßnahmen berücksichtigen insbesondere den Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schweregrade möglicher Risiken für die Rechte und Freiheiten natürlicher Personen.

(3) Die Einzelheiten der technischen und organisatorischen Maßnahmen ergeben sich aus der Anlage 3a „Technische und organisatorische Maßnahmen (TOMs)", die Bestandteil dieses Auftragsverarbeitungsvertrages ist.

(4) Die technischen und organisatorischen Maßnahmen umfassen insbesondere Regelungen zu:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Verfügbarkeitskontrolle
- Wiederherstellbarkeit
- Belastbarkeit der Systeme
- Berechtigungskonzepten

© by MP-BOS GmbH

- Verschlüsselung
- Datensicherung
- Protokollierung und Nachvollziehbarkeit
- Informationssicherheit und Risikomanagement

(5) Der Auftragnehmer betreibt ein Informationssicherheitsmanagementsystem auf Grundlage der ISO/IEC 27001 oder eines gleichwertigen anerkannten Standards.

(6) Der Auftragnehmer ist berechtigt, technische und organisatorische Maßnahmen fortlaufend weiterzuentwickeln, anzupassen oder zu ersetzen.

(7) Voraussetzung für Änderungen gemäß Absatz 6 ist, dass das insgesamt gewährleistete Schutzniveau nicht abgesenkt wird.

(8) Wesentliche Änderungen der technischen und organisatorischen Maßnahmen werden in geeigneter Weise dokumentiert.

(9) Der Verantwortliche erkennt an, dass technische und organisatorische Maßnahmen aufgrund technischer, organisatorischer oder regulatorischer Entwicklungen laufend angepasst werden können und müssen.

(10) Weitergehende Anforderungen können sich aus gesetzlichen Vorschriften, behördlichen Anforderungen, Zertifizierungen oder vereinbarten Sicherheitsrichtlinien ergeben.

§ 9 Unterstützungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Verantwortlichen im Rahmen der gesetzlichen Anforderungen und unter Berücksichtigung der Art der Verarbeitung durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung seiner datenschutzrechtlichen Pflichten.

(2) Der Auftragnehmer unterstützt den Verantwortlichen insbesondere bei der Bearbeitung von Anträgen betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch, soweit dies im Rahmen der durch den Auftragnehmer erbrachten Leistungen erforderlich ist.

(3) Soweit Anfragen betroffener Personen unmittelbar beim Auftragnehmer eingehen, wird dieser die Anfrage unverzüglich an den Verantwortlichen weiterleiten, sofern eine Zuordnung möglich ist.

(4) Der Auftragnehmer wird betroffene Personen grundsätzlich nicht ohne Weisung des Verantwortlichen unmittelbar beantworten, soweit keine gesetzliche Verpflichtung hierzu besteht.

(5) Der Auftragnehmer unterstützt den Verantwortlichen bei behördlichen Anfragen, Prüfungen oder Verfahren, soweit diese die im Auftrag verarbeiteten personenbezogenen Daten betreffen und die Unterstützung gesetzlich erforderlich oder vertraglich vereinbart ist.

(6) Die Unterstützungspflichten des Auftragnehmers beschränken sich auf Informationen und Maßnahmen, die ihm im Rahmen seiner Rolle als Auftragsverarbeiter tatsächlich möglich und zumutbar sind.

(7) Der Auftragnehmer schuldet keine rechtliche Beratung, Datenschutzberatung, Compliance-Beratung oder sonstige rechtliche Bewertung datenschutzrechtlicher Fragestellungen.

(8) Unterstützungsleistungen, die über den gewöhnlichen und vertraglich geschuldeten Umfang hinausgehen, können gesondert vergütet werden.

(9) Dies gilt insbesondere für außergewöhnliche Auswertungen, Sonderberichte, umfangreiche Prüfungsunterstützungen, individuelle Dokumentationen oder sonstige Leistungen mit erheblichem Zusatzaufwand.

(10) Weitergehende gesetzliche Unterstützungspflichten des Auftragnehmers nach Art. 28 DSGVO bleiben unberührt.

§ 10 Meldung von Datenschutzverletzungen

(1) Der Auftragnehmer informiert den Verantwortlichen unverzüglich über ihm bekannt gewordene Verletzungen des Schutzes personenbezogener Daten im Zusammenhang mit den im Auftrag verarbeiteten personenbezogenen Daten, soweit diese Verletzungen dem Verantwortlichen nicht bereits bekannt sind.

© by MP-BOS GmbH

(2) Die Information erfolgt grundsätzlich innerhalb von 48 Stunden nach Bekanntwerden des jeweiligen Vorfalls beim Auftragnehmer, soweit eine entsprechende Bewertung innerhalb dieses Zeitraums möglich ist.

(3) Die Meldung erfolgt mindestens in Textform.

(4) Die Mitteilung enthält, soweit zum Zeitpunkt der Meldung bekannt und mit angemessenem Aufwand feststellbar, insbesondere:

- eine Beschreibung der Art der Datenschutzverletzung
- die betroffenen Datenkategorien
- die betroffenen Personengruppen
- die bekannten oder vermuteten Auswirkungen
- die bereits ergriffenen oder geplanten Gegenmaßnahmen

(5) Soweit zum Zeitpunkt der Erstmeldung noch nicht alle Informationen vorliegen, werden diese nach Verfügbarkeit und im Rahmen der technischen und organisatorischen Möglichkeiten schrittweise ergänzt.

(6) Der Auftragnehmer unterstützt den Verantwortlichen im angemessenen und zumutbaren Umfang bei der Untersuchung, Bewertung und Dokumentation der Datenschutzverletzung.

(7) Der Auftragnehmer stellt dem Verantwortlichen die ihm zur Verfügung stehenden Informationen bereit, soweit dies zur Erfüllung gesetzlicher Melde-, Informations- oder Dokumentationspflichten erforderlich ist und dem Auftragnehmer dies möglich und zumutbar ist.

(8) Meldungen an Aufsichtsbehörden oder betroffene Personen erfolgen grundsätzlich ausschließlich durch den Verantwortlichen.

(9) Der Auftragnehmer wird Meldungen an Aufsichtsbehörden oder betroffene Personen nur vornehmen, soweit eine gesetzliche Verpflichtung hierzu besteht oder der Verantwortliche den Auftragnehmer ausdrücklich hierzu angewiesen hat.

(10) Unterstützungsleistungen des Auftragnehmers, die über den üblichen und vertraglich geschuldeten Umfang hinausgehen, können gesondert vergütet werden.

(11) Weitergehende gesetzliche Pflichten der Vertragsparteien nach Art. 33 und Art. 34 DSGVO bleiben unberührt.

§ 11 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt dem Auftragnehmer die allgemeine Genehmigung zum Einsatz von Unterauftragsverarbeitern im Sinne des Art. 28 Abs. 2 DSGVO.

(2) Der Auftragnehmer ist berechtigt, zur Erbringung der vertraglich vereinbarten Leistungen weitere Auftragsverarbeiter oder sonstige Unterauftragnehmer einzusetzen.

(3) Der Auftragnehmer führt eine aktuelle Liste der eingesetzten Unterauftragsverarbeiter.

(4) Die Liste der Unterauftragsverarbeiter wird dem Verantwortlichen auf Anfrage in geeigneter Form zur Verfügung gestellt.

(5) Beabsichtigt der Auftragnehmer die Beauftragung eines neuen Unterauftragsverarbeiters oder eine wesentliche Änderung bestehender Unterauftragsverhältnisse, wird der Verantwortliche hierüber rechtzeitig vor Wirksamwerden informiert.

(6) Der Verantwortliche kann der Beauftragung eines neuen Unterauftragsverarbeiters innerhalb der Mitteilungsfrist aus wichtigem datenschutzrechtlichem Grund widersprechen.

(7) Ein wichtiger Grund liegt insbesondere vor, wenn konkrete Tatsachen die Annahme rechtfertigen, dass der Einsatz des vorgesehenen Unterauftragsverarbeiters gegen datenschutzrechtliche Anforderungen verstößt oder die Rechte und Freiheiten betroffener Personen erheblich gefährdet.

(8) Im Falle eines Widerspruchs werden die Vertragsparteien zunächst versuchen, eine einvernehmliche Lösung zu finden.

© by MP-BOS GmbH

(9) Kann innerhalb angemessener Zeit keine einvernehmliche Lösung erzielt werden, ist jede Vertragspartei berechtigt, die betroffenen Leistungen oder – soweit erforderlich – den Vertrag außerordentlich zu kündigen.

(10) Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich mindestens zu den Datenschutzpflichten, die sich aus diesem Auftragsverarbeitungsvertrag ergeben.

(11) Der Auftragnehmer bleibt gegenüber dem Verantwortlichen für die ordnungsgemäße Erfüllung der Datenschutzpflichten durch eingesetzte Unterauftragsverarbeiter verantwortlich.

(12) Die Verarbeitung personenbezogener Daten durch Unterauftragsverarbeiter erfolgt grundsätzlich innerhalb der Europäischen Union (EU) beziehungsweise des Europäischen Wirtschaftsraums (EWR), soweit keine abweichende zulässige Vereinbarung getroffen wird oder eine gesetzliche Verpflichtung besteht.

§ 12 Drittlandverarbeitung

(1) Die Verarbeitung personenbezogener Daten erfolgt grundsätzlich ausschließlich innerhalb der Europäischen Union (EU) beziehungsweise des Europäischen Wirtschaftsraums (EWR).

(2) Eine Übermittlung personenbezogener Daten in Staaten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums (Drittländer) erfolgt grundsätzlich nicht.

(3) Abweichend von Absatz 2 ist eine Drittlandübermittlung nur zulässig, soweit eine gesetzliche Verpflichtung hierzu besteht, soweit der Verantwortliche dies ausdrücklich angewiesen oder genehmigt hat oder soweit die Voraussetzungen der DSGVO für eine zulässige Drittlandübermittlung erfüllt sind.

(4) Der Auftragnehmer wird vor einer Drittlandübermittlung sicherstellen, dass ein angemessenes Datenschutzniveau gemäß den Anforderungen der DSGVO gewährleistet ist.

(5) Hierzu können insbesondere folgende geeignete Garantien herangezogen werden:
- Angemessenheitsbeschlüsse der Europäischen Kommission
- Standardvertragsklauseln der Europäischen Kommission
- verbindliche interne Datenschutzvorschriften (Binding Corporate Rules)
- sonstige nach der DSGVO zulässige Übermittlungsinstrumente

(6) Der Auftragnehmer wird den Verantwortlichen auf Anfrage über die wesentlichen datenschutzrechtlichen Grundlagen einer zulässigen Drittlandübermittlung informieren.

(7) Weitergehende Anforderungen der DSGVO sowie behördliche Vorgaben zur Drittlandübermittlung bleiben unberührt.

§ 13 Kontrollrechte und Nachweise

(1) Der Auftragnehmer weist die Einhaltung seiner datenschutzrechtlichen und informationssicherheitsbezogenen Verpflichtungen durch geeignete Nachweise nach.

(2) Der Verantwortliche erkennt an, dass Zertifizierungen, Prüfberichte, Auditnachweise, Informationssicherheitsnachweise sowie vergleichbare Dokumentationen geeignete Nachweise im Sinne des Art. 28 DSGVO darstellen können.

(3) Der Auftragnehmer unterhält ein Informationssicherheitsmanagementsystem nach ISO/IEC 27001 oder einem gleichwertigen anerkannten Standard.

(4) Die Vorlage gültiger Zertifizierungen, Prüfberichte, Auditnachweise, Selbstauskünfte oder vergleichbarer Dokumentationen gilt grundsätzlich als geeigneter Nachweis für die Erfüllung wesentlicher Kontroll- und Nachweispflichten des Auftragnehmers.

(5) Vor der Durchführung eines Audits wird der Verantwortliche zunächst die ihm zur Verfügung gestellten Nachweise, Zertifizierungen, Berichte und Dokumentationen prüfen.

(6) Weitergehende Kontrollen oder Audits sind nur zulässig, soweit die bereitgestellten Nachweise zur Erfüllung der gesetzlichen Kontrollpflichten des Verantwortlichen im Einzelfall nicht ausreichend sind.

(7) Vor-Ort-Audits beim Auftragnehmer sind nur bei berechtigtem Anlass zulässig.

© by MP-BOS GmbH

(8) Audits sind mindestens vier (4) Wochen vor dem geplanten Termin schriftlich anzukündigen.

(9) Audits dürfen ausschließlich während der üblichen Geschäftszeiten des Auftragnehmers durchgeführt werden.

(10) Der Verantwortliche trägt sämtliche ihm entstehenden Kosten, sowie die angemessenen internen Aufwendungen des Auftragnehmers im Zusammenhang mit der Durchführung eines Audits.

(11) Der Auftragnehmer ist berechtigt, Audits auf einen angemessenen Umfang zu beschränken, soweit dies zur Wahrung von Betriebs- und Geschäftsgeheimnissen, Informationssicherheitsinteressen oder datenschutzrechtlichen Verpflichtungen gegenüber anderen Kunden erforderlich ist.

(12) Der Auftragnehmer kann die Durchführung eines Audits ablehnen oder einschränken, soweit hierdurch Sicherheitsinteressen, Vertraulichkeitsverpflichtungen oder die Rechte anderer Kunden beeinträchtigt würden.

(13) Der Verantwortliche ist verpflichtet, sämtliche im Rahmen von Audits erlangten Informationen vertraulich zu behandeln.

(14) Gesetzliche Kontrollrechte der Datenschutzaufsichtsbehörden bleiben unberührt.

§ 14 Löschung und Rückgabe von Daten

(1) Nach Beendigung des Hauptvertrages richtet sich die Rückgabe und Löschung personenbezogener Daten nach den Regelungen der AGB, sowie den Bestimmungen dieses Auftragsverarbeitungsvertrages.

(2) Der Auftragnehmer stellt dem Verantwortlichen die von diesem verarbeiteten Daten innerhalb der vertraglich vereinbarten Exportfrist zur Verfügung.

(3) Die Bereitstellung erfolgt grundsätzlich in Form eines standardisierten SQL-Datenbankexports oder eines vergleichbaren vom Auftragnehmer unterstützten Standardformats.

(4) Ein Anspruch auf die Bereitstellung individueller Exportformate, Datenmigrationen, Datenkonvertierungen oder sonstiger Sonderleistungen besteht nicht.

(5) Nach Ablauf der vertraglich vereinbarten Exportfrist ist der Auftragnehmer berechtigt, die personenbezogenen Daten des Verantwortlichen sowie vorhandene Kopien zu löschen oder zu anonymisieren, soweit keine gesetzlichen Aufbewahrungspflichten oder sonstigen gesetzlichen Verpflichtungen entgegenstehen.

(6) Gesetzliche Aufbewahrungs-, Nachweis- oder Dokumentationspflichten des Auftragnehmers bleiben unberührt.

(7) Soweit personenbezogene Daten aufgrund gesetzlicher Verpflichtungen weiterhin aufbewahrt werden müssen, wird deren Verarbeitung auf den jeweiligen gesetzlichen Zweck beschränkt.

(8) Nach Durchführung der Löschung kann der Verantwortliche keine Wiederherstellung, erneute Bereitstellung oder Herausgabe der betroffenen Daten verlangen.

(9) Weitergehende Regelungen zur Datenherausgabe, Exportfrist und Datenlöschung ergeben sich aus den AGB.

§ 14 Löschung und Rückgabe von Daten

(1) Nach Beendigung des Hauptvertrages richtet sich die Rückgabe und Löschung personenbezogener Daten nach den Regelungen der AGB sowie den Bestimmungen dieses Auftragsverarbeitungsvertrages.

(2) Der Auftragnehmer stellt dem Verantwortlichen die von diesem verarbeiteten Daten innerhalb der vertraglich vereinbarten Exportfrist in Form eines standardisierten SQL-Datenbankexports oder eines vergleichbaren unterstützten Standardformats zur Verfügung.

(3) Nach Ablauf der Exportfrist ist der Auftragnehmer berechtigt, die personenbezogenen Daten sowie vorhandene Kopien zu löschen oder zu anonymisieren, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

(4) Gesetzliche Aufbewahrungs-, Nachweis- oder Dokumentationspflichten des Auftragnehmers bleiben unberührt.

(5) Weitergehende Regelungen zur Datenherausgabe, Exportfrist und Datenlöschung ergeben sich aus den AGB.

© by MP-BOS GmbH

§ 15 Haftung

(1) Für die Haftung der Vertragsparteien gelten die Haftungsregelungen des Hauptvertrages, soweit in diesem Auftragsverarbeitungsvertrag keine abweichenden zwingenden gesetzlichen Regelungen vorgesehen sind.

(2) Die gesetzlichen Haftungsregelungen der DSGVO, insbesondere Art. 82 DSGVO, bleiben unberührt.

(3) Soweit mehrere Beteiligte für einen datenschutzrechtlichen Schaden verantwortlich sind, richtet sich die Haftung nach den gesetzlichen Bestimmungen.

(4) Der Verantwortliche stellt sicher, dass die Verarbeitung personenbezogener Daten auf einer geeigneten Rechtsgrundlage erfolgt und die datenschutzrechtlichen Informationspflichten gegenüber den betroffenen Personen erfüllt werden.

(5) Der Auftragnehmer haftet nicht für datenschutzrechtliche Verstöße, die auf Weisungen, Vorgaben, Dateninhalte oder Verarbeitungsvorgänge des Verantwortlichen zurückzuführen sind, soweit der Auftragnehmer seine gesetzlichen Prüf- und Hinweispflichten erfüllt hat.

§ 16 Laufzeit und Beendigung

(1) Dieser Auftragsverarbeitungsvertrag tritt mit Abschluss des Hauptvertrages in Kraft.

(2) Die Laufzeit dieses Auftragsverarbeitungsvertrages richtet sich nach der Laufzeit des jeweiligen Hauptvertrages.

(3) Der Auftragsverarbeitungsvertrag endet automatisch mit der Beendigung des Hauptvertrages, ohne dass es einer gesonderten Kündigung bedarf.

(4) Die Verpflichtungen des Auftragnehmers zur Löschung, Rückgabe, Vertraulichkeit und zum Datenschutz bestehen über die Beendigung dieses Auftragsverhältnisses hinaus fort, soweit gesetzliche Vorschriften dies vorsehen oder die jeweilige Verpflichtung ihrem Wesen nach fortbesteht.

(5) Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

(6) Ein wichtiger Grund liegt insbesondere vor, wenn eine Vertragspartei schwerwiegend oder dauerhaft gegen datenschutzrechtliche Verpflichtungen verstößt und eine Fortsetzung der Zusammenarbeit unzumutbar wird.

§ 17 Schlussbestimmungen

(1) Dieser Auftragsverarbeitungsvertrag ergänzt den zwischen den Vertragsparteien geschlossenen Hauptvertrag über die Nutzung von BOS-ID.

(2) Soweit in diesem Auftragsverarbeitungsvertrag keine besonderen Regelungen getroffen werden, gelten die Bestimmungen des Hauptvertrages.

(3) Bei Widersprüchen zwischen den Regelungen dieses Auftragsverarbeitungsvertrages und sonstigen vertraglichen Vereinbarungen gehen die datenschutzrechtlichen Regelungen dieses Auftragsverarbeitungsvertrages vor, soweit dies zur Einhaltung der DSGVO oder sonstiger zwingender Datenschutzvorschriften erforderlich ist.

(4) Änderungen und Ergänzungen dieses Auftragsverarbeitungsvertrages bedürfen mindestens der Textform, soweit gesetzlich keine strengere Form vorgeschrieben ist.

(5) Für diesen Auftragsverarbeitungsvertrag gilt das Recht der Bundesrepublik Deutschland unter Berücksichtigung der unmittelbar anwendbaren Bestimmungen der Datenschutz-Grundverordnung (DSGVO).

(6) Sollten einzelne Bestimmungen dieses Auftragsverarbeitungsvertrages ganz oder teilweise unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

(7) Zwingende Bestimmungen der DSGVO sowie sonstiger anwendbarer Datenschutzvorschriften gehen entgegenstehenden vertraglichen Regelungen vor.

© by MP-BOS GmbH

Anlage 3a

Technische und organisatorische Maßnahmen (TOMs)

§ 1 Zweck der technischen und organisatorischen Maßnahmen

(1) Die Maßnahmen dienen der Gewährleistung eines angemessenen Schutzniveaus hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten.

(2) Die Maßnahmen werden unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schweregrade möglicher Risiken für die Rechte und Freiheiten natürlicher Personen umgesetzt.

(3) Die jeweils aktuellen technischen und organisatorischen Maßnahmen (TOMs) gemäß Art. 32 DSGVO sind unter folgendem Link abrufbar:

www.mpbos.de/dsgvo-tom

Die dort dokumentierten Maßnahmen werden regelmäßig überprüft und bei Bedarf aktualisiert. Die jeweils aktuelle Fassung ist Bestandteil dieser Vereinbarung. Änderungen dürfen das vereinbarte Schutzniveau nicht unterschreiten.

© by MP-BOS GmbH

■ Anlage 3b

Verzeichnis der Unterauftragsverarbeiter

§ 1 Allgemeines

(1) Der Auftragnehmer ist berechtigt, zur Erbringung der vertraglich vereinbarten Leistungen Unterauftragsverarbeiter einzusetzen.

(2) Die nachfolgende Übersicht enthält die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter im Sinne des Art. 28 DSGVO.

(3) Änderungen der Unterauftragsverarbeiter richten sich nach den Regelungen des Auftragsverarbeitungsvertrages.

§ 2 Eingesetzte Unterauftragsverarbeiter

Unternehmen	**Sitz / Verarbeitungsort**	**Leistung**
Hetzner Online GmbH	Deutschland / EU	Hosting, Serverbetrieb, Infrastruktur, Datenspeicherung, Backup

© by MP-BOS GmbH

■ Anlage 4

Informationssicherheitsrichtlinie

§ 1 Zweck und Geltungsbereich

(1) Die MP-BOS GmbH verpflichtet sich zur Aufrechterhaltung eines angemessenen und wirksamen Informationssicherheitsniveaus für sämtliche Geschäftsprozesse, Informationswerte, IT-Systeme und Dienstleistungen.

(2) Diese Informationssicherheitsrichtlinie definiert die grundlegenden Sicherheitsziele, Sicherheitsprinzipien und organisatorischen Rahmenbedingungen für den Schutz von Informationen und informationsverarbeitenden Systemen.

(3) Die Richtlinie gilt für alle Beschäftigten, Führungskräfte, freien Mitarbeiter, Dienstleister, Auftragnehmer sowie sonstige Personen, die auf Informationen oder Systeme der MP-BOS GmbH zugreifen.

(4) Die Anforderungen dieser Richtlinie gelten insbesondere für die Entwicklung, Bereitstellung und den Betrieb der SaaS-Plattform BOS-ID.

§ 2 Sicherheitsziele

(1) Ziel der Informationssicherheit ist der Schutz von:
- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität
- Nachvollziehbarkeit von Informationen

(2) Die MP-BOS GmbH verfolgt das Ziel, Informationen vor unbefugtem Zugriff, Manipulation, Verlust, Offenlegung oder Zerstörung zu schützen.

(3) Informationssicherheit ist integraler Bestandteil sämtlicher Geschäfts-, Entwicklungs- und Betriebsprozesse.

§ 3 Informationssicherheitsmanagementsystem

(1) Die MP-BOS GmbH betreibt ein Informationssicherheitsmanagementsystem (ISMS).

(2) Das ISMS orientiert sich an den Anforderungen der ISO/IEC 27001 einem gleichwertigen anerkannten Standard.

(3) Die Informationssicherheit wird durch dokumentierte Prozesse, Richtlinien und Kontrollen gesteuert.

(4) Das ISMS wird regelmäßig überprüft und fortlaufend weiterentwickelt.

§ 4 Rollen und Verantwortlichkeiten

(1) Die Geschäftsleitung trägt die Gesamtverantwortung für die Informationssicherheit.

(2) Informationssicherheitsaufgaben werden organisatorisch definiert und geeigneten Verantwortlichen zugewiesen.

(3) Alle Beschäftigten sind verpflichtet, die Vorgaben zur Informationssicherheit einzuhalten.

(4) Sicherheitsvorfälle, Schwachstellen oder Sicherheitsrisiken sind unverzüglich an die zuständigen Stellen zu melden.

§ 5 Risikomanagement

(1) Informationssicherheitsrisiken werden regelmäßig identifiziert, bewertet und behandelt.

(2) Die Risikobewertung berücksichtigt insbesondere technische Risiken, organisatorische Risiken, personelle Risiken, Lieferanten- und Dienstleiterrisiken und regulatorische Risiken.

(3) Für identifizierte Risiken werden angemessene Schutzmaßnahmen festgelegt.

© by MP-BOS GmbH

§ 6 Zugriffsschutz und Berechtigungen

(1) Zugriffe auf Informationen und Systeme erfolgen ausschließlich auf Grundlage eines dokumentierten Berechtigungskonzeptes.

(2) Berechtigungen werden nach dem Need-to-Know-Prinzip vergeben.

(3) Administratorrechte werden auf das erforderliche Minimum beschränkt.

(4) Privilegierte Zugriffe werden besonders geschützt und überwacht.

(5) Mehrfaktor-Authentifizierung wird für privilegierte Zugriffe eingesetzt.

§ 7 Personal und Security Awareness

(1) Beschäftigte werden regelmäßig zu Informationssicherheit und Datenschutz geschult.

(2) Sicherheitsrelevante Sensibilisierungsmaßnahmen werden regelmäßig durchgeführt.

(3) Personen mit Zugriff auf vertrauliche Informationen werden zur Vertraulichkeit verpflichtet.

(4) Die Verpflichtung zur Vertraulichkeit besteht auch nach Beendigung der Tätigkeit fort.

§ 8 Sichere Entwicklung und Änderungsmanagement

(1) Sicherheitsanforderungen werden bereits bei der Planung, Entwicklung und Weiterentwicklung von BOS-ID berücksichtigt.

(2) Änderungen an Systemen und Anwendungen erfolgen nach definierten Prozessen.

(3) Produktiv-, Test- und Entwicklungsumgebungen werden organisatorisch und technisch getrennt betrieben.

(4) Sicherheitsrelevante Änderungen werden vor ihrer Einführung angemessen geprüft.

§ 9 Schwachstellen- und Patchmanagement

(1) Bekannte Sicherheitslücken werden risikobasiert bewertet.

(2) Sicherheitsrelevante Updates und Patches werden zeitnah eingespielt.

(3) Kritische Schwachstellen werden priorisiert behandelt.

(4) Die Wirksamkeit von Sicherheitsmaßnahmen wird regelmäßig überprüft.

§ 10 Betriebssicherheit und Monitoring

(1) Die Betriebsumgebung wird kontinuierlich überwacht.

(2) Technische Überwachungs- und Alarmierungsmechanismen dienen der frühzeitigen Erkennung von Störungen und Sicherheitsereignissen.

(3) Sicherheitsrelevante Ereignisse werden dokumentiert und ausgewertet.

(4) Protokollierungs- und Monitoringdaten werden gegen unbefugte Veränderungen geschützt.

§ 11 Incident Management

(1) Die MP-BOS GmbH unterhält dokumentierte Verfahren zur Behandlung von Sicherheitsvorfällen.

(2) Sicherheitsvorfälle werden bewertet, priorisiert, dokumentiert und nachverfolgt.

(3) Geeignete Gegenmaßnahmen werden unverzüglich eingeleitet.

(4) Sicherheitsvorfälle werden zur kontinuierlichen Verbesserung ausgewertet.

© by MP-BOS GmbH

§ 12 Lieferanten- und Dienstleistermanagement

(1) Lieferanten und Dienstleister werden risikobasiert ausgewählt und bewertet.

(2) Sicherheits- und Datenschutzanforderungen werden vertraglich geregelt.

(3) Kritische Dienstleister werden regelmäßig überprüft.

(4) Der Einsatz von Unterauftragnehmern erfolgt unter Berücksichtigung der gesetzlichen und vertraglichen Anforderungen.

§ 13 Business Continuity und Notfallmanagement

(1) Die MP-BOS GmbH unterhält Verfahren zur Sicherstellung der Geschäftskontinuität.

(2) Für wesentliche Systeme und Prozesse bestehen Notfall- und Wiederanlaufverfahren.

(3) Datensicherungen werden regelmäßig durchgeführt.

(4) Notfallmaßnahmen werden regelmäßig überprüft und weiterentwickelt.

§ 14 Cloud- und Plattform-Sicherheit

(1) BOS-ID wird in Rechenzentren innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums betrieben.

(2) Die Plattform wird durch technische und organisatorische Sicherheitsmaßnahmen geschützt.

(3) Sicherheitsmaßnahmen werden regelmäßig überprüft und angepasst.

(4) Kundendaten werden mandantengetrennt verarbeitet.

§ 15 Kontinuierliche Verbesserung

(1) Die Informationssicherheit wird fortlaufend überprüft und verbessert.

(2) Erkenntnisse aus Audits, Sicherheitsvorfällen, Risikobewertungen und Kundenanforderungen fließen in die Weiterentwicklung des Informationssicherheitsmanagementsystems ein.

(3) Die Geschäftsleitung unterstützt die kontinuierliche Verbesserung der Informationssicherheit als dauerhafte Unternehmensaufgabe.

© by MP-BOS GmbH