



Vertrag zur Auftragsverarbeitung Wartung, Services & Support

Gültig mit Anwendbarkeit der DSGVO ab 25. Mai 2018
„Vertrag über eine Auftragsverarbeitung nach Art 28 DSGVO“

abgeschlossen zwischen

MAG Mental Acrobatics Group

Richard Novy

Arsenal Objekt 16 Top 66

1030 Wien, Austria

UID ATU42898209

und

Auszufüllende Informationen bitte in BLOCKBUCHSTABEN und HANDSCHRIFTLICH

FIRMENNAME lt. Firmenbuchauszug | Markenname

Zeichnungsberechtigter des Unternehmens VORNAME

FIRMENBUCHNUMMER falls registriertes Unternehmen

Zeichnungsberechtigter des Unternehmens NACHNAME

VORNAME und NACHNAME (bei EPU, Privatperson, Juristische Person)

UID/VAT (B2B) | Geburtsdatum

ANSCHRIFT

POSTLEITZAHL

ORT

Einleitung, Geltungsbereich, Definitionen

1. Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag oder firmenintern, welches ebenfalls vertraglich mit Mitarbeitern bzw. Abgestellten zu regeln ist, da eine Geheimhaltungserklärung zwar ebenfalls nach der EU DSGVO verpflichtend ist, jedoch nicht den Umfang dieses Vertrages widerspiegeln kann.
2. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.
3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

Gegenstand und Dauer

Gegenstand

Gegenstand der Vereinbarung sind die Rechte und Pflichten der Parteien im Rahmen der Leistungserbringung gemäß Auftrag, Leistungsbeschreibung und AGB, soweit eine Verarbeitung von personenbezogenen Daten durch den Auftragnehmer als Auftragsverarbeiter für den Auftraggeber gemäß Art. 28 DSGVO erfolgt. Dies umfasst alle Tätigkeiten, die der Auftragnehmer zur Erfüllung des Auftrags erbringt und die eine Auftragsverarbeitung darstellen.

Gegenstand des Vertrages ist **nicht** die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Im Zuge der Leistungserbringung des Auftragnehmers als zentraler IT-Dienstleister im Bereich Wartung und Support, Hostings, der Administration von Client-Server-Systemen und IT Komponenten des Auftraggebers, kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden. Dies gilt auch, sofern der Auftrag nicht ausdrücklich auf diese Vereinbarung zur Auftragsverarbeitung verweist.

Der Auftragnehmer erbringt nur Leistungen während folgender Normalarbeitszeit, sofern nicht schriftlich z.B. ein 24 x 7 Support vereinbart worden ist, welches nur durch eine schriftliche Zusatzvereinbarung getroffen werden kann.

Montag bis Donnerstag	09.00 und 16.00 Uhr	(Ortszeit Wien)
Freitag	09.00 und 12.00 Uhr	(Ortszeit Wien)

Ausgenommen sind Arbeiten während Betriebssperren, Fenster- und Feiertagen, oder ähnlichen bekannt gegebenen Zeiten und Tage, die online jederzeit einsichtig und öffentlich zugänglich sind, unter: <http://www.mental.at/kontakt/>

Der Auftragnehmer übernimmt folgende Verarbeitungen:

- Angebotslegung, Ein- und Verkauf, und Implementierung von Produkten**
- Angebotslegung, Ein- und Verkauf, und Implementierung von Services**

Wartung der IT Infrastruktur inkl. Dokumentation

Der Vertragsgegenstand „Wartung der IT Infrastruktur inkl. Dokumentation“ regelt die Wartung für alle in der seitens unseres Unternehmens erstellten Dokumentation aufgeführten Geräte und Software durch unser Unternehmen, sofern unser Unternehmen administrativen Zugang zu Wartung innehat. **Eine Wartung mit Ausschluss der Dokumentation durch Unternehmen ist dezidiert ausgeschlossen**, jedes von Auftraggeber implementierte Gerät in die IT Landschaft ist den Auftragnehmer unmittelbar zu melden, um diese in die Dokumentation einfließen lassen zu können, damit gewährleisten wir alle zu treffenden Maßnahmen hinsichtlich der DSGVO. Dieser Vertragsgegenstand umfasst Serviceleistungen, um die Betriebsbereitschaft der Maschinen aufrechtzuerhalten. Der Auftragnehmer kann den störungsfreien Betrieb der Anlage jedoch nicht garantieren.

Die Wartungsleistung umfasst alle, für einen ordentlichen Betrieb erforderlichen Arbeiten zur Hard- und Softwarepflege, allerdings **dezidiert ausgenommen sind** Major Batch Releases, außergewöhnliche Sicherheitspatches und Update Einspielungen, die durch Sicherheitslücken Dritter (Hersteller) verursacht werden, da diese nicht durch unser Unternehmen, aus verständlichen Gründen weder vorhersehbar und kalkulierbar sind.

Im Wartungsumfang enthalten ist die Arbeitszeit in dem bereits definierten Zeitraum (Normalarbeitszeit), und der telefonische Support (aktiver Anruf vom Auftraggeber, etwaige aktive Rückrufe sind im Wartungsaufwand nicht enthalten).

Der Auftragnehmer übernimmt keine Haftung für Fehler von Softwareprodukten jeglicher Art. Führt der Auftragnehmer aufgrund eines Auftrages des Kunden Serviceleistungen durch, zu denen Sie nach diesem Vertrag nicht verpflichtet ist, so werden diese Leistungen dem Kunden nach den zurzeit gültigen Stundensätzen berechnet. Die Durchführung der Wartung dient der Erhaltung der Betriebsbereitschaft und erfolgt in Übereinstimmung mit den Richtlinien des Herstellerwerkes der Komponenten. Die normalen Reaktionszeiten werden wie genannt vereinbart und beziehen sich auf die Störungsannahme.

- | | | | |
|--------------------------|-----------------------------------|----------------------------|--|
| <input type="checkbox"/> | Reaktionszeit ¹ | innerhalb von Stunden | <input type="checkbox"/> 4 <input type="checkbox"/> 8 <input type="checkbox"/> 16 |
| <input type="checkbox"/> | Reparaturzeit ² | innerhalb von Arbeitstagen | <input type="checkbox"/> 4 <input type="checkbox"/> 8 |
| <input type="checkbox"/> | Ersatzgerät ³ | innerhalb von Stunden | <input type="checkbox"/> 8 <input type="checkbox"/> 16 <input type="checkbox"/> 32 |

Werden keine spezifizierten Zeitangaben vereinbart, so wird vom Auftragnehmer ein Techniker bei Freiwerden entsendet. Der Auftraggeber hat jedoch keinen Anspruch auf Reihung im Helpdesk Management des Auftragnehmers und wird etwaigen Besitzern eines Wartungsvertrages nachgestellt.

¹ Nach Mitteilung einer Störung durch den Auftraggeber bleibt es dem Auftragnehmer vorbehalten, die Störung telefonisch und unter Mithilfe des Auftraggebers- oder am Aufstellungsort des betroffenen Gerätes zu beseitigen bzw. diese durch Remotewartung zu beheben. Der Auftragnehmer verpflichtet sich die Störungsbeseitigung innerhalb des vereinbarten Zeitraums nach Störungsmeldung (Reaktionszeit) aufzunehmen, wenn die Remotewartung bzw. die telefonische Beratung zur Störungsabhilfe erfolglos war, oder ein Ortstermin zur Störungsbeseitigung unabwendbar ist. ² Der Auftragnehmer verpflichtet sich, innerhalb des vereinbarten Zeitraumes (= Reparaturzeit, ab dem Zeitpunkt der Störungsmeldung) einen Reparaturversuch des in Störung befindlichen Gerätes durchzuführen. Kann die Reparatur erfolgreich durch den Auftragnehmer umgesetzt werden, so gilt diese Störung als behoben. Ist die Reparatur durch den Auftragnehmer nicht durchführbar (Geräteschaden, Abnutzung, Überbeanspruchung, Herstellerfehler, unsachgemäße Bedienung, etc.), so eröffnet, sofern das Gerät durch den Auftragnehmer verkauft und geliefert wurde, und ein Anspruch auf Gewährleistung bzw. Garantie besteht, einen RMA Fall, der nach handelsüblichen Abläufen der Lieferanten bzw. Herstellern gehandhabt wird.

³ Der Auftraggeber hat die optionale Möglichkeit eines Ersatzgerätes. Der Auftragnehmer verpflichtet sich, innerhalb des vereinbarten Zeitraumes (= Reparaturzeit, ab dem Zeitpunkt der Störungsmeldung) ein Ausweichgerät zu stellen, wenn die

Störung bis dahin nicht beseitigt ist. Das Ausweichgerät muss zumindest einen Betrieb innerhalb der Anlage aufrechterhalten und nicht den bisherigen Leistungsumfang des gestörten Gerätes entsprechen.

Wenn sich herausstellt, dass die Herstellung der Betriebsbereitschaft nicht mehr möglich ist, oder einen wirtschaftlich unverhältnismäßigen Aufwand erfordert, entfällt sowohl die Pflicht der Instandsetzung als auch die Pflicht der Bereitstellung eines Ersatzgerätes, sofern dies vereinbart wurde. Ein wirtschaftlich unverhältnismäßiger Aufwand liegt bei einer Reparatur vor, die inklusiven Ersatzteilkosten, Vergütungsaufwand für die Reparatur jeweils inklusive Mehrwertsteuer ein Drittel des Betrages übersteigt, den das Gerät zur Zeit der Reparatur wert ist.

Insoweit, als der Auftraggeber schriftlich erklärt, die Reparatur möge trotz des Kostenrisikos fortgeführt werden, bleiben die Pflichten der Instandsetzung und der Bereitstellung der Anlage des Verkäufers bestehen, die sich ergebenden Mehrkosten dafür werden aber gesondert in Rechnung gestellt. Der Auftragnehmer dokumentiert die Wartung. Stellt sich bei dem Versuch einer Störungsbeseitigung heraus, dass die erforderliche Reparatur wirtschaftlich unverhältnismäßig ist, hat der Auftragnehmer dieses in Form eines Kostenvoranschlages festzuhalten bzw. dem Auftraggeber schriftlich oder mündlich dies mitzuteilen.

Die Wartung der Geräte hat am Wartungsort zu erfolgen, sofern die Wartung Vorort durchführbar ist. Soll die Anlage an einem anderen Ort betrieben werden, so hat der Auftraggeber den Auftragnehmer hiervon frühzeitig schriftlich in Kenntnis zu setzen.

Der Auftragnehmer trägt alle Kosten, die mit der Ersatzteilbeschaffung zusammenhängen (nicht jedoch die Kosten für die Ersatzteile, die der Auftraggeber in jedem Fall zu tragen hat). Die Kosten für die notwendige Ausrüstung der Technik mit Werkzeugen, trägt der Auftragnehmer.

Im Vertragsgegenstand „Wartung der IT Infrastruktur inkl. Dokumentation“ werden folgende **Vergütungen** vereinbart, wie folgt:

<input type="checkbox"/>	Remote Wartung ⁴	monatliche Pauschale	EUR
	Verrechnung:	¼ jährlich im Voraus	
<input type="checkbox"/>	Vorort Wartung ⁵	Stundenpauschale	EUR
	Verrechnung:	nach Aufwand	
<input type="checkbox"/>	Notfall Service ⁶	Stundenpauschale	EUR
	Verrechnung:	nach Aufwand	

⁴ die monatliche Pauschale der Remote Verwaltung beinhaltet alle Störungen, welche telefonisch -und unter Mithilfe des Auftraggebers oder durch den Remotezugriff auf das System behoben werden können. Nicht beinhaltet in der Pauschale sind Zusatzkonfigurationen an den Servern wie z.B. erweiterte Userverwaltung (neue User), erweiterte Einstellungswünsche (Softwareinstallationen auf Wunsch des Auftraggebers) und ähnliche Arbeiten, die nicht im Vorfeld vereinbart wurden.

⁵ wird eine Remote Wartung vereinbart, so gilt bei der Vorortwartung der vereinbarte Stundensatz ab dem Eintreffen des Technikers des jeweilig aktuellen Einsatz- bzw. Standortes. Es werden hierbei keine zusätzlichen Wegzeiten, Fahrtkosten oder Spesen in Rechnung gestellt, sofern dies im üblichen Bereich der Anzahl von Technikereinsätzen Vorort nicht übersteigt. Dies gilt für Standorte in Wien.

Für Standorte außerhalb von Wien wird folgende **Fahrtkostenpauschale** vereinbart:

- Standort 1 _____ EUR
- Standort 2 _____ EUR
- Standort 3 _____ EUR

⁶ wird seitens des Auftraggebers eine sofortige Problemlösung angestrebt, welche die Reaktionszeiten und Reparaturzeit weit unterschreiten, so tritt das Notfall Service in Kraft, sofern ein Techniker durch den Auftragnehmer entsendet werden kann. Es werden hierbei keine zusätzlichen Wegzeiten, Fahrtkosten oder Spesen in Rechnung gestellt, sofern dies im üblichen Bereich der Anzahl von Technikereinsätzen Vorort nicht übersteigt. Dies gilt für Standorte in Wien.

Für Standorte außerhalb von Wien wird folgende **Fahrtkostenpauschale im Notfall** vereinbart:

- Standort 1 _____ EUR
- Standort 2 _____ EUR
- Standort 3 _____ EUR

Zusätzlich zur Remote Wartung wird pro Gerät, welches einer Fernwartung zugeführt werden kann (Server, Workstation, Laptop, Mobile Devices), eine **Lizenz zur Remote Software** benötigt um den reibungslosen Zugriff zu gewähren.

- Remote Lizenz** pro Gerät und Jahr EUR
- Anzahl: STK

Sichere VPN Verbindung

Um einige Services und Remote Wartungen durchführen zu können wird eine sichere VPN Verbindung mit einem strikten Regelwerk seitens unseres Unternehmens benötigt. Darunter fallen Remote Zugriff auf Virtuelle Server Infrastruktur (VMWare, Citrix, ...), Netzwerkkomponenten (Switches, WLAN, ...) und ähnliche Geräte, aber auch für Services wie Endpoint Protection und Email Services.

VPN Verbindung vorhanden ja nein

Monatliche Pauschale EUR _____

Ersatzgeräte Service Verrechnung: ¼ jährlich im Voraus

Wird seitens des Auftraggebers die optionale Möglichkeit eines Ersatzgeräte Services vereinbart, so wird nach Feststellung einer nicht durch den Auftragnehmer zu erledigende Reparatur, die Bereitstellung eines Ersatzgerätes veranlasst, welches einen Weiterbetrieb des Systems gewährleistet, jedoch muss das Ersatzgerät nicht den gleichen Spezifikationen des zur Reparatur ausgeschriebenen Gerätes entsprechen, sondern überbrückt den Ausfall des jeweiligen Gerätes. Die Geräte zum Ersatzgeräteservice (z.B. Firewall, Drucker, Switches, ...) sind hier dezidiert anzugeben. Gerätschaften des Auftraggebers die nicht hier bzw. in einer gesonderten Auflistung als schriftlicher Zusatz enthalten sind nicht Ersatzgerätefähig.

Gerät 1: _____

Seriennummer: _____

Modellnummer: _____

monatliche Pauschale EUR

Gerät 2: _____

Seriennummer: _____

Modellnummer: _____

monatliche Pauschale EUR

Gerät 3: _____

Seriennummer: _____

Modellnummer: _____

monatliche Pauschale EUR

Gerät 4: _____

Seriennummer: _____

Modellnummer: _____

monatliche Pauschale EUR

Gerät 5: _____

Seriennummer: _____

Modellnummer: _____

monatliche Pauschale EUR

Zusatzleistungen

zum Vertragsgegenstand „Wartung der IT Infrastruktur inkl. Dokumentation“

Über die vorgenannten Leistungen hinaus verpflichtet sich der Auftragnehmer auf Abruf nachgenannte Leistungen gegen Zahlung einer weiteren Vergütung zu erbringen, die da sind,

Beseitigungen von Störungen, ...

- ... die auf unsachgemäßem Gebrauch der Anlage
z.B. Bedienungsfehler, Anschluss ungeeigneter Zusatzeinrichtungen- beruhen,
- ... die auf Fälle höherer Gewalt zurückzuführen sind
z.B. Stromschäden, Blitzschäden, Wasserschäden-,
- ... die auf einem unsachgemäßen Transport vom Aufstellungsort
an einen anderen Ort beruhen.

Diese zusätzlichen Leistungen werden im Rahmen der Erfüllung der weiteren Geschäfte des Auftragnehmers erfüllt. Soweit Kapazitäten frei sind und keine anderen Verpflichtungen des Auftragnehmers entgegenstehen, erfüllt der Auftragnehmer diese Verpflichtungen zu seinen üblichen Normalarbeitszeiten.

Ist ein Stundenpauschale für Wartungsarbeiten Vorort vereinbart, so erfolgt die Verrechnung dem vereinbarten Stundensatz gleichgestellt, ist dies nicht der Fall, so gelten die zum Zeitpunkt geltenden Standardsätze des Auftragnehmers.

Falls eine Datensicherung oder eine Datenrücksicherung/Neuinstallation von Software durch das Wartungspersonal des Auftragnehmers durchgeführt werden muss, so werden die Kosten hierfür mit dem derzeit geltenden Stundensatz des Auftragnehmers in Rechnung gestellt, wobei wiederum bei vereinbartem Wartungsentgelt Vorort die Kosten angeglichen werden.

Ersatzteile & Pflegemittel

Wenn Instandsetzungsarbeiten ohne Einsatz von kostenträchtigen Ersatzteilen, hierunter fallen Ersatzteile mit einem Wert inklusive Mehrwertsteuer von über EUR 3.000,00 nicht möglich sind, hat der Auftragnehmer den Auftraggeber hiervon zu unterrichten. Die Kosten der Ersatzteile, Schmierungsstoffe und weiterer Mittel, ohne die eine ordnungsgemäße Wartung nicht möglich ist, trägt der Auftraggeber.

Mitwirkungspflichten des Auftraggebers

Der Auftraggeber trägt Obacht, die Bedienungsanweisung, insbesondere hinsichtlich der Bedienung und der Pflege, zu befolgen. Der Auftraggeber hat dem Auftragnehmer auftretende Störungen unmittelbar nach deren Auftreten anzuzeigen. Die Anzeige hat ausführlich, unter Berücksichtigung der in der Bedienungsanleitung aufgeführten Fehleranalyse, zu erfolgen.

Bei der Wartung wird der Auftragnehmer vom Auftraggeber unterstützt, indem dieser fachkundiges Personal für die Durchführung der Wartungsarbeiten abstellt, dass mit den Programmen und den Systemen vertraut ist. Bevor Wartungsarbeiten durchgeführt werden, ist der Auftraggeber verpflichtet Daten und Programme zu sichern.

Wenn die Wartungsarbeiten es erfordern, hat der Auftraggeber Programme, Daten, Datenträger entfernen. Ansprüche des Auftraggebers, insbesondere auf Schäden wie entgangenen Gewinn, ausgebliebene Einsparung, Schäden aus Ansprüchen Dritter gegen den Kunden, Verlust von Daten usw. sind in jedem Fall ausgeschlossen. Der Auftraggeber ist verpflichtet, den Auftragnehmer bei der Durchführung der Wartung umfassend zu unterstützen. Er hat z.B. räumliche Möglichkeiten für die Aufbewahrung von Ersatzteilen, Werkzeug zu schaffen. Ebenso hat er die erforderlichen technischen Voraussetzungen –z.B. Übertragungsleitungen - kostenlos zur Verfügung zu stellen.

Der Auftraggeber trägt dafür Sorge, dass die mit der Wartung beauftragten Mitarbeiter des Auftragnehmers nach Ankündigung, von Montag - Freitag in der Zeit von 08.00 - 18.00 Uhr, Zugang zu den Geräten haben. In besonders dringenden Fällen kann eine Wartung auch außerhalb dieser Zeiten vereinbart werden.

Der Auftraggeber trägt die volle Verantwortung für die korrekte Durchführung der Datensicherung bzw. für alle gespeicherten Daten. Der Auftraggeber verpflichtet sich die Geräte entsprechend den vom Hersteller herausgegebenen Bedienungsanleitungen zu betreiben. Alle vom Auftraggeber verwendeten Zubehörteile müssen den vom Hersteller empfohlenen Normen entsprechen oder vom Auftragnehmer als geeignet eingestuft werden.

Der Auftraggeber trägt dafür Sorge, dass das Stromnetz gemäß den einschlägigen Normen ausgelegt und frei von Spannungsschwankungen und Störungen ist, die den Betrieb der Geräte beeinträchtigen. Beim Auftreten einer Störung teilt der Kunde diese Störung dem Auftragnehmer unverzüglich mit.

Bevor der Auftraggeber eine Maschine für den Service übergibt, hat er daraus alle Programme, Daten und Datenträger zu entfernen.

Vergütung

Die vereinbarten Gebühren gelten für die in der Normalarbeitszeit des Auftragnehmers anfallenden Wartungsarbeiten und sind exklusive den gesetzlich zu entrichtenden Abgaben (MwSt., ARA, etc.). Der Auftragnehmer weist die Mehrwertsteuer durch Rechnungserstellung aus. Der Rechnungsbetrag ist ohne Abzug netto Kassa zu entrichten, sofern keine andere Regelung getroffen wurde.

Für Wartungsarbeiten, die an einem Wochenende, an einem Feiertag oder außerhalb der Normalarbeitszeiten anfallen wird eine zusätzliche Gebühr pro Stunde vereinbart, wie folgt:

EUR _____

Insoweit, als der Auftragnehmer Zusatzleistungen des Vertrages erbringt, gelten die für die von dem Auftragnehmer für regelmäßige Wartungsarbeiten geltend gemachten stundenweise Gebührensätze, in ihrer jeweiligen Höhe. Fahrtkosten und Spesen werden gesondert und/oder nach aktuellen Bestimmungen verrechnet.

Wenn der Auftraggeber seinen Geschäftsbetrieb, und damit die Anlage an einen um 50 Kilometer entfernten Ort als den Aufstellungsort von dem Geschäftssitz des Auftragnehmers verlegt, hat der Auftraggeber dem Auftragnehmer die zusätzlichen Kilometer pro Kilometer (gesetzliches Kilometergeld) zu erstatten. Der Auftraggeber hat den Auftragnehmer über eine Verlegung der Anlage rechtzeitig zu informieren. Wird der Auftragnehmer nicht informiert, so hat dieser das einseitige Recht zur Kündigung des Vertrages mit Datum der Verlegung.

□ Email Security Service

Der Vertragsgegenstand „Email Security Service“ regelt den Einsatz von Maßnahmen zur Sicherheit im Email Verkehr und gewährleistet eine Schutzmaßnahme hinsichtlich der DSGVO, insbesondere die **sicher Übertragung der Daten** (inkl. Verschlüsselung) **vom Provider oder Domainprovider bis zum Email Server des Kunden** (eingehende Emails), ebenso wie der Schutz vor schädlichen Inhalten und Programmen und Verlust von Daten.

Für das korrekte senden der Daten vom Email Server des Kunden (ausgehende Emails) ist der Kunde selbst verantwortlich. Hierbei kann unser Support Team selbstverständlich zur Seite stehen.

Unser Unternehmen stellt eine technische Lösung zur Verfügung der Hersteller Barracuda Networks, wie folgt:

Barracuda Email Security Gateway

Durch den Schutz vor eingehender Malware, Spam, Phishing und Denial-of-Service-Angriffen stellt der Barracuda Email Security Gateway sicher, dass die Produktivität nicht durch Angriffe über das E-Mail-System beeinträchtigt wird. Leistungsfähige Verschlüsselungstechnologie verhindert, dass sensible Daten von Unbefugten eingesehen werden. Alle Technische Daten zur eingesetzten Technologie finden Sie unter: <https://www.barracuda.com/products/emailsecuritygateway>

Hersteller:	Barracuda Networks
Standardsoftware:	<input checked="" type="checkbox"/> ja, Virtuelle Appliance
Eingesetzte Lösungen:	Barracuda Email Security Gateway
Datenstandort:	Österreich (Arsenal)
Drittstaatenübermittlung:	<input checked="" type="checkbox"/> nein
Verschlüsselung:	<input checked="" type="checkbox"/> ja, TLS, SSL
SMTP über TLS/SSL aktiviert:	<input checked="" type="checkbox"/> ja ¹
Schwache Verschlüsselung erlauben:	<input checked="" type="checkbox"/> nein ²
SSLv3 erlauben:	<input checked="" type="checkbox"/> nein ³
Dauer der Aufbewahrung in Tagen:	30 ⁴
Zugriff durch Dritte:	<input checked="" type="checkbox"/> nein ⁵
Mehrstufige Absichts-Analyse:	<input checked="" type="checkbox"/> ja
Echtzeit-Absichts-Analyse:	<input checked="" type="checkbox"/> ja
Virens Scanner:	<input checked="" type="checkbox"/> ja

Zweck des Einsatzes

Erfüllung von Aufträgen und Vertragsgrundlagen
Schutz vor schädlichen Inhalten und Programmen
Queue Spooling um Verlust von Daten vorzubeugen ⁴

¹ Beschreibung: SMTP über TLS für eingehende E-Mail-Nachrichten wird verwendet.

² Beschreibung: Um PCI-konform zu sein, muss Sie diese Option auf Nein gesetzt werden.

³ Beschreibung: Kompatibilität zu alte Email Servern, wird mit DSGVO nicht mehr unterstützt.

⁴ Die maximale Anzahl der Tage für die Aufbewahrung einer Nachricht. Bei erhöhtem Emailaufkommen, kann sich dieser Aufbewahrungszeitraum verkürzen (ressourcenabhängige Festplattengröße)

⁵ Der Zugriff ist nur durch geschultes und fachkundige Mitarbeiter unseres Unternehmens über administrative Accounts möglich und auf ein Minimum reduziert, ein direkter Zugriff Kundenseitig ist nicht möglich.

Allgemeine Providerangaben

Name des Providers _____

Servername | IP (z.B. mail.provider.at) _____

Protokoll POP3 (S) IMAP (S)

Port (z.B. 995, 993) _____

Gewünschtes Abfrageintervall 30 60 90 120

Postfächer zur Abholung

Username | Email Adresse: _____

Username | Email Adresse: _____

Username | Email Adresse: _____

Username | Email Adresse: _____

Username | Email Adresse: _____

Username | Email Adresse: _____

Username | Email Adresse: _____

Username | Email Adresse: _____

Passwörter werden hier nicht gelistet und gesondert übermittelt

Übermittlung nach Sicherheitsüberprüfung

SMTP über TLS/SSL aktiviert ja

Übermittlungstechnologie **VPN + SMTP über TLS**

LAN IP Adresse Ihres Servers _____

Port _____

Übermittlungstechnologie **SMTP über TLS**

Public IP Adresse Ihres Servers _____

Port _____

Vergütung

Es wird eine Vergütung wie folgt vereinbart.

Monatliche Pauschale für alle Email Adressen EUR _____

Monatliche Pauschale für einzelne Postfächer Anzahl _____

EUR _____

☐ Email Security Service Advanced

Der Vertragsgegenstand „Email Security Service Advanced“ regelt den Einsatz von erweiterten Maßnahmen zur Sicherheit im Email Verkehr und gewährleistet eine erweiterte Schutzmaßnahme hinsichtlich der DSGVO, insbesondere die **sicher Übertragung der Daten** (inkl. Verschlüsselung) **vom Provider oder Domainprovider bis zum Email Server des Kunden** (eingehende Emails), ebenso wie der Schutz vor schädlichen Inhalten und Programmen und Verlust von Daten.

Der Einsatz von „Email Security Service Advanced“ setzt den Punkt „Email Security Service“ voraus.

Für das korrekte senden der Daten vom Email Server des Kunden (ausgehende Emails) ist der Kunde selbst verantwortlich. Hierbei kann unser Support Team selbstverständlich zur Seite stehen.

Unser Unternehmen stellt eine technische Lösung zur Verfügung der Hersteller Barracuda Networks, wie folgt:

Barracuda Email Cloud Protection Layer

Der Barracuda Cloud Protection Layer sorgt einerseits dafür, dass E-Mails für bis zu 96 Stunden gespoilt (Queue) werden, mit der Option, den Datenverkehr auf einen zweiten Server umzuleiten und die Vorfilterung von schädlichen Inhalten und Programmen, sowie Viren, Trojaner und ähnliche Bedrohungen. Grundsätzlich ist ein passwortgeschützter Zugriff auf das Barracuda BCC möglich. Individuelle Berechtigungen schützen vor einem missbräuchlichen Zugriff. Ein direkter Zugriff ist nur ausgewählten Administratoren möglich.

Hersteller:	Barracuda Networks
Standardsoftware:	<input checked="" type="checkbox"/> ja, Virtuelle Appliance
Eingesetzte Lösungen:	Barracuda Email Cloud Protection Layer
Datenstandort:	Deutschland, EU
Drittstaatenübermittlung:	<input checked="" type="checkbox"/> nein
Verschlüsselung:	<input checked="" type="checkbox"/> ja, TLS, SSL
SMTP über TLS/SSL aktiviert:	<input checked="" type="checkbox"/> ja ¹
Schwache Verschlüsselung erlauben:	<input checked="" type="checkbox"/> nein ²
Zugriff durch Dritte:	<input checked="" type="checkbox"/> nein ⁵
Virens Scanner:	<input checked="" type="checkbox"/> ja

Zweck des Einsatzes

Erfüllung von Aufträgen und Vertragsgrundlagen
Schutz vor schädlichen Inhalten und Programmen
Queue Spooling um Verlust von Daten vorzubeugen ⁴

¹ Beschreibung: SMTP über TLS für eingehende E-Mail-Nachrichten wird verwendet.

² Beschreibung: Um PCI-konform zu sein, muss Sie diese Option auf Nein gesetzt werden.

⁵ Der Zugriff ist nur durch geschultes und fachkundige Mitarbeiter unseres Unternehmens über administrative Accounts möglich und auf ein Minimum reduziert, ein direkter Zugriff Kundenseitig ist nicht möglich.

Vergütung

Es wird eine Vergütung wie folgt vereinbart.

- Monatliche Pauschale für alle Email Adressen EUR _____
- Monatliche Pauschale für einzelne Postfächer Anzahl _____
EUR _____

Webhost

Unser Unternehmen stellt dem Auftraggeber Speicherplatz (Webspace) auf einem seitens unseres Unternehmens verwalteten Shared Server (Webhost) der Firma UPC Business Austria GmbH zur Verfügung. Der Auftragnehmer hat hierdurch die Möglichkeit, Dateien wie eine Homepage oder auch Bilder, Programme oder andere Anwendungen auf dem Speicherplatz (Webspace) abzulegen und diese somit im Internet zugänglich zu machen.

Die Server sind im Network Operating Center (NOC) von UPC Business untergebracht, das bedeutet, diese entsprechen den hohen Sicherheitsanforderungen, sind 7x24 Stunden überwacht und verfügen über sehr leistungsfähige multiple nationale sowie internationale Internetanbindungen. Eine unterbrechungsfreie Stromversorgungseinheit (USV) stellt die Stromversorgung sicher. Ein Backbone Autoswitch gewährleistet das sofortige Umschalten auf eine Ersatzleitung bei Ausfall einer Leitung. Im Einzelfall kann es bei der Umschaltung zu kurzen Service-Unterbrechungen kommen.

Name des Providers _____

Ihre Domain _____

Statische Webseite (html, htm, php)

Wordpress inkl. MySQL Datenbank

Wordpress inkl. MySQL Datenbank & Divi Theme

Wartung der Seite durch den Auftragnehmer ja nein

wenn "ja" übernimmt der Auftraggeber die Aktualisierung der grundlegenden eingesetzten Technologien (z.B. Wordpress, Theme, Plugins) im Umfang das einer Wartung

einmal pro Monat einmal pro Woche einmal pro Halbjahr

Änderungen der Texte, Bilder, neue Seiten und Inhalte werden über den Stundensatz nach Aufwand abgerechnet.

Vergütung

Es wird eine Vergütung wie folgt vereinbart.

Monatliche Pauschale Hosting EUR _____

Monatliche Pauschale Wartung EUR _____

Endpoint Protection

Unser Unternehmen stellt Ihnen ein skalierbares, zentralisiertes Sicherheitsmanagement zur Verfügung (**Policy Manager**). Die beste Software für Unternehmenssicherheit besteht aus einem mehrschichtigen Schutz, der einfach zu verwalten und zu steuern ist. Der **Policy Manager** ist das zentrale Management-Tool der Business Suite und bietet erweiterte Funktionen für die lokale Verwaltung des Endgeräteschutzes in anspruchsvollen IT-Umgebungen kombiniert mit Automatisierung. Sie können alle Ihre Sicherheitsanwendungen mit einem Tool verwalten, Sicherheitsrichtlinien definieren und verteilen, die Gesamtsicherheit Ihres Unternehmens überwachen und das Endnutzerverhalten im Unternehmensnetzwerk steuern.

Voraussetzung dafür ist eine VPN Verbindung und eine Wartung durch unser Unternehmen, sowie der Erwerb der entsprechenden Lizenzen über unseren Partner F-Secure.

- Schützen Sie alle Ebenen Ihrer IT-Infrastruktur dauerhaft mittels automatisierter Updates
- Definieren und verteilen Sie Sicherheitsrichtlinien zentral und überwachen Sie die Gesamtsicherheit Ihres Unternehmens
- Verwalten Sie sowohl physische als auch virtuelle Umgebungen mit nur einem Tool
- Steuern Sie den Web-Zugriff, um Ihr Netzwerk zu schützen und die Produktivität zu erhöhen
- Blockieren Sie bestimmte Inhalte von unbekanntem Seiten und verweigern Sie die externe Steuerung gefährdeter Assets
- Autorisieren Sie Endnutzer dazu, Online-Banking und andere geschäftskritische Transaktionen sicher durchzuführen
- Verringern Sie den Netzwerk-Traffic und erhöhen Sie die Skalierbarkeit mit F-Secure Proxy
- **Automatisieren Sie das Patchmanagement mit dem Software Updater (nur Premium Edition)**

Client Security Standard

Client Security Premium

handelt es sich um weit mehr als nur ein Anti-Malware-Tool - es bietet Schutzelemente der nächsten Generation, wie Bedrohungs-Intelligence, Verhaltensanalyse und proaktiven Schutz vor allen neuen Bedrohungen. Client Security ist ein Unternehmenssicherheitsprodukt, das Ihnen die beste Windows-Sicherheit für die Endgeräte in Ihrem Unternehmen bietet - Jahr ein, Jahr aus.

Server Security Standard

Server Security Premium

eine Anti-Malware-Suite speziell für Server, die preisgekrönter Schutz für Dateiserver bietet. Server Security bietet einen verbesserten Echtzeitschutz vor Viren, Trojanern, Spyware, Rootkits und anderer Malware. Das Tool bietet zentralisierte und lokale Schnittstellenmanagementoptionen über den Policy Manager oder über eine integrierte Web-Konsole.

<input type="checkbox"/> Monatliche Pauschale pro Client	EUR	_____
<input type="checkbox"/> Monatliche Pauschale pro Server	EUR	_____
<input type="checkbox"/> Monatliche Pauschale	EUR	_____

Erhöhung der Vergütung

Die Höhe der Vergütung für die Wartung der Anlage beruht auf den bei Unterzeichnung des Vertrages geltenden Stundensätzen des Auftragnehmers. Die Vergütungssätze beruhen auf den Kostenfaktoren des Auftragnehmers. Wenn sich die aktuellen Stundensätze des Auftragnehmers aufgrund der Erhöhung der Kostenfaktoren ändern, ist er nach Ablauf der ersten Wartungsperiode berechtigt, die Vergütung entsprechend der Entwicklung der Vergütungssätze zu erhöhen. Die Erhöhung der Vergütung kann nur für den Beginn einer neuen Wartungsperiode erklärt werden. Weitere Voraussetzung ist, dass der Auftragnehmer die Erhöhung der Vergütung vier Monate vor Inkrafttreten schriftlich ankündigt.

Haftung

Der Auftragnehmer haftet in voller Schadenshöhe für eigenes grobes Verschulden, nämlich für Vorsatz und grobe Fahrlässigkeit. Dieses gilt auch bei grobem Verschulden leitender Angestellter. Darüber hinaus haftet der Auftragnehmer dem Grunde nach bei jeder schuldhaften Verletzung wesentlicher Vertragspflichten. In diesen Fällen haftet der Auftragnehmer der Höhe nach nur auf Ersatz des typischen, vorhersehbaren Schadens.

Ansprüche des Kunden, insbesondere auf mittelbare Schäden wie entgangenen Gewinn, ausgebliebene Einsparung, Schäden aus Ansprüchen Dritter gegen den Kunden, Verlust von Daten usw. sind in jedem Fall ausgeschlossen. Die Haftung ist unabhängig vom Rechtsgrund, auf EUR 10.000,00 oder eine Servicegebühr derjenigen Maschine begrenzt, die den Schaden verursacht hat oder Gegenstand des Anspruchs ist oder in direkter Beziehung dazu steht. Es gilt der jeweils höhere Betrag.

Verbrauchsmaterialien wie Farbbänder, Disketten, Toner und Materialsätze (Bildtrommel) sowie Feuer, Blitzschlag, Vorsatz, Erdbeben, Kernenergie, Kriegereignisse, Einbruch, Vandalismus und Diebstahl, Stromversorgung durch Dritte, Reparaturversuche des Kunden, Reparaturversuche Dritter, Einwirkungen auf Geräte und Software durch den Kunden oder Dritte sind von der Haftung ausgenommen bzw. entheben den Auftragnehmer von der Haftungspflicht.

Für Verstöße gegenüber Lizenzrechten, Urheberrechten Dritter insbesondere bei Standard Software ist der Auftragnehmer nicht haftbar. Der Auftragnehmer ist auch nicht verpflichtet solche Verstöße zu melden oder anzuzeigen, er behält sich jedoch das Recht vor den Auftraggeber diesbezüglich zu informieren und etwaig benötigte Rechte und Lizenzen zum Kauf anzubieten.

Vertraulichkeit

Unabhängig von dem Bestehen des Vertrages verpflichtet sich der Auftragnehmer, über alle ihm in Erfüllung des Vertrages bekannt gewordenen/ bekanntwerdenden Geschäfts-/ Betriebsgeheimnisse und Geschäfts-/ Betriebsangelegenheiten Stillschweigen zu bewahren. Dies gilt auch für die Zeit nach Ablauf des Vertrages.

Vertragsänderungen

Mündliche Nebenabreden sind nicht getroffen. Sämtliche Vertragsänderungen, sowohl Änderungen als auch Ergänzungen, -inklusive dieser Regelung- bedürfen der Schriftform.

Teilunwirksamkeit

Sollte eine der vorstehenden Regelungen des Vertrages unwirksam sein, so lässt dies die Gültigkeit der anderen Regelungen und des Vertrages unberührt. Die Vertragsparteien verpflichten sich, hinsichtlich der unwirksamen Regelung eine neue zu schaffen, die dem wirtschaftlich Gewollten der unwirksamen Regelung am nächsten kommt.

Diverses

Über diesen Wartungsvertrag hinaus gelten die Allgemeinen Geschäftsbedingungen. Es wird bestätigt, dass er die Allgemeinen Geschäftsbedingungen unseres Unternehmens zur Kenntnis genommen wurden und deren Anwendung auf diesen Vertrag Zustimmung gegeben wurde. Erfüllungsort für die Leistungen aus diesem Vertrag ist Wien. Es gilt österreichisches Recht.

Dauer

Die Verarbeitung beginnt mit Zeichnung des Vertrages und ersetzt und erweitert jegliche vormals getroffenen Vereinbarungen und Verträge und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags durch eine Partei, mit dem Hinweis auf Gültigkeit durch das Inkrafttreten der EU Datenschutzgrundverordnung (DSGVO) mit 25. Mai 2018.

Erweitert dieser Vertrag einen bisher getroffenen Vertrag (z.B. Wartungsvertrag, dessen Inhalt weiter als Hauptvertrag gilt), so wird das Kündigungsrecht seitens des Auftraggebers auf eine jährliche Kündbarkeit umgestellt, und zwar jeweils zum ersten eines Kalenderjahres mit 6-monatiger Kündigungsfrist in schriftlicher Form. Eine Kündigung per Email ist nicht zulässig, es gilt das Datum des Poststempels (Einschreiben), desgleichen gilt auch für die Dauer dieser Vereinbarung.

Ort der Verarbeitung

Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

Datenverarbeitungstätigkeiten auch nur zum Teil auch außerhalb der EU bzw. des EWR durchgeführt, und zwar in:

Das angemessene Datenschutzniveau ergibt sich aus:

- einem Angemessenheitsbeschluss der Europäischen Kommission nach Art 45 DSGVO.
- einer Ausnahme für den bestimmten Fall nach Art 49 Abs 1 DSGVO.
- verbindlichen internen Datenschutzvorschriften nach Art 47 iVm Art 46 Abs 2 lit b DSGVO.
- Standarddatenschutzklauseln nach Art 46 Abs 2 lit c und d DSGVO.
- genehmigten Verhaltensregeln nach Art 46 Abs 2 lit e iVm Art 40 DSGVO.
- einen genehmigten Zertifizierungsmechanismus nach Art 46 Abs 2 lit f iVm Art 42 DSGVO.
- von der Datenschutzbehörde bewilligte Vertragsklauseln nach Art 46 Abs 3 lit a DSGVO.
- einer Ausnahme für den Einzelfall nach Art 49 Abs 1 Unterabsatz 2 DSGVO.

http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

Art und Zweck der Verarbeitung

Die Verarbeitung ist folgender Art: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten. Die Verarbeitung dient Zweck der im Gegenstand definierten Agenden und Tätigkeiten.

Art der Daten

Es werden jegliche Daten verarbeitet, die der Erfüllung des Auftrags bzw. des vorliegenden Vertrages dienen und dessen Erfüllung erfordern.

Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind die folgenden allgemeinen Daten:

- Kunden
- Lieferanten
- Interessenten
- Angestellte
- freie Mitarbeiter
- Werksvertragsnehmern, oder ähnliche Personen die zur Erledigung des Tagesgeschäftes in Beziehung mit unserem Unternehmen bzw. dem Kunden stehen,
- sowie Behörden, Ämter, Gemeinden oder ähnliche Institutionen die der Vertragserfüllung dienen bzw. unser Unternehmen gesetzlich verpflichtet ist in bestimmten Fällen (siehe Anhang der Gesetzestexte) Daten zu übermitteln.
- sonstige:

Kategorien der Daten

Stammdaten

- betriebliche Stammdaten
 - Firmenname Firmenwortlaut Firmenzusatz
 - Adresse Postleizahl Ort Land
 - Interne Systemnummer
 - allgemeine Telefonnummer allgemeine Email Adresse
 - Webseite
 - UID Nummer (VAT No) Firmenbuchnummer
 - Währung zur Rechnungslegung Zuordnung Bankverbindung
 - Zahlungsziel Stundensätze Kundenbetreuer intern
 - Lieferantenummer im Fremdsystem
 - Abweichende Rechnungsadresse Abweichende Lieferanschrift
 - Status aktiv/passiv (passiv = länger keine Kundenbeziehung bzw. Bestellung, gekündigter Kunde)
 - sonstige:
-
-

Personendaten

- Vorname Nachname Titel Anrede
 - Funktion im Unternehmen interne Systemnummer
 - Telefondurchwahl Fax Durchwahl Mobiltelefonnummer
 - Private Telefonnummer (nur durch persönliche Bekanntgabe)
 - Private Mobiltelefonnummer (nur durch persönliche Bekanntgabe)
 - persönliche Email Adresse im Unternehmen
 - Status aktiv/passiv (passiv = z.B. ausgeschieden aus dem Unternehmen)
 - Profitcenter Abteilung
 - sonstige:
-
-

Daten im Tagesgeschäft

- Bestelldaten Vertragsdaten Abrechnungsdaten
 - Zahlungsdaten Leistungsdaten Korrespondenz
 - sonstige:
-
-

Zahlungen

- Zahlungsausfälle

Mitarbeiterdaten

- Vorname Nachname Titel Anrede
 Funktion im Unternehmen interne Systemnummer
 Telefondurchwahl Fax Durchwahl Mobiltelefonnummer
 Private Telefonnummer (nur durch persönliche Bekanntgabe)
 Private Mobiltelefonnummer (nur durch persönliche Bekanntgabe)
 persönliche Email Adresse im Unternehmen
 Status aktiv/passiv (passiv = z.B. ausgeschieden aus dem Unternehmen)
 Profitcenter Abteilung
 sonstige:
-
-

Personaldaten zur Lohnverrechnung *

* diese werden nicht von unserem Unternehmen direkt verarbeitet, könnten aber im Bereich Email, Email Security, Email Archivierung betroffen sein.

- Sozialversicherungsnummer Kontonummern
 Private Adressdaten des Mitarbeiters (Adresse, Postleitzahl Ort)
 Versicherungsverträge (für Jahresausgleich)
 Krankmeldung
 sonstige:
-
-

Emails

- Bestandsdaten
 Name
 E-Mail-Adresse
 ggf. weitere Headerdaten
 Inhaltsdaten“ (Inhalte von E-Mails – „Body“), ...
 sonstige:
-
-

IT Dokumentation

- Interne LAN IP Adressen
 - Externe WAN IP Adressen (Public IP's)
(z.B. MX Records, TXT, CNAME, A und ähnliche Einträge)
 - DNS Daten
 - Gerätehersteller
 - Gerätelieferant
 - Modelnummer
 - Seriennummer
 - Software
 - Betriebssystem
 - Firmware Version
 - Freischaltungs_codes
 - Keys
 - Versionsnummer
 - Gerätenamen
 - Lizenzcodes
 - Token
 - Freischaltungs_codes
 - Laufwerksbezeichnungen
 - Datenordnerstruktur
 - Rechtevergaben
 - Administrative Accounts
 - Zugangsdaten zu externen Dienstleistern (z.B. Provider, SIP, Email, Cloudsysteme, ...)
 - Passwörter für Services (z.B. Email Passwörter, Webseiten, Datenbanken, Cloudservices, ...)
 - Verwendete Ports
 - Services
 - Zugangspunkte
 - Verschlüsselung
 - Zertifikate
 - Konfigurationen (z.B. Backup von Einstellungen), Snapshots
 - Nachrichtenflüsse
 - Backupflüsse
 - Prozessbeschreibungen
 - Telefonanschlüsse
 - SIP Daten
 - Mobile Daten
 - Zugangscodes für Gebäude, Alarmanlagen
 - VPN Daten
 - sonstige Zugangscodes
 - sonstige zur Vertragserfüllung notwendige Daten
 - sonstige:
-
-

Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

Wahrung der Vertraulichkeit und Verschwiegenheit: Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32ff DSGVO ergriffen hat. Konkret handelt es sich hierbei um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Einzelheiten hierzu finden sich im Anhang 1 – technische und organisatorische Maßnahmen.

Mitwirkungspflicht bei Betroffenenrechten: Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Betroffenenrechte nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer durchzuführen (sicherzustellen).

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten. Dazu gehören Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation.

Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu erstellen hat.

Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind, sofern dies gesetzlich zulässig ist und keine anderen gesetzlichen Regelungen der Offenlegung widersprechen (z.B. Archivierung von Emails).

Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, sämtliche in seinem Besitz gelangten Unterlagen, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, in dessen Auftrag zu vernichten, sofern nicht andere gesetzliche Regelungen dieser Vorgangsweise widersprechen (z.B. Archivierung von Emails).

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

Unterauftragsverhältnisse

Die Beauftragung von Subunternehmern ist grundsätzlich gestattet, sofern es zur Umsetzung und Vertragserfüllung dient z.B. im Bereich Cloud Services ist ein Dritter (Hersteller Service) heranzuziehen. Explizit erwähnt seien hier Anbieter wie Microsoft (Office 365, Azure Services, ...), Barracuda Networks (Email Archivierung, Email Security, Essentials, Backup, ...) oder Cookiebot (rechtskonforme Cookie Notice als Service, ...), Acronis (Online Backup, File Backup, FileShare, ...), F-Secure (Endpoint Protection, Software Updates, Mobile Protection...) und ähnliche von Dritten angebotene Services die der Kunde direkt nutzt oder unser Unternehmen als Subunternehmer anbietet und verwaltet.

Rechte und Pflichten des Auftraggebers

Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ebenso ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu erstellen hat.

Ebenso verpflichtet sich der Auftraggeber alle Punkte des Bereichs „Pflichten des Auftragnehmers“ auf Gegenseitigkeit einzuhalten, sofern diese den Auftraggeber ebenso verpflichten die gesetzlichen Vorgaben zu erfüllen, insbesondere die Einhaltung und Maßnahmen der in der EU Datenschutz Grundverordnung festgelegten Bereiche.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentieren oder fernmündlich bestätigen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Haftung Datenschutz

Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haftet der Auftraggeber als Gesamtschuldner. Unter diesen Voraussetzungen ersetzt der Auftraggeber dem Auftragnehmer ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

Der Auftragnehmer haftet jedoch dem Auftraggeber für Schäden, die der Auftragnehmer und seine Mitarbeiter im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen, gilt nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

Sonderkündigungsrecht

Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender, vorsätzlicher Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, sofern dies gerichtlich festgestellt wird. Dies gilt auf Gegenseitigkeit, sprich auch der Auftragnehmer kann den Hauptvertrag und diese Vereinbarung ohne Frist kündigen, wenn der Auftraggeber schwerwiegend und vorsätzlich gegen Datenschutzvorschriften verstößt.

Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer bzw. Auftraggeber die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

Sonstiges

Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Für Nebenabreden ist die Schriftform erforderlich.

Die Einrede des Zurückbehaltungsrechts wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Formalbestimmungen und anwendbares Recht Schlussbestimmungen

1. Für sämtliche Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag vereinbaren die Vertragsparteien die ausschließliche Zuständigkeit des sachlich zuständigen Gerichtes in Österreich.
2. Allfällige Änderungen und/oder Ergänzungen dieses Vertrages bedürfen der Schriftform.
3. Sollten einzelne Bestimmungen dieses Vertrages ungültig sein, so berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Diejenige Regelung, die dem beabsichtigten Zweck am nächsten kommt, soll an die Stelle der ungültigen Bestimmung treten.
4. Änderungen des gegenständlichen Vertrages sind jederzeit möglich und werden mit dem der Erstveröffentlichung folgenden Tag rechtswirksam.
5. Für diese Geheimhaltungsvereinbarung gilt österreichisches Recht. Ausgeschlossen sind seine Verweisungsnormen und das UN-Kaufrecht. Gerichtsstand für alle Streitigkeiten zu diesem Vertrag und Erfüllungsort ist jeweils Wien.
6. Verbraucher: Für Klagen gegen Verbraucher ist laut § 14 österreichischen Konsumentenschutzgesetzes Gerichtsstand deren Wohnsitz, gewöhnlicher Aufenthalt oder Beschäftigungsort, wenn dieser im Inland liegt.

Zeichnungsberechtigter VORNAME

Zeichnungsberechtigter des Vertragspartners VORNAME

Zeichnungsberechtigter NACHNAME

Zeichnungsberechtigter des Vertragspartners NACHNAME

Firmenmäßige Zeichnung (inkl. Stempel)

Firmenmäßige Zeichnung (inkl. Stempel)

Zeichnungsberechtigter UNTERSCHRIFT

Zeichnungsberechtigter UNTERSCHRIFT

Ort Datum

Ort Datum

Übermittlung der ausgefüllten Vereinbarung per Fax an **+43 1 406 00 97 DW 12**
oder ausgefüllt und gescannt per Email an: **dsgvo@mental.at**

Anhang 1 – technische und organisatorische Maßnahmen (TOM)

Die technischen und organisatorischen Maßnahmen (TOMs) unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist beiden Parteien gestattet, alternative adäquate Maßnahmen umzusetzen, soweit das gesetzlich verlangte Sicherheitsniveau nicht unterschritten wird.

Beide Parteien erklären rechtsverbindlich, dass sie alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen zu haben. Die Beschreibung der Maßnahmen (z.B. durch das gesetzlich verlangte Verarbeitungsverzeichnis sowie der technischen und organisatorischen Maßnahmen) müssen so detailliert erfolgen, dass für einen sachkundigen Dritten (z.B. Behördenvertreter zur Prüfung) allein aufgrund der Beschreibung jederzeit dies zweifelsfrei erkennbar ist.

Die Datensicherheitsmaßnahmen können von beiden Parteien der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das gesetzlich verlangte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen haben beide Parteien unverzüglich umzusetzen.

Beide Parteien ergreifen die technischen und organisatorischen Maßnahmen, damit die Rechte etwaiger betroffenen Personen nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen können.

Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen nicht oder nicht mehr genügen, benachrichtigen sich beide Parteien unverzüglich. **Der Auftragnehmer kann den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten unterstützen** (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation), **hat jedoch keinen direkten Einfluss die Einhaltung bzw. Umsetzung seitens des Auftraggebers, und ist dadurch bei Verstößen durch den Auftraggeber Schad- und klaglos zu halten.**

Beide Parteien werden nochmals darauf hingewiesen, dass Sie für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten haben und auch Ihre Interna darüber zu dokumentieren haben.

Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit (Dokumentationspflicht nach der DSGVO).

Vertraulichkeit

1. Zutrittskontrolle:
Beide Parteien verpflichten sich gegenüber dem **Schutz vor unbefugtem Zutritt** zu Datenverarbeitungsanlagen über geeignete und angemessene Maßnahmen, die zu dokumentieren sind.
2. Zugangskontrolle:
Beide Parteien verpflichten sich gegenüber dem **Schutz vor unbefugter Systembenutzung** zu Datenverarbeitungsanlagen über geeignete und angemessene Maßnahmen, die zu dokumentieren sind. Insbesondere zur Umsetzung von sicheren Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Verschlüsselung von Datenträgern mobiler Geräte.
3. Zugriffskontrolle:
Beide Parteien verpflichten sich gegenüber dem **Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen** über geeignete und angemessene Maßnahmen, die zu dokumentieren sind. Darunter fallen Maßnahmen wie, Standardprozess für Berechtigungsvergabe, periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten
4. Pseudonymisierung:
Beide Parteien verpflichten sich, sofern für die jeweilige Datenverarbeitung möglich, die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung zu entfernen, und gegebenenfalls gesondert aufzubewahren.
5. Klassifikationsschema für Daten:
Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung

Integrität

1. Weitergabekontrolle beider Parteien:
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Email Archivierung, Verschlüsselung, Virtual Private Networks (VPN)
2. Eingabekontrolle beider Parteien:
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, sofern dies technisch und wirtschaftlich umsetzbar ist.

Verfügbarkeit und Belastbarkeit

1. Verfügbarkeitskontrolle:

Beide Parteien verpflichten sich zum **Schutz gegen zufällige oder mutwillige Zerstörung** bzw. Verlust, darunter fallen Maßnahmen wie Backup-Strategie, unterbrechungsfreie Stromversorgung, Virenschutz, Firewall, URL und Applikationskontrolle, Meldewege und Notfallpläne, Standardprozesse bei Wechsel bzw. Ausscheiden von Mitarbeitern

2. Lösungsfristen:

Beide Parteien verpflichten sich **zur Einhaltung von Lösungsfristen** für Daten

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1. Datenschutz-Management

Beide Parteien verpflichten sich zum Datenschutz einschließlich regelmäßiger Mitarbeiter-Schulungen, Mitarbeiter Sensibilisierung, Incident-Response-Management (Vorfallreaktionsplan), Datenschutzfreundliche Voreinstellungen

2. Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, Auswahl des Auftragsverarbeiters, Vorabüberzeugungspflicht, Nachkontrollen

Anhang 2- Rechtsgrundlagen

Art. 6 DSGVO

Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(2) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch

a) Unionsrecht oder

b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche — um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist — unter anderem

a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,

b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,

c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,

d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,

e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

§212 des Unternehmensgesetzbuches „UGB“

Allgemeine Aufbewahrungspflicht für Geschäftsbücher, Konten und Aufzeichnungen. Unternehmen sind verpflichtet, Aufzeichnungen über alle Lieferungen von Gütern und Dienstleistungen zu führen inkl. alle innergemeinschaftlichen (EU) Anschaffungen zu dokumentieren, den gesamten Import und Export sowie alle Mehrwertsteuerrelevanten Informationen aufzubewahren. Hauptbuch, Debitorenbuchhaltung, Kreditorenbuchhaltung, (Einkaufs- und) Verkaufsadministration, Inventarlisten. Aufzeichnungen zur Auftragsvergabe

Aufbewahrungsfrist: Minimum 7 Jahre ab Ende des jeweiligen Geschäftsjahres / Kalenderjahres

§132 der Bundesabgabenordnung „BAO“ § 132 Abs. 1

Grundsätzliche Verpflichtung der Steuerpflichtigen, auf Verlangen der Steuerbehörde, alle möglicherweise steuerrelevanten Unterlagen zur Verfügung zu stellen. Verpflichtung eine dementsprechende Verwaltung zu führen, die alle Bücher, Aufzeichnungen und sonstige Datenträger umfasst und mit Hilfe derer der Steuerpflichtige jederzeit seinen Rechte und Pflichten gegenüber der Steuerbehörde nachweisen kann. Unternehmen sind verpflichtet der Steuerbehörde, auf Verlangen, relevante Informationen bezüglich der Steuerpflicht vom Dritten zugänglich zu machen. In Fällen, in denen Unternehmen gesetzlich verpflichtet sind Steuerzahlungen von Dritten einzubehalten (z.B. Mehrwertsteuer), können die Unternehmen auch aufgefordert werden, den Steuerbehörden Informationen über diese Dritten zugänglich zu machen. Ein Unternehmen ist verpflichtet, Aufzeichnungen über alle Lieferungen von Gütern und Dienstleistungen zu führen; für alle innergemeinschaftlichen (EU) Anschaffungen, den gesamten Import und Export, sowie alle relevanten Informationen für die Mehrwertsteuer.

Generelle Verpflichtung zumindest die folgenden Aufzeichnungen aufzubewahren:

- (i) Eingehende und ausgehende Mehrwertsteuerrechnungen
- (ii) Dokumente bezüglich Lieferungen und Akquisitionen innerhalb der EU
- (iii) Dokumente über Güter, die von außerhalb der EU importiert werden beziehungsweise in Länder außerhalb der EU exportiert werden

Aufbewahrungsfrist: Minimum 7 Jahre ab Ende des jeweiligen Geschäftsjahres / Kalenderjahres

EU Verordnung (EG) Nr. 450/2008

Implementierung eines Verwaltungssystems um die Anforderungen bezüglich Buchführung, Aufzeichnungen und anderen Datenträgern, wie sie in der allgemeinen Zollverordnung definiert sind, nachzukommen. Grundsätzliche Verpflichtung der Steuerpflichtigen, auf Verlangen der Zollbehörde, alle relevanten Unterlagen zur Verfügung zu stellen.

Aufbewahrungsfrist: Minimum 3 Jahre ab Ende des jeweiligen Geschäftsjahres / Kalenderjahres

§ 29 BFA-VG Übermittlung personenbezogener Daten Stand 15.02.2018

(1) Die gemäß §§ 27 Abs. 1 sowie 28 verarbeiteten Daten dürfen folgenden Empfängern übermittelt werden, soweit diese sie zur Erfüllung der ihnen übertragenen Aufgaben benötigen:

1. den Sicherheitsbehörden (§ 4 SPG),
2. den staatsanwaltschaftlichen Behörden,
3. den Zivil- und Strafgerichten und Justizanstalten,
4. den Verwaltungsgerichten der Länder,
5. dem Amt des Hochkommissärs der Vereinten Nationen für Flüchtlinge in Österreich,
6. den Vertragsparteien eines Abkommens zur Bestimmung des für die Prüfung eines Asylantrages oder eines Antrages auf internationalen Schutz zuständigen Staates oder den Behörden der Staaten, die die Dublin-Verordnung anzuwenden haben,
7. den für die Vollziehung der Genfer Flüchtlingskonvention zuständigen ausländischen Behörden, wenn die Feststellung der Identität sowie die Asylgewährung ohne eine Übermittlung an diese Behörden nicht möglich und gewährleistet ist, dass solche Daten nicht Behörden jenes Staates zugänglich werden, in dem der Asylwerber oder der Flüchtling behauptet, Verfolgung befürchten zu müssen,
8. den österreichischen Vertretungsbehörden,
9. den Behörden nach dem NAG,
10. den Staatsbürgerschaftsbehörden,
11. den Personenstandsbehörden,
12. den mit der Vollziehung des Ausländerbeschäftigungsgesetzes betrauten Behörden,
13. den Finanzstrafbehörden,
14. den Jugendwohlfahrtsträgern,
15. den Rechtsberatern (§§ 49 bis 52),
16. den Rückkehrberatern,
17. den Abgabenbehörden,
18. den Dolmetschern für Zwecke der Erbringung einer Dolmetschleistung nach § 12a.

Im Übrigen sind Übermittlungen nur zulässig, wenn dafür eine ausdrückliche gesetzliche Ermächtigung besteht.

(2) Die gemäß § 27 Abs. 1 Z 1 bis 11 und Z 19 und gemäß § 28 verarbeiteten Daten dürfen folgenden Empfängern übermittelt werden, soweit diese sie zur Erfüllung der ihnen übertragenen Aufgaben benötigen:

1. Organen des Bundes und der Länder, die Aufgaben zur Erfüllung der Grundversorgungsvereinbarung vollziehen,
2. dem Arbeitsmarktservice und den mit Betreuung und Integrationshilfe betrauten Einrichtungen der Gebietskörperschaften,
3. den Gebietskrankenkassen und dem Hauptverband der österreichischen Sozialversicherungsträger,
4. dem Bundesministerium für Europa, Integration und Äußeres, und
5. dem Österreichischen Integrationsfonds.

(3) Die gemäß § 27 Abs. 1 Z 1 bis 9 und 11 verarbeiteten Daten dürfen den Meldebehörden übermittelt werden, soweit diese sie zur Erfüllung der ihnen übertragenen Aufgaben benötigen.

Art. 4 Nr.1 DSGVO Personenbezogene Daten

Personenbezogene Daten sind nach Art. 4 Nr.1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden »betroffene Person«) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, Dies umfasst z. B. Name, Geburtsdatum, Anschrift, Einkommen, Beruf, Kfz-Kennzeichen, Konto-oder Versicherungsnummer. Auch pseudonymisierte Daten, zum Beispiel eine IP-Adresse oder Personalnummer, aus denen die betroffene Person indirekt bestimmbar wird, gelten als personenbezogener Daten.

Art. 32 DSGVO Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

§ 1487a ABGB Verjährung erbrechtlicher Ansprüche

ABGB - Allgemeines bürgerliches Gesetzbuch

(1) Das Recht, eine Erklärung des letzten Willens umzustoßen, den Geldpflichtteil zu fordern, letztwillige Bedingungen oder Belastungen von Zuwendungen anzufechten, nach erfolgter Einantwortung ein besseres oder gleiches Recht geltend zu machen, den Geschenknehmer wegen Verkürzung des Pflichtteils in Anspruch zu nehmen oder sonstige Rechte aus einem Geschäft von Todes wegen zu fordern, muss binnen drei Jahren ab Kenntnis der für das Bestehen des Anspruchs maßgebenden Tatsachen gerichtlich geltend gemacht werden. Unabhängig von dieser Kenntnis verjähren diese Rechte dreißig Jahre nach dem Tod des Verstorbenen.

(2) Abs. 1 gilt sinngemäß für die Aneignung durch den Bund.

§ 12 Abs. 1 Z 1 bis 5 AStV Alarmeinrichtungen

§ 12.

(1) Die Behörde hat Alarmeinrichtungen vorzuschreiben, wenn auf Grund besonderer Verhältnisse zu befürchten ist, dass der Eintritt einer vorhersehbaren Gefahr nicht rechtzeitig von allen Arbeitnehmer/innen wahrgenommen werden und ihnen daher im Gefahrenfall nicht ausreichend Zeit zur sicheren Flucht oder zum Ergreifen von Maßnahmen zur Gefahrenabwehr verbleiben könnte.

Solche Verhältnisse können begründet sein in

1. der Art der Arbeitsvorgänge oder Arbeitsverfahren,
2. der Art oder Menge der vorhandenen Arbeitsstoffe,
3. den vorhandenen Einrichtungen oder Arbeitsmitteln,
4. der Lage, den Abmessungen, der baulichen Gestaltung oder der Nutzungsart der Arbeitsstätte oder
5. der höchstmöglichen Anzahl der in der Arbeitsstätte anwesenden Personen.

(2) Alarmeinrichtungen, die der Alarmierung von Arbeitnehmer/innen dienen, dürfen nur außer Betrieb gesetzt werden, wenn Vorsorge getroffen ist, dass die Arbeitnehmer/innen vom Eintritt einer Gefahr unverzüglich verständigt werden können.

(3) Wenn Alarmeinrichtungen, die der Alarmierung von Arbeitnehmer/innen dienen, vorhanden sind, sind mindestens einmal jährlich während der Arbeitszeit Alarmübungen durchzuführen. Über die Durchführung sind Aufzeichnungen zu führen

Datensicherheitsmaßnahmen

§ 54. DGSVO Datenschutzgesetz & Datenschutz Anpassungsgesetz

(1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, unter Berücksichtigung der unterschiedlichen Kategorien gemäß § 37, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß § 39.

(2) Der Verantwortliche und der Auftragsverarbeiter haben im Hinblick auf die automatisierte Verarbeitung nach einer Risikobewertung Maßnahmen zu ergreifen, um folgende Zwecke zu erreichen:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle);
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (Datenträgerkontrolle);
3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle);
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle);
5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (Zugriffskontrolle);
6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle);
7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (Eingabekontrolle);
8. Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle);
9. Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können (Wiederherstellung);
10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität).

Speicher- und Aufbewahrungsfristen

Stand: 25.01.2018

<https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html>

Nachfolgend wird eine Auswahl einiger wichtiger bundesgesetzlicher (Aufbewahrungs-)Fristen im Zusammenhang mit der datenschutzrechtlichen Speicherbegrenzung („Löschkonzepte“)[1] aufgelistet.

I Rechnungswesen, Steuer- und Zollrecht:

1. Steuerrechtliche Aufbewahrungspflicht nach § 132 Abs 1 BAO: 7 Jahre darüberhinausgehend solange sie für die Abgabenbehörde in einem anhängigen Verfahren von Bedeutung sind)
2. Unternehmensrechtliche Aufbewahrungspflicht nach §§ 190, 212 UGB: 7 Jahre
3. Umsatzsteuerrechtliche Aufbewahrungspflichten nach § 18 Abs 10 UStG (Spezialbestimmung für Grundstücke): 22 Jahre
4. Umsatzsteuerrechtliche Aufbewahrungspflicht nach § 18 Abs 2 3. Unterabsatz: 7 Jahre
5. Aufzeichnungen nach § 23 Abs. 2 Zollrechts-Durchführungsgesetz: 5 Jahre

II Vertragswesen:

1. Gewährleistung nach § 933 ABGB: 2 Jahre (bewegliche Sachen), 3 Jahre (unbewegliche Sachen)
2. Kaufpreisforderung bei beweglichen Sachen nach § 1062 iVm § 1486 ABGB: 3 Jahre
3. Kaufpreisforderung bei unbeweglichen Sachen (e contrario § 1486 ABGB): 30 Jahre
4. Forderungen von Miet- und Pachtzinsen nach § 1486 ABGB: 3 Jahre
5. Ansprüche aus einem Werkvertrag nach § 1486 ABGB (wenn die Leistung im Rahmen eines gewerblichen oder sonstigen geschäftlichen Betriebs erbracht wurde): 3 Jahre
6. Allgemeiner Schadenersatz nach § 1489 ABGB (Entschädigungsklagen): 3 Jahre (wenn Schaden und Schädiger bekannt) /ansonsten **30 Jahre** (betrifft insb auch Arbeitsunfälle!)
7. Haftungsansprüche nach § 13 PHG: **10 Jahre**

III Arbeitsverhältnisse:

1. Ansprüche auf Ersatz wegen diskriminierender Ablehnung einer Bewerbung nach §§ 15 Abs 1 und 29 Abs 1 GlbG sowie § 7k Abs 1 iVm Abs 2 Z 1 BEinstG: 6 Monate
2. Ansprüche auf Ersatz von allfälligen Vorstellungskosten nach § 1486 Z 5 ABGB: 3 Jahre
3. Ansprüche des Arbeitnehmers auf Entgelt oder auf Auslagenersatz sowie des Arbeitgebers wegen darauf gewährter Vorschüsse nach § 1486 Z 5 ABGB: 3 Jahre
4. Verfolgungsverjährung wegen Unterentlohnung nach § 31 Abs 1 VStG iVm § 29 Abs 4 LSD-BG: 3 Jahre
5. Schadenersatzansprüche des Arbeitgebers gegenüber dem Arbeitnehmer aus der Dienstnehmerhaftpflicht bei leichter Fahrlässigkeit nach § 6 DHG: 6 Monate
6. Schadenersatzansprüche des Arbeitgebers gegenüber dem Arbeitnehmer aus der Dienstnehmerhaftpflicht bei grober Fahrlässigkeit oder bei Vorsatz sowie sonstige Schadenersatzansprüche des Arbeitgebers nach § 1489 ABGB: 3 Jahre
7. Daten betreffend Lohnsteuer- und Abgabepflicht nach § 132 Abs 1 BAO: 7 Jahre
8. Daten betreffend Sozialversicherungsbeitragspflicht nach § 68 ASVG: 3 bzw. 5 Jahre
9. Haftung für Abfertigungsansprüche und Betriebs-pensionen nach Betriebsübergang nach § 6 Abs 2 AVRAG: 5 Jahre
10. Ansprüche auf Ersatz wegen diskriminierender Ablehnung einer Beförderung nach §§ 15 Abs 1 und 29 Abs 1 GlbG sowie § 7k Abs 1 iVm Abs 2 Z 1 BEinstG: 6 Monate

11. Ansprüche auf Ersatz wegen diskriminierender Schlechterstellung beim Entgelt, freiwilligen Sozialleistungen, Schulungs- und Weiterbildungsmaßnahmen oder sonstigen Arbeitsbedingungen nach §§ 15 Abs 1 und 29 Abs 1 GlbG sowie § 7k Abs 1 iVm Abs 2 Z 5 BEinstG: 3 Jahre
12. Ansprüche auf Ersatz wegen diskriminierender Belästigung nach §§ 15 Abs 1 und 29 Abs 1 GlbG sowie § 7k Abs 1 iVm Abs 2 Z 4 BEinstG: 1 Jahr
13. Ansprüche auf Ersatz wegen sexueller Belästigung nach § 15 Abs 1 GlbG: 3 Jahre
14. Anspruch auf Urlaub nach § 4 Abs 5 UrlG: 2 Jahre ab Ende des Urlaubsjahres, in dem der Urlaub entstanden ist
15. Anspruch auf Urlaubersatzleistung nach § 1486 Z 5 ABGB: 3 Jahre
16. Aufzeichnungen und Berichte über Arbeitsunfälle nach § 16 ASchG: mind. 5 Jahre
17. Aufzeichnung über Überlassung von Arbeitskräften nach § 13 Abs 3 AÜG: 5 Jahre
18. Jugendlichenverzeichnis nach § 26 Abs 2 KJBG: 2 Jahre
19. Ansprüche auf Ersatz wegen diskriminierender Beendigung des Arbeitsverhältnisses nach §§ 15 Abs 1a und 29 Abs 1a GIBG sowie § 7k Abs 1 iVm Abs 2 Z 3 BEinstG: 6 Monate
20. Ersatzansprüche des Arbeitgebers bzw. des Arbeitnehmers aus einer vorzeitigen Beendigung des Arbeitsverhältnisses nach § 34 AngG bzw. § 1162d ABGB: 6 Monate
21. Anspruch auf Ausstellung eines Dienstzeugnisses nach § 1478 ABGB: 30 Jahre

IV Branchenspezifische Fristen:

1. Geldwäschebestimmungen (Aufbewahrung der verlangten Dokumente oder der Referenzangaben sowie alle Belege und Aufzeichnungen betreffend Geschäftsbeziehungen und Transaktionen) nach § 365y GewO: 5 Jahre
2. Geldwäschebestimmungen (Identifizierungsunterlagen sowie Belege und Aufzeichnungen von sämtlichen Transaktionen und Geschäftsbeziehungen) nach § 51 BiBuG: mindestens 5 Jahre
3. Geldwäschebestimmungen (Kopien erhaltener Dokumente und Informationen, Transaktionsbelege und –aufzeichnungen) nach § 21 Finanzmarkt-Geldwäschegesetz (FM-GWG) mindestens 5 Jahre
4. Aufzeichnungs- und Aufbewahrungspflichten nach § 22 WAG 2007: 5 Jahre (tritt mit 2.1.2018 außer Kraft)
5. Aufzeichnungs- und Aufbewahrungspflichten nach § 66 WAG 2007: 5 Jahre (tritt mit 2.1.2018 außer Kraft)
6. Aufzeichnungs- und Aufbewahrungspflichten nach § 33 WAG 2018: mind. 5 Jahre bis max. 7 Jahre in besonderen Umständen nach einer Verordnung durch die FMA (in Geltung ab 2.1.2018)
7. Korrespondenz und Geschäftsbücher von Auskunftseien nach § 152 GewO: 7 Jahre
8. Aufbewahrungspflicht nach § 98 VAG: 7 Jahre
9. Aufbewahrungspflichten nach § 21 Investmentfondsgesetz (InvFG): mind. 5 Jahre (auf Anordnung der FMA im Einzelfall auch länger)
10. Aufbewahrungspflicht nach § 18 Zahlungsdienstegesetz (ZaDiG): mind. 5 Jahre
11. Abfallaufzeichnungen gem. § 17 AWG iVm § 3 Abfallnachweisverordnung (ANV): 7 Jahre
12. Aufbewahrung von Begleitscheinen iSd § 18 Abs 1 AWG 2002 iVm § 8 Abfallnachweisverordnung: 7 Jahre
13. Aufbewahrungspflichten nach der Allgemeinen Strahlenschutzverordnung (AllgStrSchV) (ua §§ 16, 19, 31): 7 Jahre
14. Aufbewahrung von Verwertungsnachweisen nach der Altfahrzeugeverordnung (§§ 5, 11, 12a iVm Anlage 3): 7 Jahre
15. Aufbewahrungspflichten nach Art 36 der EU-Verordnung 1907/2006 (REACH-Verordnung): mind. 10 Jahre

16. Aufbewahrungspflicht nach § 43 Abs. 1 Chemikaliengesetz (ChemG): 7 Jahre
17. Aufbewahrungspflicht nach Art 8 der EU-Verordnung 98/2013 über die Vermarktung und Verwendung von Ausgangsstoffen für Explosivstoffe: 5 Jahre
18. Aufbewahrungspflicht nach § 7 Giftverordnung: 7 Jahre
19. Aufzeichnungen der Erzeuger und Arzneimittelgroßhändler über psychotrope Stoffe nach § 8 Psychotropenverordnung: 3 Jahre
20. Vormerkungen von Erzeugern und Arzneimittelgroßhändler nach § 8 Suchtgiftverordnung: 3 Jahre
21. Aufbewahrung der Unterlagen nach Art 3 und 4 der EU-Verordnung 111/2005 für die Überwachung des Handels mit Drogenausgangsstoffen: 3 Jahre
22. Aufbewahrungspflicht nach § 46 Arzneimittelgesetz (AMG): 15 Jahre
23. Aufbewahrungspflicht nach § 15 Abs. 1 Arzneimittelbetriebsordnung (AMBO): 5 Jahre
24. Aufbewahrungspflicht chargenbezogener Unterlagen nach § 15 Abs. 9 Arzneimittelbetriebsordnung (AMBO): 15 Jahre
25. Identifizierungspflicht innerhalb der Lieferkette nach Art 7 EU-Kosmetikverordnung 1223/2009: 3 Jahre
26. Produktinformationsdatei nach Art 11 EU-Kosmetikverordnung 1223/2009: 10 Jahre
27. Aufbewahrungspflichten nach § 11 Abs. 3 Pflanzenschutzmittelgesetz: 5 Jahre
28. Aufbewahrungspflichten nach § 2 Abs. 6 Düngemittelverordnung: 2 Jahre
29. Aufbewahrungspflichten bzgl. Ammoniumnitratdünger nach Art 26 Abs. 3 EU-Düngemittel-Verordnung: solange der Markt mit dem Düngemittel beliefert wird, und für weitere 2 Jahre, nachdem der Hersteller es vom Markt genommen hat
30. Aufbewahrung ärztlicher Aufzeichnungen und Dokumentationen gem. § 51 Abs. 3 ÄrzteG: 10 Jahre
31. Aufbewahrung von Krankengeschichten in Krankenanstalten gem. § 10 Abs. 1 Z 3 KaKuG: 30 Jahre; Röntgenbilder, Videoaufnahmen und andere Bestandteile von Krankengeschichten, deren Beweiskraft nicht 30 Jahre hindurch gegeben ist, sowie bei ambulanten Behandlungen: 10 Jahre
32. Aufbewahrung von Dokumentationen und Zustimmungserklärungen im Zusammenhang mit medizinisch unterstützter Fortpflanzung gem. § 18 Fortpflanzungsmedizingesetz (FMedG): 30 Jahre
33. Dokumentationen im Zusammenhang mit Gewebeentnahmen gem. §§ 5, 16 Gewebesicherheitsgesetz (GSG): mind. 10 Jahre; bzgl. Teile, die für eine lückenlose Rückverfolgbarkeit unerlässlich sind: 30 Jahre
34. Dokumentation bei Organentnahmen und –transplantationen gem. §§ 3e, 3f KaKuG: 30 Jahre
35. Dokumentation von Eingängen, Abgängen und Anwendungen von Blut oder Blutbeständen im Rahmen des Blutdepots gem. § 8f KaKuG: 30 Jahre
36. Behandlungsdokumentation von medizinischen Masseuren und Heilmasseuren nach § 3 MMHmG: 10 Jahre
37. Dokumentationspflichten nach der Verordnung über die Konformitätsbewertung von Medizinprodukten: 5 bzw 15 Jahre
38. Implantatregister von Medizinproduktebetreibern nach § 10 Medizinproduktebetreiberverordnung: 30 Jahre
39. Aufbewahrung des Haushaltsbuches sowie der Belege für Personenbetreuer nach § 160 GewO: 2 Jahre
40. Gästeverzeichnisblattsammlungen nach § 19 Abs. 5 Meldegesetz-Durchführungsverordnung: 7 Jahre
41. Wochenberichtsblatt nach § 4 Abs 4 Wochenberichtsblatt-Verordnung (Ausbildung von Jugendlichen zu Kraftfahrern): 1 Jahr nach Beendigung des Lehrverhältnisses

42. Aufbewahrung von Fahrtenbüchern, Lenkzeiten, udgl nach den §§ 17 Abs 5, 17b AZG: 24 Monate
43. Aufbewahrung der Schaublätter der Fahrtschreiber bzw. der vom Kontrollgerät aufgezeichneten Daten nach § 103 Abs. 4 KFG: 2 Jahre
44. Aufbewahrung von Arbeitszeitaufzeichnungen des Zugpersonals nach § 18k AZG: 1 Jahr
45. Aufbewahrungspflicht für Fahrtenbücher zum Nachweis der Verwendung von Probekennzeichen nach § 45 Abs. 6 KFG: 3 Jahre
46. Aufbewahrungspflichten bzgl. Geschwindigkeitsmesser, Fahrtschreiber und Wegstreckenmesser nach § 24 KFG: 2 Jahre
47. Aufbewahrungspflicht des Typenscheinverzeichnisses nach § 30 KFG: 10 Jahre
48. Aufbewahrungspflicht nach § 102 Abs. 4 LFG: 2 Jahre
49. Aufbewahrung von Aufzeichnungen nach § 169 LFG: 1 Jahr
50. Arbeitszeitaufzeichnungen inkl. Ruhezeiten nach § 10 Schiffsbesatzungsverordnung (Schiffstagebuch und Bordbuch): 6 Monate
51. Aufzeichnungen über den Ausbildungsgang eines jeden Fahrschülers nach § 64b Abs. 8 und 8a Kraftfahrgesetz-Durchführungsverordnung (KDV): 3 Jahre
52. Aufbewahrungspflichten des Arbeitskräfteüberlassers betreffend überlassene Arbeitnehmer nach § 13 AÜG: 5 Jahre
53. Aufzeichnungspflichten für Betreiber von Tierheimen und Tierpensionen nach 29 Tierschutzgesetz (Vormerkbuch): 3 Jahre
54. Aufzeichnungen nach § 13 Tierhaltungs-Gewerbeverordnung: 3 Jahre