Vertrag zur Auftragsverarbeitung
Dienstleitungen & Services

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.

Dies gilt auch, sofern der Auftrag nicht ausdrücklich auf diese Vereinbarung zur Auftragsverarbeitung verweist.

Der Auftragnehmer übernimmt folgende Verarbeitungen:

❑ Verkauf & Implementierung von IT Infrastruktur

❑ Verkauf & Implementierung von Online Services und Cloudlösungen

z.B. Email Archivierung, Office 365, Cookiebot, …

❑ Allgemeine Wartung der IT Infrastruktur

❑ Dokumentation der IT Infrastruktur

❑ Remote Support

❑ Email Security Service

❑ Endpoint Security Service

❑ Webhosting auf MAG/UPC Shared Host

❑ Erstellung und Wartung von Webseiten

❑ ERP Systeme Magendas, BOS auf File Maker Basis

❑ Datenrettungsaufträge

❑ Sonstige Dienstleistungen:

_____

_____

_____

_____

_____

_____

_____

_____

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. Wartungsvertag, 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

❑ Werksvertragsnehmen, 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
❑ Lieferantennummer 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
❑ DNS Daten
❑ Externe WAN IP Adressen (Public IP´s)
(z.B. MX Records, TXT, CNAME, A und ähnliche Einträge)

❑ Gerätehersteller
❑ Gerätelieferant
❑ Modelnummer
❑ Seriennummer
❑ Firmware Version
❑ Software
❑ Betriebssystem
❑ Versionsnummer
❑ Freischaltungscodes
❑ Keys
❑ Token
❑ Gerätenamen
❑ Lizenzcodes
❑ Freischaltungscodes

❑ 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

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

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

7. 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.

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

9. 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).

10. 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 Vorgangweise 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.

11. 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

1. 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

1. 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 Auftragsnehmers“ 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.

2. 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.

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

Vergütung

Die Vergütung des Auftragnehmers ist anderswertig (z.B. Wartungsvertrag) geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

Haftung

1. 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.

2. 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.

3. Nummern (2) gilt nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

Sonderkündigungsrecht

1. 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.

2. 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.

3. 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

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.

1. 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.

2. 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.

3. 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.

4. Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen nicht oder nicht mehr genügen, benachrichtigten 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.**

5. **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.**

6. 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. Löschungsfristen:
   Beide Parteien verpflichten sich **zur Einhaltung von Löschfristen** 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 Länderaußerhalb 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 Störungsfall 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 Abgabenpflicht 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 Sozial-leistungen, Schulungs- und Weiterbildungs-maß-nahmen 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 Urlaubsersatzleistung 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 GlBG 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 Auskunfteien 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