im zeichen der zukunft

AUFTRAGSVERARBEITERVERTRAG

Abgeschlossen zwischen

.....

.....

.....

.....

(im Folgenden kurz ***Verantwortlicher***)

und

Zimmermann
Ganahl Aktiengesellschaft
Obere Lend 14
6060 Hall in Tirol
Österreich

(im Folgenden kurz ***Auftragsverarbeiter*)**.

Stand: 2018.10.13

1. Beschreibung der Datenverarbeitung

1.1. Der Auftragsverarbeiter übernimmt folgende Datenverarbeitungen:

Der Verantwortliche hat den Auftragsverarbeiter mit der Sammlung, Sortierung, Aufbereitung sowie Verwertung von Altpapier und nicht gefährlichen Abfällen bzw. für die Akten-, Datenvernichtung des übergebenen Materials beauftragt.

1.2. Die Verarbeitung beginnt ab gegenseitiger Unterzeichnung dieses Auftragsverarbeitervertrags und erfolgt auf unbestimmte Zeit bis zur Beendigung dieses Vertrags.

1.3. Die Datenverarbeitung ist folgender Art:

- Erfassen, Ordnen, Löschen oder Vernichtung von Daten.

1.4. Die Datenverarbeitung dient folgendem Zweck:

- Erbringung der zugesicherten Leistungen und Erfüllung diverser gesetzlicher Verpflichtungen

1.5. Es werden folgende personenbezogene Daten bzw. Datenkategorien verarbeitet:

- Name
- Anrede/Geschlecht
- Anschrift
- Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben
- Firmenbuchdaten
- Daten zur Bonität
- Sperrkennzeichen
- Zuordnung zu einer bestimmten Kundenkategorie (zB Abfallverband, einschließlich regionale Zuordnung, usw)
- Zugehörigkeit zu einem bestimmten Konzern
- Gegenstand der Leistung
- Bonus-, Provisionsdaten und dergleichen
- Kontaktperson beim Betroffenen zur Abwicklung der Leistung
- Bei der Leistungserbringung mitwirkende Dritte einschließlich Angaben über die Art der Mitwirkung
- Leistungsbedingungen (einschließlich Angaben über Ort der Leistung, Verpackung, usw)
- Daten zur Versicherung der Leistung und zu ihrer Finanzierung
- Daten zur Steuerpflicht und Steuerberechnung
- Zahlungsbedingungen
- Bankverbindung
- Daten zum Kreditmanagement
- Daten zum Zahlungs- oder Leistungsverhalten des Betroffenen
- Mahndaten/Klagsdaten
- Konto- und Belegdaten
- Leistungsspezifische Aufwände und Erträge
- Sonderhauptbuchvorgänge (zB Einzelwertberichtigung, Wechselforderung, Anzahlung, Bankgarantie)
- Datenvernichtung nach ÖNORM, DIN und EN-Norm (Akten, Filme, Festplatten)
- Abfallmengen

1.6. Von der Verarbeitung betroffen sind folgende Personen bzw. Personengruppen:

- Mitarbeiter des Verantwortlichen
- Geschäftspartner des Verantwortlichen

Die Datenverarbeitung durch den Auftragsverarbeiter erfolgt ausschließlich innerhalb der EU oder des EWR.

2. Allgemeine Pflichten des Auftragsverarbeiters

2.1. Der Auftragsverarbeiter gewährleistet, dass sich Personen, die Kenntnis von den im Auftrag verarbeiteten Daten haben oder erhalten können, vor Verarbeitung bzw. Kenntnis dieser Daten schriftlich zur Vertraulichkeit und zur Einhaltung des Datengeheimnisses nach § 6 DSG verpflichten, sofern diese nicht ohnedies einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

2.2. Der Auftragsverarbeiter wird den Verantwortlichen nach Möglichkeit sowohl mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung und Erfüllung von Anträgen betroffener Personen gemäß Kapitel III der DSGVO als auch bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO Pflichten unterstützen, damit der Verantwortliche seinen diesbezüglichen Pflichten nachkommen kann.

2.3. Der Auftragsverarbeiter wird den Verantwortlichen dabei unterstützen und alle erforderlichen Maßnahmen ergreifen, damit beide gemeinsam geeignete technische und organisatorische Maßnahmen treffen, um ein dem jeweiligen Risiko angemessenes Schutzniveau zu gewährleisten.

2.4. Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten des Verantwortlichen (ungeachtet, ob dieser data breach auf den Auftragsverarbeiter oder den Verantwortlichen oder einen sonstigen Dritten zurückzuführen ist) bekannt wird, wird er diese dem Verantwortlichen unverzüglich melden, die bekanntgewordene Verletzung einschließlich ihrer Auswirkungen und der getroffenen Abhilfemaßnahmen dokumentieren und dem Verantwortlichen diese Dokumentation zur Verfügung stellen. Darüber hinaus wird er den Verantwortlich bei dessen Meldung allfälliger data breaches an die Aufsichtsbehörde unterstützen und alle damit im Zusammenhang stehenden Informationen erteilen. Weiter wird er dem Verantwortlichen alle notwendigen Informationen bereitstellen, die allenfalls notwendig sind, damit dieser die vom data breach betroffene(n) Person(en) unverzüglich von der Verletzung benachrichtigen kann.

3. Technische und organisatorische Pflichten des Auftragsverarbeiters

3.1. Es gelten die in Anlage A beschriebenen technischen und organisatorischen (Sicherheits-)maßnahmen, die im Laufe des Vertragsverhältnisses einvernehmlich der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden können.

3.2. Der Auftragsverarbeiter wird die vollständige Umsetzung der vereinbarten technischen und organisatorischen Datenschutzmaßnahmen regelmäßig prüfen und dem Verantwortlichen die Ausübung seiner Kontrollrechte in diesem Zusammenhang ermöglichen, soweit dem keine berufsrechtlichen Pflichten zur Verschwiegenheit oder etwaige Vertraulichkeitsverpflichtungen entgegenstehen.

4. Subauftragsvergabe

4.1. Die Beauftragung bzw. Inanspruchnahme von Subauftragsverarbeitern (im Folgenden Subauftragnehmer) ist dem Auftragsverarbeiter prinzipiell gestattet, er wird diese dem Verantwortlichen jedoch mitteilen und dem Verantwortlichen steht ein Widerspruchsrecht zu.

4.2. Der Auftragsverarbeiter wird nur solche Subauftragnehmer auswählen, die dazu geeignet und auch verpflichtet sind, die Verarbeitung personenbezogener Daten entsprechend den Anforderungen der DSGVO und des DSG durchzuführen. Etwaige Kontrollrechte bei den Subauftragnehmern sind vom Auftragsverarbeiter auszuführen, wobei Art und Umfang der Kontrollen durch den Verantwortlichen über dessen Weisungsrecht maßgeblich bestimmt werden (können).

4.3. Nichtsdestotrotz ist der Verantwortliche auch berechtigt, jederzeit Einsicht in die zwischen dem Auftragsverarbeiter und dem Subauftragsnehmer abgeschlossenen Verträge zu nehmen bzw. durch vom Verantwortlichen bestimmte Dritte, die keine unmittelbaren Wettbewerber des Auftragsverarbeiters darstellen, nehmen zu lassen.

4.4. Die Weiterleitung von personenbezogenen Daten, die der Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeitet, an den Subauftragnehmer ist dem Auftragsverarbeiter erst gestattet, nachdem sich dieser davon überzeugt hat, dass der Subauftragnehmer die ihn nach diesem Punkt 4. treffenden Pflichten zur Gänze erfüllt hat.

5. Informationspflichten des Auftragsverarbeiters und Kontrollrechte des Verantwortlichen

5.1. Der Auftragsverarbeiter ist verpflichtet, dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der dem Auftragsverarbeiter in diesem Vertrag auferlegten Pflichten zur Verfügung zu stellen.

5.2. Sollte der Auftragsverarbeiter der Auffassung sein, dass eine vom Verantwortlichen erteilte Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder deren Mitgliedstaaten verstößt, so hat er dies dem Verantwortlichen unverzüglich und begründet mitzuteilen.

5.3. Der Verantwortliche ist berechtigt, die Einhaltung sämtlicher maßgeblichen datenschutzrechtlichen Vorschriften sowie die Einhaltung der vertraglichen Bestimmungen selbst oder durch Dritte beim Auftragsverarbeiter zu kontrollieren. Dieses Kontrollrecht umfasst insbesondere das Recht zur Einholung entsprechender Auskünften, zu deren Erteilung der Auftragsverarbeiter verpflichtet ist, sowie das Recht, sich entsprechende Belege/Zertifikate oder sonstige Bescheinigungen Dritter vorlegen zu lassen die entsprechend als Nachweis dienen. Über Aufforderung ist der Auftragsverarbeiter bzw. der Subauftragnehmer verpflichtet, die dafür erforderlichen Auskünfte zu erteilen. In begründeten Fällen kann der Verantwortliche sein Kontrollrecht auch vor Ort des Auftragsverarbeiters ausüben, wobei dabei berufsrechtliche Verschwiegenheitspflichten und Vertraulichkeitsvereinbarungen zu beachten sind.

6. Vergütung

6.1. Für die Erbringung der Leistungen unter diesem Vertrag erfolgt keine gesonderte Vergütung oder Kostenerstattung zugunsten des Auftragsverarbeiters. Die Vertragsparteien sind sich einig, dass die Leistungen unter diesem Vertrag durch das im Dienstleistungsangebot vereinbarte Entgelt mitabgegolten sind.

7. Vertragsbeendigung

7.1. Dieser Vertrag ist in seiner Dauer von dem ihm zugrundeliegenden Dienstleistungsangebot abhängig.

7.2. Ungeachtet des Fortbestands des Dienstleistungsangebots ist der Verantwortliche berechtigt, diesen Vertrag ohne Einhaltung von Kündigungsfristen oder Kündigungsterminen aus wichtigem Grund mit sofortiger Wirkung zu beenden.

7.3. Bei Beendigung des Vertrags (oder auch jederzeit vorher über entsprechendes Verlangen des Verantwortlichen) wird der Auftragsverarbeiter die im Auftrag verarbeiteten Daten (einschließlich allfälliger Kopien) nach freier Wahl des Verantwortlichen entweder selbst vernichten oder zur Gänze an den Verantwortlichen übergeben, sofern dem keine gesetzliche Pflicht zur Aufbewahrung entgegensteht. Die Vernichtung hat in einer Weise zu erfolgen, dass eine auch bloß teilweise Wiederherstellung der gelöschten Daten nicht oder nur mit technisch und wirtschaftlich unvertretbarem Aufwand möglich ist.

7.4. Der Auftragsverarbeiter ist gleichermaßen verpflichtet, die Vernichtung oder Übergabe durch allfällige Subauftragnehmer herbeizuführen.

8. Schlussbestimmungen

8.1. Änderungen und Ergänzungen dieses Vertrags einschließlich dieses Punktes bedürfen der Schriftform sowie der Unterschrift beider Vertragsparteien.

8.2. Sollten einzelne Bestimmungen dieses Vertrags ungültig oder undurchsetzbar sein oder werden, so bleibt der Restvertrag davon unberührt. Diese Bestimmungen gelten als durch gültige und durchsetzbare Regelungen ersetzt, die den von den Vertragsparteien beabsichtigten wirtschaftlichen Zweck am ehesten erreichen.

8.3. Dieser Vertrag verfügt über eine Anlage A (Technisch und Organisatorische Sicherheitsmaßnahmen), die einen integrierten Bestandteil dieses Vertrags bildet.

Dr. Thomas Baumüller MBA

Hall i. Tirol 12. Dez. 2018

Ort, Datum:

zimmermann
Ganahl Aktiengesellschaft
A-6060 Hall i.T., Obere Lend 14

Dr. Thomas Baumüller

Auftragsverarbeiter - Zimmermann Ganahl AG

Ort, Datum:

Verantwortlicher - Kunde

Anlage A: TOMs (Technische und Organisatorische Sicherheitsmaßnahmen)

Anlage A: Technische und Organisatorische Sicherheitsmaßnahmen (TOMs) der Zimmermann Ganahl Aktiengesellschaft

Allgemeines

Geeignete Maßnahmen

- Dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Datenverarbeitung
- Verfügbarkeit der personenbezogenen Daten und Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherstellbar
- Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung
- Schulung und Einhaltung genehmigter Verhaltensregeln und unternehmensweiter Richtlinien
- Fachgerechte Entsorgung von nicht mehr benötigten Datenträgern und Akten
- Sicherstellung, dass die dem Verantwortlichen unterstellten natürlichen Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten

Zutrittskontrolle

Es dürfen nur Befugte zu den Räumen mit Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, Zutritt haben.

Geeignete Maßnahmen

- Zugangskontrollsystem
- Protokollierung und Review von Zutritten in Serverräumen
- Schlüsselregelung (Schlüsselausgabe etc.)
- Protokollierung der Besucher
- Sorgfältige Auswahl von Wachpersonal
- Chipkarten-/Transponder-Schließsystem im Zentralgebäude und manuelles Schließsystem als Mindeststandard
- Videoüberwachung der Zugänge
- Sicherheitsschlösser
- Absicherung durch ein Ausweislesesystem in ausgewählten Bereichen
- Zutrittsregelung und Protokollierung im Zentralarchiv für Papierakten & Datenträger
- Sorgfältige Auswahl von Reinigungspersonal

Zugangskontrolle

Mit den Maßnahmen der Zugangskontrolle soll sichergestellt werden, dass nur Befugte Zugang zu den Datenverarbeitungseinrichtungen haben. Hier geht es nicht um die körperliche Zutrittskontrolle, sondern um den technischen/organisatorischen Zugang zu Datenverarbeitungssystemen bzw. deren Nutzungsmöglichkeit.

Geeignete Maßnahmen

- Zuordnung von individuellen Benutzerrechten
- Authentifikation mit individuellem Benutzernamen / Passwort und Smartcard
- Versperrte Schränke für Papierakten
- Einsatz einer Hardware-Firewall
- Erstellen, Zuordnung und Entzug von individuellen Benutzerprofilen mit jeweiligen Zugriffsberechtigungen
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie für Fernzugriffe
- Passwortrichtlinie inkl. Passwortlänge, regelmäßiger Passwortwechsel, automatische Sperrung von Benutzerprofilen bei Falscheingabe von Passwörter

- Automatische Sperrung von Eingabegeräten
- Verschlüsselung von mobilen Datenträgern
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz einer Software-Firewall
- Möglichkeit der Fernlöschung von Mobilen Geräten

Zugriffskontrolle

Ziel der Zugriffskontrolle ist es, mithilfe geeigneter Maßnahmen sicherzustellen, dass im Rahmen der Datenverarbeitung durch die Mitarbeiter nur auf die personenbezogenen Daten zugegriffen werden kann, für die sie eine Zugriffsberechtigung besitzen. Dritte dürfen keinen unbefugten Zugriff auf die Daten hinsichtlich Verarbeitung, Nutzung und Speicherung haben und auch eine unbefugte Entfernung der Daten darf nicht möglich sein.

Geeignete Maßnahmen

- Differenzierung von Zugriffen auf Basis von Rollen und Funktionen im Unternehmen
- Berechtigungsreview von Benutzern mit kritischen Berechtigungen
- Anzahl der Administratoren auf das Notwendigste reduziert
- Physische Löschung von Datenträgern vor Wiederverwendung
- Einsatz von Aktenvernichtern bzw. geeigneten Dienstleistern
- Verschlüsselung von Daten und Datenträgern (clientseitig)
- Regelmäßige Auswertung sämtlicher Logfiles auf Angriffe und Datenlecks
- Monitoring der Server und sonstiger IT-Systeme in Echtzeit
- Konzept für Zugriffsregelungen für bestimmte Personengruppen (Fremdfirmen, Besucher) und in Ausnahmesituationen
- Möglichkeit für IT Nutzer, Zugriffe durch andere einzuschränken
- Sichere Aufbewahrung von Datenträgern
- Ordnungsgemäße Vernichtung von nicht mehr benötigten Datenträgern
- Aktuelle Verschlüsselungssoftware
- Verwaltung der Zugriffsrechte durch den Systemadministrator
- Aktuelle Firewall, Viren- und Trojanerschutz
- Sensibilisierung und Schulung der Mitarbeiter

Weitergabekontrolle

Ziel der Weitergabekontrolle ist es, durch geeignete Maßnahmen personenbezogene Daten bei der Übertragung und beim Transport der Datenträger zu schützen.

Geeignete Maßnahmen

Einrichtung von Standleitungen bzw. VPN-Tunneln, Protokolle und Überwachung von Datenübertragungen

Eingabekontrolle

Ziel der Eingabekontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, dass die näheren Umstände der Dateneingabe nachträglich überprüft und festgestellt werden können.

Geeignete Maßnahmen

Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen); Protokollierung/Dokumentation der Eingabe, Änderung, Entfernung und Löschung von Daten; Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts; Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

Verfügbarkeitskontrolle

Ziel der Verfügbarkeitskontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, dass geschützte Daten nicht zerstört oder verloren gehen und stets verfügbar sind.

Geeignete Maßnahmen

Erstellen regelmäßiger Backups, Feuerlöschgeräte in Serverräumen und Archiven, Unterbrechungsfreie Stromversorgung (USV), Feuer- und Rauchmeldeanlagen, Testen von Datenwiederherstellung, Festgelegte Aufbewahrungsfristen, Klimaanlage in Serverräumen, Geräte zur Überwachung von Temperatur in Serverräumen, Existenz eines aktuellen Notfallplans, Existenz eines Backup- & Recoverykonzeptes, Serverräume nicht unter flüssigkeitsführenden Leitungen und unter der Wassergrenze, Spiegeln von Festplatten, Einsatz aktueller Anti-Virensoftware

Möglichkeit differenzierter Verarbeitung

Es muss sichergestellt werden, dass Daten, die für verschiedene Zwecke erhoben wurden, auch für die jeweiligen Zwecke getrennt verarbeitet werden können.

Geeignete Maßnahmen

Erstellung eines Berechtigungs-/Zugriffskonzepts, Festlegung von Datenbankrechten, Trennung von Produktiv- und Testsystem