Anlage 2
- VEREINBARUNG ÜBER DIE DATENVERARBEITUNG.

Smart Customer Master Data Management - UNISERV Provided Infrastructure ("UPI")

der Firma Uniserv GmbH, Rastatter Str. 13, 75179 Pforzheim

Stand: Mai 2018

1. Allgemeines

1.1. Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Smart Customer MDM Vertrag (nachfolgend „Hauptvertrag“) in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Diese Anlage gilt für Personenbezogene Daten, die von UNISERV und seinen Unterauftragsverarbeitern im Zusammenhang mit der CDH Solution UPI verarbeitet werden. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrages.

1.2. Die **Anhänge 1 und 2** sind Bestandteil dieser Anlage. Sie legen den vereinbarten Gegenstand, die Art und den Zweck der Verarbeitung, die Art der Personenbezogenen Daten, die Kategorien der Betroffenen Personen und die anzuwendenden technischen und organisatorischen Maßnahmen fest.

1.3. UNISERV und der Kunde sind sich darüber einig, dass es in der Verantwortung jeder Partei liegt, die Anforderungen zu überprüfen und zu übernehmen, die durch die Datenschutz Grundverordnung 2016/679 ("DSGVO") an die Verantwortlichen und Auftragsverarbeiter gestellt werden, insbesondere in Bezug auf die Artikel 28 und 32 bis 36 der DSGVO, wenn und soweit sie auf die Personenbezogenen Daten des Kunden/der Verantwortlichen anwendbar sind, die im Rahmen der Leistungserbringung verarbeitet werden.

1.4. UNISERV wird als Auftragsverarbeiter tätig und der Kunde, und die Rechtspersonen, denen er die Nutzung der CDH Solution gestattet, handeln als Verantwortliche im Rahmen des DPA. Der Kunde ist einziger Kontaktpunkt und allein verantwortlich für die Einholung aller relevanten Genehmigungen, Zustimmungen und Einwilligungen für die Verarbeitung Personenbezogener Daten gemäß dieser Anlage, soweit erforderlich, der Zustimmung der Verantwortlichen zum Einsatz von UNISERV als Auftragsverarbeiter. Soweit vom Kunde Genehmigungen, Zustimmungen, Weisungen oder Einwilligungen erteilt werden, werden diese nicht nur im Namen des Kunden, sondern auch im Namen anderer Verantwortlicher, die die CDH Solution nutzen, erteilt. Wenn UNISERV den Kunden informiert oder ihm Meldungen übermittelt, gelten diese Informationen oder Meldungen als von denjenigen Verantwortlichen erhalten, denen der Kunde die Nutzung der CDH Solution gestattet hat. Es liegt in der Verantwortung des Kunden, diese Informationen und Meldungen an die entsprechenden Verantwortlichen weiterzuleiten.

2. SICHERHEIT DER VERARBEITUNG

2.1. UNISERV hat die in **Anhang 2** aufgeführten technischen und organisatorischen Maßnahmen umgesetzt und wird diese anwenden. Der Kunde hat diese Maßnahmen geprüft und erklärt sich damit einverstanden, die Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, des Kontextes und der Zwecke der Verarbeitung Personenbezogener Daten angemessen sind.

2.2. UNISERV wendet die in **Anhang 2** beschriebenen technischen und organisatorischen Maßnahmen auf alle UNISERV Kunden gleichermaßen an, die im selben Rechenzentrum gehostet werden und die CDH Solution UPI erhalten. UNISERV kann die in Anhang 2 aufgeführten Maßnahmen jederzeit ohne Vorankündigung ändern, solange sie ein vergleichbares oder besseres Sicherheitsniveau aufrechterhält. Einzelne Maßnahmen können durch neue Maßnahmen ersetzt werden, die dem gleichen Zweck dienen, ohne das Sicherheitslevel zum Schutz Personenbezogener Daten zu beeinträchtigen.

3. UNISERV PFLICHTEN

3.1. UNISERV wird Personenbezogene Daten nur in Übereinstimmung mit den dokumentierten Weisungen des Kunden verarbeiten. Die Vereinbarung (einschließlich dieser Anlage) stellt eine solche dokumentierte Erst-Weisung dar, und jede Nutzung des CDH Solution stellt dann eine weitere Weisung dar. UNISERV unternimmt alle zumutbaren Anstrengungen, um allen anderen Weisungen des Kunden zu folgen, soweit sie nach Datenschutzrecht erforderlich, technisch durchführbar und ohne Änderungen an der CDH Solution möglich sind. Sollte eine der vorgenannten Ausnahmen zu treffen oder UNISERV anderweitig einer Weisung nicht nachkommen können oder der Meinung sein, dass eine Weisung gegen das Datenschutzrecht verstößt, wird UNISERV den Kunden benachrichtigen (E-Mail erlaubt).

3.2. UNISERV kann auch Personenbezogene Daten verarbeiten, sofern dies nach geltendem Recht erforderlich ist. In einem solchen Fall wird UNISERV den Kunden vor der Verarbeitung über diese rechtliche Anforderung informieren, es sei denn, das betreffende Recht verbietet solche Informationen wegen eines wichtigen öffentlichen Interesses.

3.3. Zur Verarbeitung Personenbezogener Daten gewährt UNISERV und seine Unterauftragsverarbeiter nur befugten Personen Zugang, die sich zur Vertraulichkeit verpflichtet haben. UNISERV und seine Unterauftragsverarbeiter werden die Personen, die Zugang zu Personenbezogenen Daten haben, regelmäßig in Bezug auf die anwendbaren Datensicherheits- und Datenschutzmaßnahmen schulen.

3.4. Auf Wunsch des Kunden wird UNISERV angemessen mit dem Kunden zusammenarbeiten, um Anfragen von Betroffenen Personen oder Aufsichtsbehörden bezüglich der Verarbeitung Personenbezogener Daten durch UNISERV oder einer Verletzung Personenbezogener Daten zu bearbeiten. UNISERV wird den Kunden so bald wie zumutbar möglich über jede Anfrage informieren, die UNISERV von einer Betroffenen Person im Zusammenhang mit der Verarbeitung Personenbezogener Daten erhalten hat, ohne selbst auf diese Anfrage ohne weitere Weisungen des

Kunden zu antworten. UNISERV stellt Funktionen zur Verfügung, die die Fähigkeit des Kunden unterstützen, Personenbezogene Daten aus der CDH Solution zu berichtigen oder zu löschen oder die Verarbeitung gemäß dem Datenschutzgesetz einzuschränken. Wenn eine solche Funktionalität nicht zur Verfügung gestellt wird, wird UNISERV gemäß den Weisungen des Kunden und dem Datenschutzrecht Personenbezogene Daten berichtigen oder löschen oder deren Verarbeitung einschränken.

3.5. UNISERV wird dem Kunden eine Verletzung des Schutzes Personenbezogener Daten unverzüglich nach Kenntniserlangung melden und ihm angemessene Informationen zur Verfügung stellen, um ihn bei der Erfüllung seiner Verpflichtungen zur Meldung einer Verletzung des Schutzes Personenbezogener Daten gemäß den Anforderungen des Datenschutzrechts zu unterstützen. UNISERV kann diese Informationen in Abschnitten zur Verfügung stellen, je nachdem, zu welchem Zeitpunkt sie verfügbar werden. Eine solche Meldung ist kein Eingeständnis des Verschuldens oder der Haftung von UNISERV oder dahingehend auszulegen.

3.6. Wenn der Kunden (oder seine für die Verarbeitung Verantwortlichen) gemäß Datenschutzrecht verpflichtet sind, eine Datenschutz-Folgenabschätzung oder eine vorherige Konsultation mit einer Aufsichtsbehörde durchzuführen, stellt UNISERV auf Wunsch des Kunden diejenigen Dokumente zur Verfügung, die für die CDH Solution UPI allgemein verfügbar sind (z.B. dieses DPA, die Vereinbarung, Auditberichte oder Zertifizierungen). Jede zusätzliche Unterstützung wird zwischen den Vertragsparteien einvernehmlich vereinbart.

4. DATEN-EXPORT UND LÖSCHUNG

4.1. Während der Laufzeit und gemäß den Regelungen der Vereinbarung kann der Kunde jederzeit auf seine Personenbezogenen Daten zugreifen. Der Kunde kann seine Personenbezogenen Daten entnehmen und in einem Standardformat exportieren. Abruf und Export können technischen Beschränkungen und Voraussetzungen unterliegen. In diesem Fall werden sich UNISERV und Kunde auf eine angemessene Methode zur Ermöglichung des Zugriffs des Kunden auf die Personenbezogenen Daten verständigen.

4.2. Vor Vertragsende kann der Kunde die jeweils verfügbaren UNISERV Tools verwenden, um einen abschließenden Export der Personenbezogenen Daten aus der CDH Solution durchzuführen (was einer Rückgabe der Personenbezogenen Daten entspricht). Der Kunde erteilt UNISERV hiermit die Weisung, nach Vertragsende die auf den zum Hosting des CDH eingesetzten Servern verbliebenen Personenbezogenen Daten innerhalb einer angemessenen Zeit gemäß dem Datenschutzrecht zu löschen (spätestens innerhalb von 6 Monaten), es sei denn, deren Aufbewahrung ist nach anwendbarem Recht erforderlich.

5. ZERTIFIZIERUNGEN UND AUDITS

5.1. Der Kunde oder ein von ihm beauftragter unabhängiger externer und für UNISERV zumutbarer Prüfer (unter Ausschluss von Prüfern, die entweder Wettbewerber der UNISERV sind, oder nicht angemessen qualifiziert oder unabhängig sind) können die Kontrollumgebung und die Sicherheitspraktiken von UNISERV im Hinblick auf die von UNISERV verarbeiteten Personenbezogenen Daten prüfen, wenn:

(a) UNISERV keinen ausreichenden Nachweis über die Einhaltung der technischen und organisatorischen Maßnahmen, die die Produktivsysteme der CDH Solution schützen, erbracht hat. Dieser Nachweis kann durch (i) eine Zertifizierung über die Einhaltung von ISO 27001 oder anderer Standards (Umfang gemäß der Regelung im Zertifikat) oder (ii) einen gültigen Bericht nach ISAE 3402 und/oder ISAE 3000 oder einen anderen SOC1-3 Auditbericht erfolgen. Auf Anforderung des Kunden sind die Auditberichte oder ISO-Zertifizierungen über UNISERV verfügbar.

(b) Eine Verletzung des Schutzes Personenbezogener Daten vorliegt;

(c) eine Prüfung offiziell durch eine Aufsichtsbehörde des Kunden; oder

(d) der Kunde gemäß zwingendem Datenschutzrecht über ein direktes Auditrecht verfügt, und der Kunde nur einmal binnen eines 12-Monatszeitraums auditiert, es sei den zwingendes Datenschutzrecht verlangt häufigere Audits.

5.2. Jeder andere Verantwortliche darf die Kontrollumgebung und die Sicherheitspraktiken von UNISERV, die für die von UNISERV verarbeiteten Personenbezogenen Daten relevant sind, nur dann gemäß Abschnitt 5.1 überprüfen, wenn einer der in Abschnitt 5.1 genannten Fälle auf den anderen Verantwortlichen zutrifft. Eine solche Prüfung muss durch den Kunden gemäß Abschnitt 5.1 durchgeführt werden, es sei denn, die Prüfung muss von dem anderen Verantwortlichen selbst nach dem Datenschutzrecht durchgeführt werden. Wenn mehrere Verantwortliche, deren Personenbezogene Daten von UNISERV auf der Grundlage der Vereinbarung verarbeitet werden, ein Audit erfordern, wird der Kunde alle angemessenen Mittel einsetzen, um die Audits zu kombinieren und Mehrfach-Audits zu vermeiden.

5.3. Der Kunde ist verpflichtet, Audits mindestens sechzig Tage im Voraus anzukündigen, es sei denn, dass zwingendes Datenschutzrecht oder eine zuständige Datenschutzbehörde eine kürzere Frist vorschreiben. Häufigkeit und Umfang der Audits sind zwischen den Parteien vernünftig und nach Treu und Glauben einvernehmlich zu vereinbaren. Kundenaudits sind auf maximal drei Werktage beschränkt. Über solche Einschränkungen hinaus werden die Parteien aktuelle Zertifizierungen oder andere Auditberichte verwenden, um wiederholte Audits zu vermeiden oder zu minimieren. Der Kunde hat UNISERV die Ergebnisse eines jeden Audits zur Verfügung zu stellen.

5.4. Der Kunde trägt die Kosten von Audits, es sei denn, ein solches Audit deckt einen wesentlichen Verstoß von UNISERV gegen diese Anlage auf, in diesem Fall trägt UNISERV die eigenen Kosten des Audits. Falls sich aus einem Audit ergibt, dass UNISER seine Verpflichtungen aus dieser Anlage nicht nachgekommen ist, heilt UNISERV diesen Verstoß umgehend auf eigene Kosten.

6. UNTERAUFTRAGSVERARBEITER

6.1. UNISERV erhält hiermit eine vorherige allgemeine schriftliche Genehmigung, die Verarbeitung von Personenbezogenen Daten unter den nachfolgenden Voraussetzungen auf Unterauftragsverarbeiter zu übertragen:

(a) UNISERV beauftragt Unterauftragsverarbeiter im Rahmen schriftlicher Verträge (einschließlich elektronischer Form), die mit den Bestimmungen dieser Anlage in Bezug auf die Verarbeitung Personenbezogener Daten durch den Unterauftragnehmer übereinstimmen. UNISERV haftet für etwaige Verstöße durch den Unterauftragsverarbeiter gemäß den Bestimmungen dieser Vereinbarung;

(b) UNISERV wird die Sicherheits-, Datenschutz- und Vertraulichkeitspraktiken eines Unterauftragsverarbeiters vor dessen Auswahl bewerten, um festzustellen, dass er in der Lage ist, das in dieser Anlage geforderte Schutzniveau für Personenbezogene Daten zu bieten; und

(c) Die bei Vertragsschluss gültige Liste der Unterauftragsverarbeiter der UNISERV wird von UNISERV veröffentlicht oder dem Kunden auf Anfrage zur Verfügung gestellt, einschließlich des Namens, der Anschrift und der Rolle jedes Unterauftragsverarbeiters, den UNISERV zur Erbringung der CDH Solution einsetzt.

6.2. Der Einsatz von Unterauftragsverarbeitern erfolgt nach Ermessen der UNISERV unter der Voraussetzung, dass folgende Regelungen eingehalten werden:
(a) UNISERV informiert den Kunden im Voraus (per Email oder durch ein Posting auf dem Supportportal, das über den UNISERV Support bereitgestellt wird) über jegliche geplante Hinzufügungen oder Ersetzungen innerhalb der Liste der Unterauftragsverarbeiter, einschließlich des Namens, der Anschrift und der Rolle des neuen Unterauftragsverarbeiters; und
(b) Der Kunde kann solchen Änderungen gemäß Abschnitt 6.3 widersprechen.

6.3. Sofern der Kunde gemäß Datenschutzrecht einen berechtigten Grund hat, der Verarbeitung Personenbezogener Daten durch die neuen Unterauftragsverarbeiter zu widersprechen, kann er die Vereinbarung (beschränkt auf die CDH Solution, für den der neue Unterauftragsverarbeiter eingesetzt werden soll) durch schriftliche Erklärung gegenüber UNISERV mit Wirkung zu einem vom Kunden festgelegten Zeitpunkt kündigen, spätestens jedoch zum Ablauf von dreißig Tagen nach dem Datum der Mitteilung von UNISERV an den Kunden über den neuen Unterauftragsverarbeiter. Kündigt der Kunde nicht innerhalb dieser Frist von dreißig Tagen, so gilt der neue Unterauftragsverarbeiter als durch den Kunden genehmigt. Innerhalb der Dreißig-Tagesperiode ab dem Datum der Mitteilung von UNISERV an den Kunden, in der der UNISERV über den neuen Unterauftragsverarbeiter informiert hat, kann der Kunde verlangen, dass die Parteien in gutem Glauben zusammenkommen und eine Lösung des Widerspruchs besprechen. Diese Besprechungen verlängern die Kündigungsfrist nicht und berühren nicht das Recht von UNISERV, den/die neuen Unterauftragsverarbeiter nach Ablauf der Frist von dreißig Tagen in Dienst nehmen zu dürfen. Jede Kündigung nach diesem Abschnitt 6.3 wird von beiden Parteien als unverschuldet betrachtet und unterliegt den Bestimmungen der Vereinbarung.

6.4. UNISERV kann einen Unterauftragsverarbeiter ohne vorherige Mitteilung austauschen, wenn sich der Grund für den Austausch der zumutbaren Kontrolle von UNISERV entzieht und der umgehende Austausch aus Sicherheits- oder anderen dringenden Gründen erforderlich ist. In diesem Fall informiert UNISERV den Kunden über den neuen Unterauftragsverarbeiter unverzüglich nach seiner Ernennung. Abschnitt 6.3 gilt entsprechend.

7. INTERNATIONALE VERARBEITUNG

7.1. UNISERV ist berechtigt, die Verarbeitung von Personenbezogene Daten unter Einbeziehung von Unterauftragsverarbeitern im Sinne dieser Anlage außerhalb des Landes, in dem sich der Kunde befindet unter Einhaltung des Datenschutzrechts durchzuführen.

7.2. Sofern (i) Personenbezogene Daten eines EWR- oder schweizerischen Verantwortlichen in einem Land außerhalb des EWR, der Schweiz bzw. außerhalb eines Landes, einer Organisation oder eines Gebiets erfolgt, das von der Europäischen Union als sicheres Land mit einem angemessenen Datenschutzniveau gemäss Art. 45 GDPR anerkannt ist, verarbeitet werden, oder (ii) Personenbezogene Daten eines anderen Verantwortlichen international verarbeitet werden und eine solche internationale Verarbeitung ein angemessenes Mittel nach dem anwendbaren Recht des Verantwortlichen erfordert, und das angemessene Mittel durch den Abschluss von Standardvertragsklauseln erfüllt werden kann, gilt:
(a) UNISERV und der Kunde vereinbaren die Geltung der Standardvertragsklauseln;
(b) Der Kunde vereinbart die Standardvertragsklauseln mit jedem relevanten Unterauftragsverarbeiter wie folgt: (i) Der Kunde tritt als unabhängiger Inhaber von Rechten und Pflichten den Standardvertragsklauseln bei, die zwischen UNISERV und dem Unterauftragsverarbeiter vereinbart wurden („Beitrittsmodell“) oder (ii) der Unterauftragsverarbeiter (vertreten durch UNISERV) vereinbart die Standardvertragsklauseln mit dem Kunden ("Vollmachtsmodell"). Das Vollmachtsmodell gilt, wenn und soweit UNISERV ausdrücklich über die Liste der Unterauftragsverarbeiter gemäß Abschnitt 6.1(c) oder über eine Mitteilung an den Kunden erklärt hat, dass dieses Modell für einen Unterauftragsverarbeiter verfügbar ist; und/oder
(c) Andere Verantwortliche, denen der Kunde die Nutzung der CDH Solution gemäß der Vereinbarung gestattet, können ebenfalls die Standardvertragsklauseln mit UNISERV und/oder den relevanten Unterauftragsverarbeitern in gleicher Weise wie der Kunde gemäß den obigen Abschnitten 7.2 (a) und (b) vereinbaren. In diesen Fällen vereinbart der Kunde die Standardvertragsklauseln im Namen der anderen Verantwortlichen.

7.3. Keine der Bestimmungen in der Vereinbarung darf bei widersprüchlichen Regelungen dahingehend ausgelegt werden, dass sie Vorrang vor einer Bestimmung der Standardvertragsklauseln hat. Zur Klarstellung: Wo diese Anlage Regelungen für Audit und Unterauftragsverarbeiter in den Abschnitten 5 und 6 näher beschreibt, gelten diese Regelungen auch in Bezug auf die Standardvertragsklauseln.

7.4. Die Standardvertragsklauseln unterliegen dem Recht des Landes, in dem der Verantwortliche seinen Sitz hat.

8. DOKUMENTATION; VERARBEITUNGSVERZEICHNIS

Jede Partei ist für die Einhaltung ihrer Dokumentationspflichten verantwortlich, insbesondere für die Führung von Verarbeitungsverzeichnissen, soweit dies nach dem Datenschutzrecht erforderlich ist. Jede Partei unterstützt die andere Partei in angemessener Weise bei der Erfüllung von deren Dokumentationspflichten, einschließlich der Bereitstellung der Informationen, die die andere Partei von ihr benötigt, in einer von der anderen Partei in angemessener Weise angeforderten Form (z. B. durch die Verwendung eines elektronischen Systems), damit die andere Partei den Verpflichtungen im Zusammenhang mit der Führung von Verarbeitungsverzeichnissen nachkommen kann.

9. DEFINITIONEN

Hervorgehobene Begriffe, die hier nicht definiert werden, haben die ihnen in der Vereinbarung zugewiesene Bedeutung.

9.1. “Verantwortlicher” bezeichnet die natürliche oder juristische Person, öffentliche Behörde oder Agentur oder andere Stelle, die allein oder gemeinsam mit anderen die Zwecke und Mittel der Verarbeitung Personenbezogener Daten bestimmt; für die Zwecke dieser Anlage gilt der Verantwortliche im Verhältnis zu UNISERV, wenn der Kunde als Auftragsverarbeiter für einen anderen Verantwortlichen handelt, als zusätzlicher und unabhängiger Verantwortlicher mit den entsprechenden Rechten und Pflichten eines Verantwortlichen gemäß dieser Anlage.

9.2. “Personenbezogene Daten” bezeichnet alle Informationen in Bezug auf eine Betroffene Person, die dem Schutz des Datenschutzrechts unterliegen. In dieser Anlage sind darunter nur diejenigen personenbezogenen Daten zu verstehen, die (i) vom Kunden oder dessen Autorisierten Nutzern in der CDH Solution oder durch dessen Nutzung erfasst werden oder (ii) von UNISERV oder ihren Unterauftragsverarbeitern bereitgestellt werden oder auf die UNISERV oder seine Unterauftragsverarbeiter zugreifen, um den Support gemäß dem Hauptvertrag zu leisten. Personenbezogene Daten sind eine Teilmenge der Kundendaten.

9.3. “Verletzung des Schutzes Personenbezogener Daten” bezeichnet eine/n bestätigte/n (1) versehentliche oder widerrechtliche Vernichtung, Verlust, Veränderung, eine unbefugte Offenlegung von bzw. einen unbefugten Zugang Dritter zu Personenbezogenen Daten oder (2) einen vergleichbaren Vorfall mit Personenbezogenen Daten, bei denen der Verantwortliche in jedem Fall gemäß Datenschutzrecht zur Meldung an die zuständigen Datenschutzbehörden oder gegenüber den Betroffenen Personen verpflichtet ist.

9.4. “Auftragsverarbeiter” bezeichnet eine natürliche oder juristische Person, öffentliche Behörde oder Agentur oder andere Stelle, die Personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, sei es direkt als Auftragsverarbeiter eines Verantwortlichen oder indirekt als Unterauftragsverarbeiter eines Auftragsverarbeiters, der Personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

9.5. “Standardvertragsklauseln” (auch als „EU-Modellklauseln“ bezeichnet) bezeichnet die Standardvertragsklauseln (Auftragsverarbeiter) bzw. jegliche nachfolgenden von der Europäischen Kommission veröffentlichten Versionen dieser Klauseln (die automatisch gelten).

Anhang 1 zur VEREINBARUNG ÜBER DIE DATENVERARBEITUNG.

Datenexporteur

Der Datenexporteur ist der Kunde der die CDH Solution von UNISERV bezieht und mit der die autorisierte Nutzer Personenbezogene Daten erfassen, ändern, nutzen, löschen oder anderweitig verarbeiten können. Wenn der Kunde anderen Verantwortlichen erlaubt, die CDH Solution ebenfalls zu nutzen, sind diese anderen Verantwortlichen ebenfalls Datenexporteure.

Datenimporteur

UNISERV und ihre Unterauftragsverarbeiter stellen die CDH Solution UPI zur Verfügung und erbringen den CDH Managed Service vom Standort Pforzheim(Deutschland), Niederlande oder an anderen Standorten aus an, an denen UNISERV Personal in der Organisation CDH Managed Service beschäftigt. UNISERV erbringt die Services im Rahmen des Life Cycle der CDH Solution und gemäß seiner Release-Strategie, für die aktuelle Fassung der CDH Solution sowie ggf. für ältere Fassungen. Details zu den Leistungen und Bedingungen des CDH Managed Service ergeben sich aus der Anlage 1 "Service Level Agreement", welcher als Anlage Bestandteil des Hauptvertrages ist.

Betroffene Personen

Sofern nicht anderweitig durch den Datenexporteur angegeben, lassen sich die übermittelten Personenbezogenen Daten in der Regel einer der folgenden Kategorien von Betroffenen Personen zuordnen: Mitarbeiter, Subunternehmer, Geschäftspartner oder sonstige Personen, deren Personenbezogene Daten in der CDH Solution gespeichert werden.

Datenkategorien

Die übermittelten Personenbezogenen Daten betreffen die folgenden Datenkategorien:
Der Kunde bestimmt die Kategorien von Daten in der CDH Solution. Die übermittelten Personenbezogenen Daten lassen sich in der Regel einer der folgenden Datenkategorien zuordnen: Name, Telefonnummer, E-Mail-Adresse, Zeitzone, Anschrift, Systemzugriff/-nutzung/-Berechtigungsdaten, Name des Unternehmens, Vertragsdaten, Rechnungsdaten und anwendungsspezifische Daten, die von den autorisierten Nutzern des Kunden in der CDH Solution erfasst werden, wie beispielsweise Bankkontendaten sowie Kredit- oder Debitkartendaten.

Besondere Datenkategorien (falls zutreffend)

Die übermittelten Personenbezogenen Daten lassen sich den folgenden besonderen Datenkategorien zuordnen: wie in der Vereinbarung (insbes. der Order Form) dargelegt (sofern zutreffend).

Verarbeitungsvorgänge / Zwecke

Die übermittelten Personenbezogenen Daten werden folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen:

- Verwendung von Personenbezogenen Daten, um die CDH Solution einzurichten, zu betreiben, zu überwachen und bereitzustellen (einschließlich operativen und technischen Supports)
- Bereitstellung von Consulting Services
- Kommunikation mit autorisierten Nutzern
- Speicherung von Personenbezogenen Daten in Rechenzentren
- Upload von Korrekturen oder Upgrades in die CDH Solution
- Erstellen von Sicherungskopien der Personenbezogenen Daten
- Rechnergestützte Verarbeitung von Personenbezogenen Daten, einschließlich Datenübertragung, Abruf von Daten, Zugang zu Daten
- Netzwerkzugang, um die Übertragung von Personenbezogenen Daten zu ermöglichen
- Ausführung von Anweisungen des Kunden gemäß der Vereinbarung

Anhang 2 zur VEREINBARUNG ÜBER DIE DATENVERARBEITUNG.

Technisch Organisatorische Maßnahmen der UNISERV GmbH

Technische und organisatorische Maßnahmen nach DSGVO

Bei der Uniserv GmbH wurden die im Folgenden aufgeführten Maßnahmen zur Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme getroffen.

Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO berücksichtigt.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Die Maßnahmen werden bei Bedarf, mindestens aber einmal jährlich überprüft und falls erforderlich aktualisiert.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b EU-DS-GVO)

1.1 Zutrittskontrolle

Ein unbefugter Zutritt zu Datenverarbeitungsanlagen ist zu verhindern.

1.1.1 Gebäudesicherung

Das freistehende Betriebsgebäude ist durch eine Alarmanlage (VdS geprüft) mit Anschluss an eine Alarmzentrale gesichert. Die Eingänge und Türen des Gebäudes sind mit Sicherheits- bzw. mit Codekartenschlössern versehen. Die Geschlossenheit vorhandener Fluchttüren wird durch eine Alarmanlage sichergestellt. Alle Erdgeschossfenster sind mit Glasbruchsensoren und Magnetkontakten gesichert. In allen Räumen des Erdgeschosses und den Fluren aller Stockwerke sind zusätzlich Bewegungsmelder installiert.

1.1.2 Zutrittskontrollsystem

Der Zutritt zum Gebäude und zum Sicherheitsbereichen wird durch ein mehrstufiges Zugangskontrollsystem mit berührungslosen Codekarten geregelt und protokolliert.
Betriebsfremde Personen können das Firmengebäude nur nach Einlass durch das Empfangspersonal betreten.

1.1.3.Sicherheitsbereich

Der Sicherheitsbereich besteht aus den Räumen Serverraum und Datenarchiv. Das Datenarchiv und der Serverraum sind fensterlos und durch separate Zutrittskontrolle gesichert. Der Zutritt zum Sicherheitsbereich ist durch eine restriktive Zutrittsregelung nur den dort arbeitenden Personen gestattet.

1.2 Zugangskontrolle

Eine unbefugte Systemnutzung ist zu verhindern.

Alle Datenverarbeitungssysteme sind mit einem Passwortschutz versehen. Die verwendeten Passwörter müssen bestimmten Kriterien bezüglich Länge und Zeichenvorrat entsprechen sowie regelmäßig geändert werden. Die bei Uniserv geltende Passwort-Policy ist in der für alle Mitarbeiter geltenden Datenschutz-Richtlinie dokumentiert. An- und Abmeldevorgänge an Produktionssystemen für eigene Zwecke und für die Auftragsdatenverarbeitung werden protokolliert. Ein restriktiv konfiguriertes Firewall-System verhindert den Zugang vom Internet zum internen Netzwerk und regelt den Zugang vom internen Netz ins Internet.

1.3 Zugriffskontrolle / Benutzerkontrolle

Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems möglich sein

Der Zugriff auf Daten ist durch entsprechende Berechtigungskonzepte und Benutzerprofile geregelt. Dies erfolgt sowohl auf Betriebssystem- als auch auf Datenbank oder Anwendungsebene.
Berechtigungsänderungen müssen durch die Personalabteilung oder den Vorgesetzten veranlasst und genehmigt werden.

Datenträger werden nur im Datenarchiv mit restriktiver Zutrittskontrolle gelagert.

Die Festplatten von Laptops sind standardmäßig verschlüsselt. Dadurch wird unbefugter Zugriff auf Daten selbst bei Verlust oder Diebstahl der Geräte verhindert.

Fernwartung findet nur zur Sicherstellung der Hardwareverfügbarkeit in bei Rechenzentrumsbetrieb üblichem Rahmen statt.

1.4 Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben werden.

Durch folgende Maßnahmen wird sichergestellt, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:
Einsatz von Berechtigungskonzepten und Benutzerprofilen, sowohl auf Betriebssystem- als auch auf Datenbank oder Anwendungsebene.
Strikte Trennung von Datenverarbeitungssystemen für eigene Zwecke, Test und Entwicklung sowie für die Auftragsverarbeitung.

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a EU-DS-GVO, Art. 25 Abs. 1 EU-DS-GVO)

Die Verarbeitung personenbezogener Daten hat in einer Weise zu erfolgen, dass die

Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

In der Regel müssen bei Uniserv die Daten personenbezogen verarbeitet werden. Dies gilt insbesondere für Daten, die im Auftrag für Kunden verarbeitet werden. Daher ist dort eine Pseudonymisierung nicht anwendbar.

Wenn immer möglich sollen Tests statt mit realen personenbezogene Daten mit pseudonymisierten Daten durchgeführt werden. Sollten Test nur mit realen personenbezogenen Daten möglich sein sind dafür die gleichen Bedingungen wie für Produktionsverarbeitungen einzuhalten. Eine Anonymisierung ist nur für statistische Auswertungen angezeigt.

2. Integrität (Art. 32 Abs. 1 lit. b EU-DS-GVO)

2.1 Weitergabekontrolle / Übertragungskontrolle

Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich sein.

Die Übertragung personenbezogener Daten auf elektronischem Weg erfolgt nur unter Einsatz von Verschlüsselung entweder per eMail oder über den Uniserv Up- und Download-Service. Die Übertragungen werden protokolliert.
Der Versand von Daten erfolgt ausschließlich durch Mitarbeiter der Abteilung Data Processing Service (DPS). Eingehende Daten werden sofort in DPS erfasst, analysiert und einem Auftrag zugeordnet.
Die Vorgehensweise bei der Datenübertragung ist durch entsprechende Betriebsanweisungen und Arbeitsanweisungen sowie in der Datenschutz-Richtlinie geregelt.

2.2 Eingabekontrolle / Datenträgerkontrolle / Speicherkontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

.

Abhängig vom verwendetem Betriebssystem, Datenbanksystem bzw. der Anwendung werden Datenzugriffe, Änderungen und Systemaktivitäten auf unterschiedliche Art erfasst oder protokolliert.
Im Rahmen der Auftragsdatenverarbeitung durchgeführte Aktionen werden protokolliert und sind jederzeit nachvollziehbar.

3. Verfügbarkeit und Belastbarkeit / Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b EU-DS-GVO)

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.

Die Daten sind bei Uniserv durch folgende Maßnahmen vor zufälliger Zerstörung oder Verlust geschützt:

Alle Räume und Flure sind mit Rauchmeldern ausgestattet, das Band- bzw. Kassettenarchiv ist zusätzlich mit speziellem Brandschutzmaßnahmen gesichert (F90 konform). Es ist eine Brandmeldeanlage installiert, die direkt zur Feuerwehrzentrale aufgeschaltet ist. Außerdem existieren Brand- und Notfallanweisungen, die allen Mitarbeitern bekannt sind. Zum Schutz vor Wasserschäden sind an kritischen Stellen Feuchtigkeitssensoren installiert, die mit der Alarmanlage verbunden sind.
Die Server sind mit USVs gegen Überspannungen durch Blitzschlag und gegen kurzzeitigen Stromausfall gesichert.

Die Serverräume werden durch redundant ausgelegte Klimaanlagen gekühlt. Störungen der Klimageräte werden automatisch über eine Alarmmeldezentrale an die IT-Abteilung gemeldet.

Sonstige kritische Technikstörungen werden ebenfalls über eine rund um die Uhr besetzte Alarmmeldezentrale gemeldet. Eine schnelle Erreichbarkeit von IT-Fachpersonal ist gewährleistet und im IT-Notfallhandbuch ist dokumentiert, wie bei Störungen zu handeln ist.

Das zentrale Storage-System ist redundant ausgelegt und auf 2 Gebäudeflügel und unterschiedliche Brandabschnitte verteilt. Die Festplatten sind durch RAID-Verfahren gegen Ausfall geschützt.

Die produktiven Server werden bei Uniserv in einem VMware ESXi-Cluster betrieben. Dadurch ist sichergestellt, dass bei einem Hardware Ausfall die virtualisierten Server-Systeme, die auf der ausgefallenen Hardware liefen, automatisch auf einem anderen ESXi-Host wieder hochgefahren werden. Außerdem findet ein automatischer Lastausgleich zwischen den ESXi-Hosts im Cluster statt, in dem VMs von überlasteten Hosts automatisch auf weniger ausgelastete Hosts migriert werden.

Wichtige Server- und Storage-Systeme werden über ein Monitoring-System überwacht. Bei Problemen erfolgt automatisch eine Alarmierung der IT-Administratoren.

Bei Uniserv werden täglich Datensicherungen durchgeführt. Die Backup-Daten werden verschlüsselt in der Cloud in einem deutschen Rechenzentrum ausgelagert.

Außerdem kommen Schutzprogramme wie z.B. Virenscanner unterschiedlicher Hersteller, SPAM-Filter, Mail- und Web-Proxy zum Einsatz, um Daten vor mutwilliger Zerstörung oder Verlust zu schützen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d EU-DS-GVO, Art. 25 Abs. 1 EU-DS-GVO)

4.1 Datenschutz-Management

Bei der Uniserv GmbH ist ein Datenschutz-Management-System etabliert, welches in Form einer Datenschutz-Richtlinie dokumentiert ist, die regelmäßig aktualisiert und optimiert wird.

Dieses Dokument enthält diverse Richtlinien und Handlungsvorgaben für den Umgang mit personenbezogenen Daten und dient damit der Einhaltung der Rechenschaftspflicht gemäß Art.5 Abs.2 und der Dokumentationspflichten nach Art.28, 30, 32, 35 DSGVO. Die vorliegende Richtlinie gilt für alle Mitarbeiter von Uniserv und für alle Personen, die weisungs- und vertragsgemäß für Uniserv tätig sind.

Alle Uniserv Mitarbeiter wurden über die Bestimmungen des Bundesdatenschutzgesetzes und der DSGVO belehrt, sind schriftlich auf die Wahrung des Datenschutzes und der Vertraulichkeit verpflichtet und werden regelmäßig zu Datenschutz-Themen geschult. Ein externer betrieblicher Datenschutzbeauftragter ist bestellt.

4.2 Incident-Response-Management

Bei Uniserv ist ein Prozess zum Incident-Response-Management etabliert, der in der Datenschutz-Richtlinie dokumentiert ist.

Alle Mitarbeiter sind darüber informiert, dass alle möglicherweise datenschutzrechtlich relevanten Datenschutzvorfälle sofort der Geschäftsführung, dem Datenschutzbeauftragten oder dem IT-Leiter zu melden sind. Sollte ein Sicherheitsvorfall die Vermutung einer meldepflichtigen Datenschutzverletzung nach Art.33, 34 DSGVO nahelegen, wird durch die Geschäftsführung, den IT-Leiter und den Datenschutzbeauftragen der Vorfall geprüft und das weitere Vorgehen festgelegt.

Die Geschäftsführung dokumentiert gemäß Art. 33 DSGVO evtl. auftretende Datenschutzvorfälle, deren Auswirkungen sowie ergriffene Abhilfemaßnahmen, um bei Bedarf eine Prüfung durch die Aufsichtsbehörde zu ermöglichen.

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DS-GVO)

Bei Uniserv werden - soweit möglich, angemessen und praktikabel - datenschutzfreundliche Voreinstellungen bei Programmen und Anwendungen vorgenommen.

Bei der Auftragsverarbeitung werden die Vorgaben des verantwortlichen Auftraggebers umgesetzt.

4.4 Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 EU-DS-GVO ohne entsprechende Weisung des Auftraggebers

Für im Auftrag verarbeitete Daten gibt es ein formalisiertes Auftragsmanagement. Data Processing Services (DPS) protokolliert auf den RZ-Aufträgen schriftlich die Verarbeitungsschritte entsprechend den Weisungen des Auftraggebers, bereitet die Jobs vor und kontrolliert die Ergebnisse. Alle Aufträge müssen schriftlich vorliegen. Die Vorgehensweise ist in entsprechenden Arbeitsanweisungen dokumentiert.

Sofern personenbezogene Daten durch externe Dienstleister im Auftrag verarbeitet werden, wird durch folgende Maßnahmen eine datenschutzkonforme Verarbeitung sichergestellt:

- Sorgfältige Auswahl der Auftragnehmer.
- Abschluss eines Auftragsverarbeitungsvertrags mit Überprüfung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen gemäß Artikel 32 DSGVO.
- Beim Auftragnehmer muss ein Datenschutzbeauftragter bestellt sein und seine Mitarbeiter müssen auf die Wahrung des Datenschutzes und der Vertraulichkeit gemäß DSGVO verpflichtet sein.
- Der Auftraggeber wird vorab über die Nutzung von Unterauftragnehmer informiert.

Änderungshistorie

Version	Datum	Beschreibung / Änderung	Autor(en)	Review
0.1	08.05.2018	Erstentwurf	Andreas Reichert	
0.2	11.05.2018	Erster Review		Roland Pfeiffer
0.3	15.05.2018	Zweites Review		D. Dei Giudici
1.0	15.05.2018	Freigabe als Version 1.0		Roland Pfeiffer D. Dei Giudici