

# Vereinbarung zur Verarbeitung und Sicherheit von Daten

zwischen

Ihnen, als Kunde für folgende DREI Produkte: vServer (Managed und Unmanaged) ; Dedicated Server (Managed)

im Folgenden „**Verantwortlicher**“ genannt

und

**Hutchison Drei Austria GmbH**

Brünner Straße 52

1210 Wien

im Folgenden „**Auftragsverarbeiter**“ genannt

## 1. Begriffsbestimmungen

„**Befugte Personen**“ bezeichnet (i) befugte Mitarbeiter des Auftragsverarbeiters: Das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis zum Auftragsverarbeiter, denen auf Grund ihrer berufsmäßigen Beschäftigung personenbezogene Daten anvertraut werden bzw. zugänglich gemacht werden sowie (ii) alle Vertragspartner, Bevollmächtigte, (externe) Berater sowie Rechnungs- oder Wirtschaftsprüfer des Auftragsverarbeiters, die einen berechtigten/legitimen Bedarf an der Kenntnis personenbezogener Daten haben oder dem Auftragsverarbeiter bei seiner, in dieser Vereinbarung getroffenen, Verpflichtungen unterstützen den Datenschutz einzuhalten und die jeweils in ausreichendem Umfang schriftlich zur Geheimhaltung der personenbezogenen Daten im Einklang mit dieser gegenständlichen Vereinbarung verpflichtet sind.

„**Personenbezogene Daten**“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person (betroffene Person) beziehen; als identifizierbar wird eine Person angesehen, die direkt oder indirekt, insbesondere in Bezug auf eine Kennung wie beispielsweise einen Namen, eine Kennnummer, einer Nummer eines öffentlichen Verzeichnisses, einem Standortdatum, einer E-Mail Adresse, einer MSISDN, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden können. Der Begriff „Person“ bezieht sich auf natürliche, aber auch auf juristische Personen, da jedes personenbezogene Datum einer Person, das im Rahmen der Erbringung eines Telekommunikationsdienstes verarbeitet wird, in die Regulierung der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie) die durch die Richtlinie 2009/140/EG geändert wurde, fällt. Diese Richtlinie unterscheidet bei dem Begriff „Nutzer“ nicht zwischen juristischen und natürlichen Personen.

„**Verarbeitung**“ bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben/Erfassen, das Aufzeichnen, das Organisieren, das Ordnen, das Speichern, das Anpassen oder das Verändern, das Auslesen, das Abfragen, das Verwenden, das Offenlegen durch Übermitteln,

Verbreiten oder eine andere Form des Bereitstellen, das Abgleichen oder das Verknüpfen, das Einschränken, das Löschen oder das Vernichten.

„**Pseudonymisierung**“ bezeichnet die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

„**Anonymisierung**“ bezeichnet die Verarbeitung von personenbezogenen Daten durch die Verwendung einer oder mehrerer Techniken/Arten, die von der Artikel 29 Gruppe in [0829/14/DE WP216](#) beschrieben werden und/um so jeglichen Personenbezug von dem Datum (zu) entfernen. Das Datum kann nach der Anonymisierung nicht mehr einer bestimmten Person zugeordnet werden.

„**Datensicherheitsverletzung**“ bezeichnet eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise gemäß dieser Vereinbarung verarbeitet wurden.

„**Regulierung**“ bezeichnet die aktuellen Datenschutzbestimmungen, insbesondere die Datenschutzgrundverordnung 2016/679 (im Folgenden DSGVO), die e-Privacy Richtlinie 2002/58/EG, die Richtlinie 611/2013 über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäß der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates (Datenschutzrichtlinie für elektronische Kommunikation), das Österreichische Telekommunikationsgesetz (TKG) und der [ISPA-Code of Conduct](#) (<https://www.ispa.at/wissenspool/datenschutz/>).

„**Datenschutzgesetz**“ bezeichnet das [österreichische Datenschutzgesetz, BGBl. I Nr. 24/2018](#).

„**Vertrauliche Informationen**“ bezeichnet die Bestimmungen dieser Vereinbarung sowie Betriebs- oder Geschäftsgeheimnisse und wirtschaftliche, finanzielle, kommerzielle oder technische Informationen, Know-How oder andere Informationen in Bezug auf den Verantwortlichen, mit dem Verantwortlichen verbundene Unternehmen oder in Bezug auf den Auftragsverarbeiter, unabhängig von Form und Medium, ob mündlich oder schriftlich offengelegt sowie ob vor oder nach dem Abschluss dieser Vereinbarung, in Verbindung mit jeder Art der Vervielfältigung dieser Informationen unabhängig von Form und Medium sowie jeglicher Teil dieser Information, ausgenommen wenn (i) die Information dem Empfänger bereits vor der Offenlegung durch die offenlegende Partei zugekommen ist, (ii) die Information während der Offenlegung allgemein zugänglich war bzw. später ohne eine Verletzung dieser Bestimmungen öffentlich zugänglich wurde, (iii) die Information dem Empfänger durch einen Dritten ohne einer Verletzung einer Vertraulichkeitspflicht zugekommen ist, (iv) die Information dem Empfänger über seine Mitarbeiter unabhängig von der offenlegenden Partei ohne Zugang zu der entsprechenden Information zugegangen ist.

## **2. Verantwortlicher von personenbezogenen Daten**

2.1. Die Verantwortung zur Verarbeitung von personenbezogenen Daten obliegt ausschließlich dem Verantwortlichen. Der Verantwortliche bleibt dies auch zu jeder Zeit und für alle Zwecke der Datenverarbeitung, die in Zusammenhang mit dieser Vereinbarung bzw. ähnlichen Vereinbarungen stehen.

- 2.2. Der Verantwortliche ist verantwortlich für die Einhaltung seiner Pflichten unter den datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtfertigung der Übermittlung von personenbezogenen Daten sowie der Entscheidung über die Verarbeitung und Nutzung der Daten.

### **3. Auftragsverarbeiter**

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Rahmen der Bereitstellung von Computer- und Storeressourcen für die DREI Produkte vServer (Managed/Unmanaged) und Dedicated Server (Managed). Die personenbezogenen Daten werden für die Erfüllung der vertraglichen Dienstleistungen der og. Produkte inkl. dazugehörigen Kundenservice sowie dem technischen Service (Wartung, Monitoring, Konfiguration, Installation von Software auf Kundenwunsch, Einspielung von Updates und Erstellung von Backups) verarbeitet.

### **4. Pflichten des Auftragsverarbeiters**

- 4.1. Der Auftragsverarbeiter verpflichtet sich, alle Daten, die er vom Verantwortlichen empfängt, ausschließlich gemäß den Anweisungen des Verantwortlichen oder den Vereinbarungen mit dem Verantwortlichen und nur im Zusammenhang mit dieser Vereinbarung zu verarbeiten.
- 4.2. Der Auftragsverarbeiter hat
- a) alle personenbezogenen Daten streng vertraulich zu behandeln sowie ein solches Maß an Sorgfalt anzuwenden, das angemessen ist, um einen unbefugten Zugriff, Gebrauch oder Offenlegung zu vermeiden;
  - b) personenbezogene Daten, sowie den Zugang zu diesen, ausschließlich nur für die Erbringung der Dienstleistung vServer (Managed/Unmanaged) und Dedicated Server (Managed) und somit für jene Zwecke zu verarbeiten, die in dieser Vereinbarung für die DREI Produkte vServer (Managed/Unmanaged) und Dedicated Server (Managed) bestimmt werden. Der Gebrauch, der Verkauf, der Verleih, die Übertragung, die Verbreitung sowie die Veröffentlichung oder jede andere Form der Verarbeitung der personenbezogenen Daten für eigene Zwecke des Auftragsverarbeiters oder für die Zwecke von Dritten ist ausschließlich nur mit schriftlicher Zustimmung des Verantwortlichen gestattet;
  - c) auf keinen Fall direkt oder indirekt personenbezogene Daten ohne ausdrückliche schriftliche Zustimmung an nicht autorisierte Personen zu übermitteln, es sei denn die Übermittlung wird aufgrund von Rechtsvorschriften bzw. von einer Behörde gefordert. In einem solchen Fall hat der Auftragsverarbeiter (i) alle Anstrengungen zu unternehmen, um den Verantwortlichen noch vor der Übermittlung zu informieren und falls dies nicht möglich ist, hat diese Information möglichst unmittelbar danach zu erfolgen; (ii) für die Handlungen und Unterlassungen von unbefugten Dritten die

Verantwortung gegenüber dem Verantwortlichen so zu tragen, als wären es die Handlungen und Unterlassungen des Auftragsverarbeiters.

## 5. Weitere Auftragsverarbeiter / Autorisierte Personen

- 5.1. Der Auftragsverarbeiter bedient sich bei der Auftragsverarbeitung keiner weiteren Auftragsverarbeiter – siehe Anhang.

Der Auftragsverarbeiter ist jederzeit gegenüber dem Verantwortlichen zur Einhaltung dieser Vereinbarung und damit im Zusammenhang stehenden Vereinbarungen durch die weiteren Auftragsverarbeiter verantwortlich.

## 6. Informationssicherheit

- 6.1. Der Auftragsverarbeiter sichert zu, dass die Erhebung, der Zugang, die Nutzung, die Speicherung, die Löschung sowie die Offenlegung von personenbezogenen Daten immer in Anwendung und Beachtung aller geltenden Datenschutzgesetze sowie aller sonstigen anwendbaren Verordnungen und Richtlinien erfolgen.

- 6.2. Zusätzlich zu Punkt 6.1., setzt der Auftragsverarbeiter organisatorische, physische und technische Schutzmaßnahmen zum Schutz der personenbezogenen Daten ein, die jedenfalls den Stand der Technik berücksichtigen, die sicherstellen, dass alle Schutzmaßnahmen, einschließlich der Art und Weise, wie personenbezogene Daten erhoben, abgerufen, verwendet, gespeichert, verarbeitet, entsorgt/gelöscht und offengelegt werden, den geltenden Datenschutzgesetzen und dieser Vereinbarung entsprechen. Der Auftragsverarbeiter übermittelt mit der Unterfertigung dieser Vereinbarung die konkret getroffenen technischen und organisatorischen Maßnahmen gemäß dem Anhang 1 „*Technische und organisatorischen Maßnahmen im Zusammenhang mit einer Datenverarbeitung gemäß DSGVO/DSG 2018*“.

## 7. Datensicherheitsverletzung

- 7.1. Der Verantwortliche unterliegt der DSGVO, die reguliert, dass jede Datensicherheitsverletzung innerhalb von 72 Stunden nach Bekanntwerden an die zuständige Datenschutzbehörde gemeldet werden muss.

- 7.2. Daher hat der Auftragsverarbeiter  
a) dem Verantwortlichen Kontaktdaten zu nennen, an den sich der Verantwortliche zur Unterstützung im Zusammenhang mit Datensicherheitsverletzungen wenden kann.

Kontaktdaten: [dpo@drei.com](mailto:dpo@drei.com) oder [noc@drei.com](mailto:noc@drei.com)

- b) den Verantwortlichen bei einer Datensicherheitsverletzung so bald wie möglich, jedoch spätestens 48 Stunden nachdem dem Auftragsverarbeiter die Verletzung bekannt wurde, zu benachrichtigen sowie bei der Benachrichtigung des Kunden zu unterstützen, indem der Auftragsverarbeiter über jegliche Datensicherheitsverletzung telefonisch oder per E-Mail informiert. Hierbei werden die Kontaktdaten des Verantwortlichen bei Vertragsabschluss verwendet.

Unmittelbar nach der Benachrichtigung des Verantwortlichen durch den Auftragsverarbeiter über eine Datensicherheitsverletzung haben die Parteien diese Datensicherheitsverletzung zu untersuchen. Der Auftragsverarbeiter verpflichtet sich mit dem Verantwortlichen diesbezüglich zusammenzuarbeiten.

- 7.3. Der Auftragsverarbeiter bemüht sich mit allen Mitteln jede Datensicherheitsverletzung unverzüglich zu beheben sowie jede weitere Datensicherheitsverletzung gemäß den geltenden Datenschutzbestimmungen, Gesetzen, Vorschriften und Standards zu verhindern.

## **8. Sicherheitsüberwachung – Kontrollrechte des Verantwortlichen**

- 8.1. Auf schriftliche Anfrage hat der Auftragsverarbeiter dem Verantwortlichen alle relevanten Unterlagen zur Verfügung zu stellen, um die Einhaltung dieser Vereinbarung sowie aller anwendbaren Gesetze und Industriestandards zu bestätigen und um überprüfen zu können, ob jene Datenanwendungen personenbezogener Daten, die dem gegenständlichen Vertragsverhältnis unterliegen, den Sicherheitsstandards entsprechen. Der Verantwortliche behandelt die übermittelten Informationen des Auftragsverarbeiters als vertrauliche Informationen.
- 8.2. Der Auftragsverarbeiter wird regelmäßig durch Auditoren auf die Einhaltung der Sicherheitsmaßnahmen und der datenschutzrechtlichen Anforderungen überprüft. Das Ergebnis einer solchen Überprüfung teilt der Auftragsverarbeiter dem Verantwortlichen gerne auf Anfrage mit.

## **9. Rückgabe oder Löschung von personenbezogenen Daten**

- 9.1. Für die DREI Produkte vServer (Managed/Unmanaged) und Dedicated Server (Managed) gelten folgende Lösungsfristen:

Dedicated Server (Managed): 4 Wochen nach Kündigung werden die personenbezogenen Daten auf der/den physischen Festplatten eigenständig von H3A nach dem Stand der Technik gelöscht.

vServer(Managed/Unmanaged): 4 Wochen nach Kündigung werden die personenbezogenen Daten seitens H3A nach dem Stand der Technik gelöscht.

Für die Verarbeitung der Kundendaten für das Produkt sowie für die Erbringung der Telekommunikation ist Drei selbst Verantwortlicher. Diese Datenverarbeitung unterliegt nicht dieser Vereinbarung und ist somit auch nicht von dieser Lösungsfrist betroffen. Es gelten die AGBs sowie die Datenschutzerklärung auf [www.drei.at/datenschutz](http://www.drei.at/datenschutz).

## **10. Haftung**

- 10.1. Unabhängig von anderen Haftungsbeschränkungen zwischen dem Verantwortlichen und Auftragsverarbeiter wird die Haftung für Schäden jeglicher Art, die sich aus einer Regulierung im Zusammenhang mit dieser Vereinbarung ergeben, ausgeschlossen. Davon werden Schäden ausgenommen, die vorsätzlich oder grob fahrlässig verursacht wurden.

## **11. Dauer und Beendigung**

- 11.1. Die Vertragsdauer und Kündigungsmodalität dieser Vereinbarung folgt der Vertragsdauer und Kündigungsmodalität des zwischen den Vertragsparteien abgeschlossenen Vertrages zu den DREI Produkten vServer und Dedicated Server. Die Vertragsdauer tritt mit Unterzeichnung des Angebotes in Kraft.
- 11.2. Sollte kein entsprechender Rahmenvertrag oder sonstige Vereinbarungen zwischen den Vertragsparteien bestehen, so tritt diese Vereinbarung durch beidseitige Unterschrift der Parteien in Kraft und ist bis zur Beendigung, auf Basis einer Kündigungsfrist von drei (3) Monaten durch eine schriftliche Kündigung einer der beiden Parteien, in Kraft.
- 11.3. Liegt eine wesentliche Vertragsverletzung vor, kann diese Vereinbarung unverzüglich in Schriftform außerordentlich gekündigt werden. Eine wesentliche Vertragsverletzung liegt unter anderen vor, wenn:
- a) Die andere Partei eine wesentliche Verletzung begeht bzw. einer Verpflichtung aus dieser Vereinbarung nicht nachkommt und dieser auch nach einer vierzehn (14) tägigen Frist nach Aufforderung nicht Folge leistet.
  - b) Eine Regulierungsbehörde oder andere Behörde, die für die Vertragsparteien zuständig ist, entscheidet, dass die Bestimmung zur Bereitstellung der relevanten Dienstleistung, die im Zusammenhang mit dieser Vereinbarung steht, gegen geltende Gesetze, Vorschriften, Entscheidungen oder sonstige Verordnungen verstößt oder die Erbringung der Dienstleistung per se unzulässig wird. In diesem Fall kann kein Schadenersatz von der anderen Partei gefordert werden; oder
  - c) Eine erforderliche behördliche Ermächtigung bzw. Formalerfordernis ist aus irgendeinem Grund entfallen, zurückgezogen worden oder nicht mehr gültig. Gesetzt den Fall, dass die Genehmigung bzw. Formalerfordernis nicht entfällt, zurückgezogen oder ungültig wird, obwohl eine der Vertragsparteien fahrlässig oder vorsätzlich gegen verwaltungsrechtliche oder gesetzliche Bestimmungen verstößt, handelt es sich nicht um eine wesentliche Verletzung, die die verletzte Partei daher auch nicht zur außerordentlichen Kündigung der relevanten Dienstleistungen ermächtigen kann.
  - d) Sich die wirtschaftliche Lage der anderen Vertragspartei verschlechtert oder ein Insolvenzantrag mangels kostendeckenden Vermögens abgewiesen wird.
- 11.4. Auch nach Beendigung dieser Vereinbarung (oder einer Leistung im Zusammenhang mit dieser Vereinbarung) bleiben die Rechte und Pflichten aus dieser Vereinbarung bis zum Zeitpunkt der Kündigung unberührt bestehen.

**12. Geltendes Recht und Gerichtsstand**

- 12.1. Die in dieser Vereinbarung getroffenen Verpflichtungen sowie ihre Gültigkeit, ihre Erfüllung und damit verbundene Streitigkeiten unterliegen dem österreichischen Recht. Der Verantwortliche sowie der Auftragsverarbeiter sichern beide die ausschließliche Zuständigkeit der österreichischen Gerichte zu.

Verantwortlicher

Hutchison Drei Austria GmbH

-----  
Ort, Datum

-----  
Ort, Datum

-----  
Unterschrift

-----  
Unterschrift

## Anhang 1:

<p style="text-align: center;"><b>Mindestanforderungen für von Hutchison Drei Austria GmbH als Auftragsverarbeiter im Zusammenhang mit einer Auftragsverarbeitung gemäß DSGVO.</b></p>
--

Zwischen dem Verantwortlichen und Auftragsverarbeiter soll eine datenschutzrechtliche Auftragsverarbeitervereinbarung abgeschlossen werden.

Die Regelungen der Datenschutzgrundverordnung (EU 2016/679) treffen Verantwortliche und Auftragsverarbeiter gleichermaßen. In diesem Dokument soll nachweislich dokumentiert werden, dass der Auftragsverarbeiter hinsichtlich Etablierung eines geforderten Datenschutzmanagementsystems seine ihn treffenden Verpflichtungen gemäß DSGVO erfüllt.

In der Auftragsverarbeitervereinbarung ist gemäß Art 25 Abs 3 DSGVO zu dokumentieren, was der Gegenstand und die Dauer, Art und Zweck, die Art der personenbezogenen Daten sowie die Kategorien betroffener Personen der Auftragsverarbeitung ist. Dies ist in untenstehender Tabelle einzutragen.

Der Auftragsverarbeiter hat nach einer Risikobewertung jedenfalls nachstehende Maßnahmen zu ergreifen. Diese Maßnahmen stellen Mindestanforderungen an die zwischen H3A und dem Auftragsverarbeiter einzugehende Vertragsbeziehung hinsichtlich der Verarbeitung personenbezogener Daten für H3A durch den Auftragsverarbeiter dar. Eine konkrete inhaltliche Beschreibung, wie die Maßnahmen konkret vom Auftragsverarbeiter erfüllt werden, ist in untenstehender Tabelle zu dokumentieren.

Sollte ein Auftragsverarbeiter mit mehreren unterschiedlichen Auftragsverarbeitungen beauftragt werden, so ist die untenstehende Tabelle für jede Art der Auftragsverarbeitung neu auszufüllen und an dieser Stelle als weiterer Anhang hinzuzufügen.

Dieser Anhang gilt als integrierter Anhang des datenschutzrechtlichen Auftragsverarbeitungsvertrags zwischen H3A und dem Auftragsverarbeiter.



Beschreibung der Datenverarbeitung	
<p><b>Gegenstand der Datenverarbeitung (sowie Art und Zweck der Datenverarbeitung):</b> Beschreiben Sie möglichst detailliert Ihre Aufgabe als Auftragsverarbeiter bzw. das Projekt oder Ihre Dienstleistung.</p>	<p>In Rahmen der Bereitstellung von Computer- und Storageressourcen für die DREI Produkte vServer (Managed/Unmanaged) und Dedicated Server (Managed) werden für die Erfüllung der vertraglichen Dienstleistungen der og. Produkte inkl. dazugehörigen Kundenservice sowie dem technischen Service (Wartung, Monitoring, Konfiguration, Installation von Software auf Kundenwunsch, Einspielung von Updates und Erstellung von Backups) personenbezogene Daten verarbeitet.</p> <p>Managed Dedicated/vServer: H3A implementiert das Betriebssystem und führt Basisservices auf Kundenwunsch durch (zb. Installation von Datenbanken, Webserver, etc.). Die Server werden von H3A gewartet und konfiguriert. H3A übernimmt auch Monitoring und Updates. Nach Kundenwunsch werden User von Drei hinzugefügt oder entfernt.</p> <p>Unmanaged vServer: Installation des Betriebssystems und Übergabe aller administrativen Zugänge an den Kunden. Der Kunde hat die Datenhoheit und ist eigenverantwortlich für seine Daten. (H3A hat nach Übergabe keinen Zugriff mehr auf die Systeme). Der Kunde ist auch verantwortlich für Updates seiner Systeme.</p> <p>Der Kundenservice erfolgt über ein E-Mail-Ticket System (Requesttracker)</p>
<p><b>Kategorien betroffener Personen:</b> Zutreffendes ankreuzen bzw. Personenkategorie ergänzen</p>	<p><input checked="" type="checkbox"/> Kunden von H3A  <input type="checkbox"/> potentielle Kunden von H3A  <input type="checkbox"/> Mitarbeiter von H3A  <input type="checkbox"/> Lieferanten, Vertragspartner von H3A  <input type="checkbox"/> Kinder unter 14 Jahren  <input type="checkbox"/> Sonstige: ...</p>
<p><b>Kategorien von personenbezogenen Daten:</b> Zutreffendes ankreuzen bzw. Art der Daten ergänzen</p>	<p><input type="checkbox"/> Stammdaten nach TKG  <input type="checkbox"/> Verkehrsdaten nach TKG  <input type="checkbox"/> Inhaltsdaten nach TKG  <input checked="" type="checkbox"/> Kundendaten von H3A (außerhalb des TKGs)  <input type="checkbox"/> Personaldaten von Mitarbeitern von H3A</p>

	<input type="checkbox"/> Userdaten (Kennwort, Passwörter) <input type="checkbox"/> Cookies <input type="checkbox"/> Profile <input type="checkbox"/> Sensible Daten (Daten gemäß Art 9 oder 10 DSGVO) <input type="checkbox"/> Sonstige: ...
<p><b>Verarbeitung von sensiblen Daten</b>  (falls zutreffend):  angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen</p>	<p>Es werden keine sensiblen Daten gemäß Art 9 oder Art 10 DSGVO verarbeitet.</p>
<p><b>Dauer der Datenverarbeitung:</b>  Beschreibung, nach welcher Dauer bzw. nach welchen Kriterien die Löschung bzw. Retournierung der Daten erfolgt.</p>	<p>Für das Produkt <b>Dedicated Server (Managed)</b> gilt folgende Lösungsfrist:  6 Wochen nach Kündigung werden die personenbezogenen Daten auf der/den physischen Festplatten eigenständig von H3A nach dem Stand der Technik gelöscht.</p> <p>Für das Produkt <b>vServer(Unmanaged/Managed)</b> gilt folgende Lösungsfrist:</p> <p>4 Wochen nach Kündigung werden die personenbezogenen Daten eigenständig von H3A gelöscht.</p> <p>Drei ist für die Erbringung des Kommunikationsdienstes nach dem Code of Conduct der ISPA selber Verantwortlicher. Hier gelten folgende Lösungsfristen: die Stammdaten werden nach 7 Jahren nach Vertragsbeendigung gelöscht; Verkehrsdaten werden nach 6 Monaten gelöscht. Nähere Informationen entnehmen Sie der Datenschutzerklärung auf <a href="http://www.drei.at/datenschutz">www.drei.at/datenschutz</a>.</p>

## Technische und Organisatorische Maßnahmen zur Datenübermittlung

### A. Vertraulichkeit

<p><b>Zutrittskontrolle</b> Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch:</p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Schlüssel</li> <li><input checked="" type="checkbox"/> Elektrischer Türöffner</li> <li><input checked="" type="checkbox"/> Sicherheitspersonal</li> <li><input checked="" type="checkbox"/> Videoanlage</li> <li><input checked="" type="checkbox"/> Anmeldung beim Empfang mit Personenkontrolle</li> <li><input checked="" type="checkbox"/> Tragen von Firmen-/Besucherausweisen</li> <li><input checked="" type="checkbox"/> Magnet- oder Chipkarten</li> <li><input checked="" type="checkbox"/> Portier</li> <li><input checked="" type="checkbox"/> Alarmanlagen</li> <li><input checked="" type="checkbox"/> Einbruchshemmende Fenster und/oder Sicherheitstüren</li> <li><input checked="" type="checkbox"/> Begleitung von Besuchern im Unternehmensgebäude</li> <li><input type="checkbox"/> Sonstiges: ...</li> </ul>
<p><b>Zugangskontrolle</b> Schutz vor unbefugter Systembenutzung durch:</p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Kennwörter (einschließlich entsprechender Policy)</li> <li><input checked="" type="checkbox"/> Automatischer Sperrmechanismen</li> <li><input checked="" type="checkbox"/> Zwei-Faktor-Authentifizierung</li> <li><input checked="" type="checkbox"/> Verschlüsselung von Datenträgern</li> <li><input type="checkbox"/> Sonstiges: ...</li> </ul>
<p><b>Zugriffskontrolle</b> Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:</p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Standard-Berechtigungsprofile auf „need to know-Basis“</li> <li><input checked="" type="checkbox"/> Protokollierung von Zugriffen</li> <li><input checked="" type="checkbox"/> Periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten</li> <li><input checked="" type="checkbox"/> Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger</li> <li><input checked="" type="checkbox"/> Standardprozess für Berechtigungsvergabe</li> <li><input checked="" type="checkbox"/> Sichere Aufbewahrung von Speichermedien</li> <li><input checked="" type="checkbox"/> Datenschutzgerechte Wiederverwendung von Datenträgern</li> <li><input checked="" type="checkbox"/> Clear-Desk/ Clear-Screen Policy</li> <li><input type="checkbox"/> Sonstiges: ...</li> </ul>
<p><b>Pseudonymisierung</b> Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt.</p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Ja</li> <li><input checked="" type="checkbox"/> Nein</li> </ul>
<p><b>Verschlüsselung der Daten während der Übertragung</b></p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Ja</li> <li><input type="checkbox"/> Nein</li> </ul> <p>Wenn ja, dann Beschreibung des angewendeten Verschlüsselungsprotokolls und der Verschlüsselungsstärke (z.B. nach <a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-">https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-</a></p>

	<a href="#">02102.pdf? blob=publicationFile</a> E-Mail und (Intern) Webinterface via TLS Verschlüsselung. Offen: Welche Version wird verwendet? → AP: G.Schlesier
<b>Verschlüsselung der gespeicherten Daten</b>	<input checked="" type="checkbox"/> Ja <input type="checkbox"/> Nein Wie genau wird verschlüsselt?? → AP: G.Schlesier Wenn ja, dann Beschreibung des angewendeten Verschlüsselungsprotokolls und der Verschlüsselungsstärke ((z.B. nach <a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf? blob=publicationFile">https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf? blob=publicationFile</a> )  <input type="checkbox"/> Schlüssel liegt beim Daten-Exporteur <input type="checkbox"/> Schlüssel liegt beim Daten-Importeur <input checked="" type="checkbox"/> Sonstiges: ... Schlüssel liegt bei H3A
<b>Klassifikationsschema für Daten</b> Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich)	<input checked="" type="checkbox"/> Ja <input type="checkbox"/> Nein
<b>B. Datenintegrität</b>	
<b>Weitergabekontrolle</b> Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:	<input checked="" type="checkbox"/> Verschlüsselung von Datenträgern <input checked="" type="checkbox"/> Virtual Private Networks (VPN) <input checked="" type="checkbox"/> Verschlüsselung von Dateien <input type="checkbox"/> Elektronische Signatur <input type="checkbox"/> Sonstiges: ...
<b>Eingabekontrolle</b> Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch:	<input checked="" type="checkbox"/> Protokollierung <input type="checkbox"/> Dokumentenmanagement <input type="checkbox"/> Sonstiges: ...
<b>C. Verfügbarkeit und Belastbarkeit</b>	
<b>Verfügbarkeitskontrolle</b> Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:	<input checked="" type="checkbox"/> Backup-Strategie (online/offline; on-site/off-site) <input checked="" type="checkbox"/> Virenschutz <input checked="" type="checkbox"/> Meldewege und Notfallpläne <input checked="" type="checkbox"/> Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum <input checked="" type="checkbox"/> Unterbrechungsfreie Stromversorgung (USV, Dieselaggregat) <input checked="" type="checkbox"/> Firewall <input checked="" type="checkbox"/> Security Checks auf Infrastruktur- und Applikationsebene <input checked="" type="checkbox"/> Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern

	<input type="checkbox"/> Sonstiges: ...
<b>Rasche Wiederherrstellbarkeit</b>	<input checked="" type="checkbox"/> Ja <input type="checkbox"/> Nein
<b>D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung</b>	
<b>Datenschutz-Management</b> , einschließlich regelmäßiger Mitarbeiter-Schulungen	<input checked="" type="checkbox"/> Ja <input type="checkbox"/> Nein
<b>Informationssicherheits-Zertifizierung</b> (beispielsweise ISO 27001)	<input checked="" type="checkbox"/> Ja <input type="checkbox"/> Nein Wenn ja, welche: ISO 27001
<b>Incident-Response-Management</b>	<input checked="" type="checkbox"/> Ja <input type="checkbox"/> Nein
<b>Datenschutzfreundliche Voreinstellungen</b> (Data Privacy by Default)	<input checked="" type="checkbox"/> Ja <input type="checkbox"/> Nein
<b>Auftragskontrolle</b> Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung und Überbindung der Verpflichtungen des Verantwortlichen durch:	<input type="checkbox"/> Eindeutige Vertragsgestaltung <input type="checkbox"/> Strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS) <input type="checkbox"/> Nachkontrollen <input type="checkbox"/> Formalisiertes Auftragsmanagement <input type="checkbox"/> Vorabüberzeugungspflicht <input checked="" type="checkbox"/> Sonstiges: Keine Datenverarbeitung über Auftragsverarbeiter
<b>Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen</b>	<input checked="" type="checkbox"/> Ja, folgende Maßnahmen werden gesetzt: interne Audits, sowie ISO 27001 Zertifizierungs-Audits <input type="checkbox"/> Nein
<b>E. Zusätzliche Maßnahmen</b>	
Bestellung eines/r <b>Datenschutzbeauftragten</b> gem. Art 37 bis 39 DSGVO	<input checked="" type="checkbox"/> Ja <input type="checkbox"/> Nein
Erstellung von <b>Verfahrensverzeichnissen</b> gem. Art 30 DSGVO oder – sofern nicht anwendbar – vergleichbare Dokumentationsmaßnahmen	<input checked="" type="checkbox"/> Erstellung von Verfahrensverzeichnissen <input type="checkbox"/> Erstellung einer vergleichbaren Dokumentation <input type="checkbox"/> Nein

Prozess zur Sicherstellung der <b>Meldeverpflichtungen</b> bei Datensicherheitsverletzun- gen gem. Artikel 33 und 34 DSGVO bzw. VO 611/2013.	<input checked="" type="checkbox"/> Ja <input type="checkbox"/> Nein
Auftragsverarbeiter mit Sitz außerhalb der EU haben einen Verantwortlichen Vertreter gemäß Art 27 DSGVO in der EU bestellt	<input checked="" type="checkbox"/> Nicht anwendbar, da es keinen Auftragsverarbeiter mit Sitz außerhalb der EU gibt <input type="checkbox"/> Ja <input type="checkbox"/> Nein

**Anhang 2:**

Auflistung von weiteren Auftragsverarbeitern, die vom Verantwortlichen mit Abschluss dieser Vereinbarung als genehmigt anzusehen sind:

<b>Name des Weiteren Auftragsverarbeiters</b>	<b>Anschrift</b>	<b>Leistung</b>	<b>Land, in dem personenbezogene Daten verarbeitet werden.</b>

Es werden keine weiteren Auftragsverarbeiter beauftragt.