Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DS-GVO

zwischen

(Firma, Inhaber/gesetzlicher Vertreter, Adresse, E-Mail-Adresse)

- **Verantwortlicher** - nachstehend ***Auftraggeber*** genannt -

und

intersaar GmbH

vertreten durch die Geschäftsführung Andrea Schilling und Volker Musebrink

Heinrich-Barth-Straße 23

66115 Saarbrücken

- **Auftragsverarbeiter** - nachstehend ***Auftragnehmer*** genannt

Präambel

Der Auftragnehmer ist Internet Service Provider und betreibt daneben mehrere Rechenzentren, in welche der Auftraggeber Datenbestände und komplexe Datenverarbeitungen auslagern kann. Er verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i. S. d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i. S. d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

1. Gegenstand und Dauer des Auftrags

Der Auftrag umfasst – je nach Tarif und vereinbarten Leistungen – Folgendes:

☐ **Bereitstellung von Speicherplatz auf einem Server**

☐ **Bereitstellung von virtuellen Dienst-Servern mit/ohne Wartungsleistungen**

☐ **Webhosting-Dienstleistungen** (Webdienste, E-Mail-Adressen, Zugang zu Webspace via FTP und SSH, SQL-Datenbank, Zugriff auf Control Panel, Bestellung/Registrierung von Domains sowie weitere im Zusammenhang stehende Leistungen)

☐ **Hosting von Webkonferenz-Software zur Durchführung von Online Meetings (Video-/Audiokonferenzen, Webinaren u. ä.)**

☐ sonstiges: ……

Einzelheiten zum Leistungsumfang ergeben sich aus dem jeweils zugrundeliegenden Leistungsvertrag (Hauptvertrag).

Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages. Dabei werden die vom Auftraggeber zur Verfügung gestellten personenbezogenen Daten nicht vom Auftragnehmer bearbeitet; vielmehr beschränkt sich die Verarbeitung auf Hosting, Support und Administration von Serversystemen, Erstellen von Backups, Web-Statistiken und Log-Daten, wobei ein (unbeabsichtigter) Zugriff auf personenbezogene Daten nicht gänzlich ausgeschlossen werden kann.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrages. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Art der Verarbeitung (Art. 4 Nr. 2 DS-GVO)

Die regelmäßige Verarbeitung besteht im Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Ändern, Offenlegen durch Übermitteln, Verbreiten oder sonstiges Bereitstellen sowie dem Löschen von Daten.

Art der personenbezogenen Daten (Art. 4 Nr. 1, 13, 14 und 15 DSGVO)

In der Regel werden folgende Arten von personenbezogenen Daten im Auftrag verarbeitet:

☐ Personenstammdaten (Vornamen, Nachnamen, Adressen usw.)

☐ Kommunikationsdaten (z.B. Telefon, E-Mail)

☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

☐ Kundenhistorie, Bestelldaten, Protokolldaten, Logins, Abrechnungs- und Zahlungsdaten

☐ IP-Adressen, Browser-Versionen

☐ Planungs- und Steuerungsdaten

☐ Bilddaten/Audiodaten

☐ sonstige: ……

Insbesondere bei der Erbringung von Rechenzentrumsleistungen hängt die Art der personenbezogenen Daten davon ab, was von Seiten des Auftraggebers an Daten zur Verfügung gestellt wird; grundsätzlich kommt daher die Verarbeitung aller Arten von Informationen und personenbezogenen Daten (auch Daten besonderer Kategorien) in Betracht.

Kategorien betroffener Personen (Art. 4 Nr. 1 DS-GVO)

☐ Interessenten und Kunden des Auftraggebers (bzw. deren Mitarbeiter)

☐ Beschäftigte des Auftraggebers

☐ Lieferanten des Auftraggebers (bzw. deren Mitarbeiter)

☐ Webseitenbesucher

☐ Teilnehmer an Webkonferenzen o. ä.

☐ sonstige: ……

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. In dringlichen Fällen ausnahmsweise mündlich erteilte Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

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

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungen des Auftraggebers sind nur beachtlich, wenn sie von einem Weisungsberechtigten an einen empfangsberechtigten Adressaten beim Auftragnehmer gerichtet werden. Der entsprechende Personenkreis zum Zeitpunkt des Vertragsabschlusses ist in der **Anlage Weisungsberechtigte und Weisungsempfangsberechtigte** definiert.

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht

eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Werden dem Auftragnehmer Datenträger überlassen, werden diese, sofern sie vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

Jährliche Prüfung des betrieblichen Datenschutzbeauftragten hinsichtlich aller ergriffenen technischen und organisatorischen Maßnahmen. Umsetzung einer regelmäßigen Evaluierung, Bewertung und Verbesserung. Regelmäßige Kontrolle etwaiger Subunternehmer

Das Ergebnis der Kontrollen ist zu dokumentieren.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an eine vom Auftraggeber zu benennende Person beim Auftraggeber weiterzuleiten.

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) wird vom Auftraggeber grundsätzlich gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Sind auf diesen Auftrag besondere Geheimnisschutzregeln relevant (z. B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse nach § 203 StGB etc.), obliegt es dem Auftraggeber, dem Auftragnehmer dieses mitzuteilen und die gesonderte Verpflichtung des Auftragnehmers auf deren Einhaltung zu initiieren.

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragnehmer ist als Beauftragter für den Datenschutz bestellt:

RA Stefan Wiesen, 0681 – 685 704 01, datenschutz@ra-wiesen.de

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DS-GVO unverzüglich zu informieren.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 32 bis 36 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen:

Nach Vertragsschluss erfolgen regelmäßig Folgekontrollen, und zwar grundsätzlich jährlich. Ausgenommen davon sind umfassend im Datenschutz zertifizierte Subunternehmer, deren Kontrolle im Wesentlichen auf der Grundlage eines externen Gutachtens durchgeführt werden kann. Die Kontrolle durch den Auftragnehmer erfolgt in diesem Fall synchron zur Laufzeit der Zertifizierung. Kontrollen werden im Übrigen durch (vom Subunternehmen zu belegenden) Selbstauskünfte des Subunternehmens auf der Grundlage von Fragebögen des Auftragnehmers durchgeführt, darüber hinaus auch durch Vor-Ort-Kontrollen.

Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragnehmer die in **Anlage Unterauftragnehmer** mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

Die Information hinsichtlich einer beabsichtigten Änderung erfolgt spätestens einen Monat vor dem Zeitpunkt der geplanten Übergabe der Daten schriftlich oder in Textform. Die Änderung ist zulässig, wenn der Auftraggeber nicht bis zwei Wochen vor dem Zeitpunkt der geplanten Übergabe der Daten dem Auftragnehmer gegenüber schriftlich oder in Textform Einspruch erhebt.

Im Falle des Einspruchs des Auftraggebers gegen die geplante Änderung steht dem Auftragnehmer ein außerordentliches Kündigungsrecht sowohl hinsichtlich dieser Vereinbarung als auch bezüglich des Hauptvertrages zu; Ansprüche des Auftraggebers auf Schadenersatz sind in diesem Fall ausgeschlossen, soweit der Einspruch nicht auf einem wichtigen datenschutzrechtlichen Grund beruht.

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt:

Auf der Grundlage eines Verfahrens zur Risikoanalyse identifiziert der Auftragnehmer aus den generellen Risikoquellen die relevanten Bedrohungen (Möglichkeit, dass ein Schaden entsteht) für Vertraulichkeit, Integrität und Verfügbarkeit (Belastbarkeit). Die Eintrittswahrscheinlichkeit wird systematisch ermittelt und auf dieser Basis eine Risikobewertung vorgenommen.

In der **Anlage TOM** wird die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dargestellt.

Das in der Anlage beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt.

Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt Auditbericht können vom Auftraggeber auf Wunsch eigesehen werden.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen. Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen, datenschutzgerecht zu löschen bzw. zu vernichten oder vernichten zu lassen. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Haftung

Die Haftung des Auftragnehmers ist beschränkt auf Fälle, in denen er, seine Mitarbeiter, Erfüllungsgehilfen oder ein weiterer Auftragsverarbeiter schuldhaft seinen speziell auferlegten Pflichten aus der DS-GVO nicht nachgekommen ist oder er erteilten Weisungen des Auftraggebers nicht beachtet hat oder Weisungen des Auftraggebers zuwidergehandelt hat.

Der Auftragnehmer ist von der Haftung befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Sind sowohl Auftraggeber als auch Auftragnehmer für einen Schaden verantwortlich, der bei gemeinsamer Beteiligung an einer Verarbeitung entstanden ist, so haften beide der betroffenen Person gegenüber als Gesamtschuldner; sie haften im Innenverhältnis entsprechend ihrem Anteil an der Verantwortung für den Schaden.

12. Sonstige Regelungen

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten 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.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Soweit gesetzlich zulässig vereinbaren die Parteien Saarbrücken als ausschließlichen Gerichtsstand.

Datum:

Unterschriften

……..

Auftraggeber **intersaar GmbH**

Anlage Unterauftragnehmer

Der Auftraggeber stimmt folgenden Unterauftragnehmern zu:

Name	Anschrift/Land	Leistung

Anlage Weisungsberechtigte und Weisungsempfangsberechtigte

Weisungsberechtigte Personen des Auftraggebers sind (mangels konkreter Angabe nur der im Rubrum dieser Vereinbarung aufgeführte Auftraggeber persönlich (ggf. gesetzlicher Vertreter)):
Weisungsempfangsbefugte Personen beim Auftragnehmer sind:
- Andrea Schilling, Gf., Tel. 0681 9461 0, a.schilling@intersaar.net - Volker Musebrink, Gf., Tel. 0681 9461 0, v.musebrink@intersaar.net - ….

Anlage TOM

Darstellung der technischen und organisatorischen Maßnahmen (*05/2020)*

Zugangskontrolle

Wie verhindert das Unternehmen, dass Unbefugte Zutritt oder Zugang zu Rechnern oder Akten erhalten?

Die Rechenzentren befinden sich an verschiedenen Standorten und sind zum Teil unterirdisch gelegen. Der Zugang verfügt über Sicherheitsschlösser. Der Zugang erfolgt über ein Transponder-Schließsystem. Der zutrittsberechtigte Personenkreis ist festgelegt. Die Ausgabe von Transpondern ist im Berechtigungssystem geregelt und wird dokumentiert. Der Zugang ist weiter per Videoüberwachung gesichert. Der Zutritt zu Rechenzentren ist nur in Begleitung von autorisiertem Personal statthaft. Server sind nur über ein mehrstufiges Schließsystem zu erreichen (Gebäude, Serverräume, Serverschränke).

Die Geschäftsräume des Unternehmens befinden sich im Erdgeschoss und im Obergeschoss eines Geschäftsgebäudes. Die Erdgeschossfenster sind einbruchssicher, Gebäudeschächte abgesichert. Das Gebäude verfügt über eine Alarmanlage. Das Gebäude ist mit Bewegungsmeldern und Videoüberwachung gesichert.

Der Gebäudezugang verfügt über Sicherheitsschlösser. Der Zugang erfolgt über ein Transponder-Schließsystem. Der zutrittsberechtigte Personenkreis ist festgelegt. Die Ausgabe von Transpondern ist im Berechtigungssystem geregelt und wird dokumentiert. Besucher werden persönlich in Empfang genommen und am Eingang kontrolliert. In Besprechungs- und Wartebereichen besteht kein Zugang zu Akten oder Daten. Physische Akten sind in absperrbaren Aktenschränken untergebracht.

Für den Zugang zu Einzelrechnern ist eine Anmeldung durch den Sachbearbeiter erforderlich. Die Authentifizierung ist in einer Passwortrichtlinie geregelt, die unter anderem Länge und Komplexität von Zugangsdaten sowie den Umgang mit diesen regelt. Der Arbeitsplatz wird nach spätestens 5 Minuten automatisch gesperrt.

Reinigungspersonal ist sorgfältig ausgewählt und zur Vertraulichkeit verpflichtet.

Datenträgerkontrolle

Wie verhindert das Unternehmen, dass Unbefugte Datenträger (auch Akten) lesen, kopieren, verändern oder löschen?

Für den Zugang zu Servern besteht ein Berechtigungskonzept. Nur autorisiertes Personal mit Administratorenberechtigung hat Zugang. Zugangsberechtigungen werden laufend überwacht und nötigenfalls korrigiert. Die Authentifikation erfolgt durch Benutzername/Passwort. Passwörter werden verschlüsselt gespeichert. Externe Zugriffe sind nur durch autorisiertes Personal mit VPN-Zugang möglich. Zugriffe werden protokolliert und anlassbezogen ausgewertet. Es werden Firewall-Systeme eingesetzt. Eine Übertragung von Serverdaten auf externe Medien findet nicht statt. Backup-Konzept Storage-Systeme sind ohne externe Zugriffsmöglichkeit.

Im Geschäftsbetrieb werden folgende Vorkehrungen getroffen: Datenträger, gleich welcher Art, insbesondere aber mobile, werden verschlossen aufbewahrt. Kopien werden nur gefertigt, wenn dies für den Geschäftsablauf unabdingbar ist. Mobile Datenträger, z. B. USB-Sticks, werden nur restriktiv gebraucht und sicher gelöscht (bzw. vernichtet), wenn sich ihr Gebrauch erledigt hat. Die Ausgabe von mobilen Speichermedien ist dokumentiert. Sofern mobile Datenträger personenbezogene Daten enthalten, werden diese Inhalte verschlüsselt. Das gilt auch für die Verwendung mobiler IT-Systeme, wie Notebooks, Tablets, Smartphones.

Geräte, die Speichermedien enthalten (Rechner, mobile Datenträger, eventuell Drucker oder Multifunktionsgeräte) verlassen nach ihrer Ausmusterung erst das Unternehmen, wenn die Speicher sicher gelöscht oder physisch unbrauchbar gemacht worden sind. Leasing-Geräte mit Speichermedien werden erst zurückgegeben, wenn alle enthaltenen Speicher mit einem sicheren Verfahren gelöscht sind.

Für die Entsorgung von Papiermüll stehen geeignete Aktenvernichter (mindestens Sicherheitsstufe 3) zur Verfügung, größere Mengen werden über einen zertifizierten Entsorgungsbetrieb gegen ein Entsorgungsprotokoll vernichtet, wobei für den Transport speziell dafür vorgesehene abgesperrte Behältnisse verwendet werden (DIN 66399).

Speicherkontrolle

Wie ist sichergestellt, dass nicht Unbefugte von gespeicherten Daten Kenntnis nehmen oder diese eingeben, verändern oder löschen?

Alle Einzelplatzrechner verfügen über eine Bildschirm- bzw. Rechnersperre, die automatisch nach einem definierten Zeitraum bei Verlassen des Arbeitsplatzes greift. Der befugte Benutzer muss sich am Rechner identifizieren. Die Zugangskriterien sind in der Passwortrichtlinie definiert.

Bei der Speicherung von Daten kommt, wenn möglich, Verschlüsselungstechnik zur Anwendung. In einem differenzierten Berechtigungskonzept ist festgelegt, wer von welchen Daten Kenntnis nehmen darf und ggf. Daten eingeben, verändern oder löschen darf. Die Berechtigungen werden vom Administrator auf Weisung der Geschäftsleitung eingerichtet. Die Zahl der Administratoren ist auf ein Minimum beschränkt.

Ein Löschkonzept gibt unter Berücksichtigung unter anderem der gesetzlichen Löschfristen vor, nach welchem Modus Daten bestimmter Kategorien regelmäßig gelöscht werden. Die Löschung wird protokolliert.

Benutzerkontrolle

Wie stellt das Unternehmen sicher, das durch die Verwendung von Verarbeitungssystemen keine Daten unbefugt übertragen werden (zum Beispiel über das Internet), also abfließen?

Das Berechtigungskonzept legt die zugangsberechtigten Mitarbeiter fest, die sich bei der Benutzung eines Systems identifizieren müssen. Es ist gewährleistet, dass ausscheidende Mitarbeiter oder solche, die in einen anderen Arbeitsbereich wechseln, umgehend gesperrt werden. Gegen Angriffe kommen Firewall-Technologie, Antivirensoftware und Spamfilter zur Anwendung.

Zugriffskontrolle

Wie stellt das Unternehmen sicher, dass berechtigte Personen nur auf diejenigen Daten Zugriff haben, für die sie auch berechtigt sind (Need-to-Know-Prinzip)?

Jeder Mitarbeiter hat nur Zugriff auf diejenigen personenbezogenen Daten, die für seine Tätigkeit von Belang sind. Dies wird durch das Berechtigungskonzept, welches nach Möglichkeit technisch umgesetzt wird, gewährleistet. Die Verwaltung der Rechte erfolgt durch den Systemadministrator. Zugriffe auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten werden protokolliert.

Übertragungskontrolle

Wie stellt das Unternehmen sicher und überprüft, dass Daten bei der Übertragung nur an berechtigte Empfänger übermittelt werden?

Personenbezogene Daten dürfen nur an berechtigte Empfänger übermittelt werden. Auf welchem Übertragungsweg (Normalpost, Paket, Bote, elektronische Übertragung, Fax usw.) sie übermittelt werden, ist von der Geschäftsleitung mit Blick auf ihren Schutzbedarf festgelegt. Mitarbeiter sind sensibilisiert, hinsichtlich aller Übertragungswege, die Richtigkeit der Adressdaten vor Absendung wiederholt zu überprüfen. Jedenfalls personenbezogene Daten mit mittlerem bis hohem Schutzbedarf werden bei elektronischer Übermittlung verschlüsselt übertragen (E-Mail Verschlüsselung, tls-verschlüsselte Übermittlung, VPN-Technologie).

Eingabekontrolle

Wie stellt das Unternehmen sicher, dass nachvollziehbar ist, welcher Benutzer auf welche Daten zu welchem Zeitpunkt zugegriffen hat, wenn mehrere Benutzer auf Systeme und personenbezogene Daten zugreifen können?

Die Eingabe, Änderung und Löschung von Daten im Rechenzentrumsbetrieb wird protokolliert. Personenbezogene Daten werden nur durch Systemprozeduren erzeugt (z.B. automatisierte Erfassung von Verbrauchswerten etc.). Eingaben in kundeneigene Systeme oder Root-Server werden ggf. vom Kunden selbst protokolliert.

Im allgemeinen Geschäftsbetrieb werden Eingabe, Änderung und Löschung von Daten in Systeme protokolliert. Rechte zur Eingabe, Änderung und Löschung von Daten werden auf der Basis des Berechtigungskonzepts vergeben. Durch individuelle Benutzernamen ist nachvollziehbar, wer die Eingabe, Änderung und Löschung von Daten vorgenommen hat.

Transportkontrolle

Wie stellt das Unternehmen sicher, dass bei Datenübermittlung oder Transport (auf Datenträgern) diese beim berechtigten Empfänger ankommen?

Übertragungsleitungen zwischen den Rechenzentren sind gesichert. Externe Zugriffe sind nur über VPN-Tunnel möglich und damit bei der Übermittlung gesichert. Datenverbindungen werden protokolliert. Ein physischer Transport von Datenträgern erfolgt grundsätzlich nicht.

Im allgemeinen Geschäftsablauf erfolgt die elektronische Übermittlung von Daten mit mittlerem bis hohen Schutzbedarf zumindest als verschlüsselter Anhang zu einer E-Mail, wobei der Schlüssel auf anderem Wege (z. B. telefonisch) an den berechtigten Empfänger übermittelt wird. Vorzugsweise erfolgt die elektronische Übermittlung durch eigens etablierte Systeme. Gegebenenfalls kommt VPN-Technologie zum Einsatz.

Wichtige Unterlagen können per zuverlässigen Boten verschlossen übermittelt werden. Soweit mobile Datenträger (CD-ROM, USB-Stick o.ä.) ausnahmsweise zur Anwendung kommen, werden die Inhalte verschlüsselt. Der Eingang der übertragenen Daten beim berechtigten Empfänger wird nötigenfalls durch Rückfrage verifiziert.

Rasche Wiederherstellbarkeit

Wie stellt das Unternehmen sicher, dass IT Systeme (inkl. der gespeicherten personenbezogenen Daten) nach einem Zwischenfall in einem akzeptablen Zeitrahmen wiederhergestellt werden können?

Es besteht ein Serverkonzept mit Host- und Gastmaschinen. Die Wiederherstellung von verlorenen oder beschädigten Daten ist zeitnah aus dem Backup auch auf Ersatzmaschinen möglich.

Der Datenbestand des Unternehmens selbst wird auf Server vorgehalten. Alle im Rahmen des Geschäftsbetriebs verarbeiteten personenbezogenen Daten und Informationen werden täglich hinsichtlich der Änderungen gesichert und wöchentlich vollgesichert.

Die Datenwiederherstellung aus Backups wird regelmäßig darauf überprüft, ob sie mit vertretbaren Mitteln und im akzeptablen Zeitrahmen möglich ist.

Zuverlässigkeit

Wie verhindert das Unternehmen, dass Funktionen des Systems nicht zur Verfügung stehen und auftretende Fehlfunktionen nicht gemeldet werden?

Um Fehlfunktionen des Systems zu vermeiden, kommt Software zum Einsatz, die Angriffen und Schäden entgegenwirkt. Fehlfunktionen werden automatisiert gemeldet.

Datenintegrität

Wie stellt das Unternehmen sicher, dass es durch Fehlfunktionen keine Beeinträchtigungen an den personenbezogenen Daten gibt?

Sicherheitsupdates und -patches der Hersteller der Betriebssysteme, sonstiger Software und Anwendungen werden automatisch eingespielt. Sonstige Updates werden ggf. nach vorangegangener Notwendigkeitsprüfung installiert.

Auftragskontrolle

Wie stellt das Unternehmen sicher, dass im Auftrag verarbeitete personenbezogene Daten entsprechend den Weisungen verarbeitet werden?

Wir als Auftragnehmer

Soweit das Unternehmen personenbezogene Daten im Auftrag für andere Unternehmen verarbeitet, ist gewährleistet, dass dies nur auf der Grundlage einer gesetzeskonformen Vereinbarung zur Auftragsverarbeitung und von Weisungen des Auftraggebers erfolgt.

Nach Beendigung des Auftrags werden die vorgehaltenen Daten sicher gelöscht (durch mindestens siebenmaliges Überschreiben). Die Löschung kann dem Auftraggeber nachgewiesen werden. Physische Datenträger, wie Papierdokumente, werden mit einem Aktenvernichter mindestens der Sicherheitsstufe 3 vernichtet.

Wir als Auftraggeber

Soweit externe Dienstleister in Anspruch genommen werden, sind diese sorgfältig ausgewählt im Hinblick auf ihre Eignung und darauf, dass sie hinreichende Garantien hinsichtlich der Einhaltung der Anforderungen des Datenschutzes bieten. Die beim Dienstleister ergriffenen technischen und organisatorischen Maßnahmen müssen detailliert nachgewiesen werden. Im Falle der ausgelagerten Verarbeitung von personenbezogenen Daten werden mit diesen Dienstleistern Vereinbarungen gemäß Art. 28 DSGVO geschlossen. Etwa darüberhinausgehende Weisungen werden dokumentiert.

Dienstleister werden in festgelegten Zeitabständen, die sich etwa an der Laufzeit von Zertifikaten orientieren, kontrolliert im Hinblick darauf, ob sie die Grundsätze für die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung einhalten.

Sofern es sich bei den Dienstleistern nicht um Auftragsverarbeiter handelt, werden diese zumindest auf Vertraulichkeit verpflichtet.

Verfügbarkeitskontrolle

Wie gewährleistet das Unternehmen, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind?

Die Unternehmensräume verfügen über eine Feuer- und Rauchmeldeanlage, Serverräume darüber hinaus über Löschgeräte. Wasserschäden durch Hochwasser oder Sanitäranlagen oder (Ab-)Wasserleitungen in der Nähe sind nicht zu besorgen. Serverräume sind klimatisiert und temperatur- und feuchtigkeitsüberwacht. Eine unterbrechungsfreie Stromversorgung, gewährleistet, dass Serversysteme im Falle eines Stromausfalles zumindest geregelt herunterfahren. Überspannungsschutz und Schutzsteckdosen sind installiert. Das Backup-Konzept sieht eine Spiegelung vor auf Servern in getrennten Räumen oder Gebäuden. Backup-Systeme werden regelmäßig überwacht.

In einem Notfallplan ist das Verhalten der Beteiligten im Falle eines Elementarereignisses, Angriffs, Einbruchs oder Diebstahls und anderer Sicherheitsereignisse geregelt und ein Meldeverfahren etabliert.

Trennbarkeit

Wie stellt das Unternehmen sicher, dass Daten, die zu unterschiedlichen Zwecken verarbeitet werden, getrennt voneinander verarbeitet werden?

Im Rechenzentrumsbetrieb werden Daten nur zu Abrechnungszwecken erhoben (z.B. Speichernutzung von Postfächern, verbrauchtes Datenvolumen, verbrauchte Gesprächsminuten). Daten aus Log-Dateien werden automatisiert in regelmäßigen Abständen gelöscht und dienen nur der Analyse im Störfall. Zur Abrechnung relevante Daten werden in Datenbanken auf jeweils getrennten Systemen gespeichert. Zu einem bestimmten Zweck erhobene Datenbestände werden physikalisch getrennt auf gesonderten Systemen, Partitionen oder Datenträgern gespeichert. Datenbankberechtigungen werden festgelegt.

Pseudonymisierung

Wie wird sichergestellt, dass – wenn immer möglich - personenbezogene Daten nicht ohne Hinzuziehung zusätzlicher Informationen einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen?

Im Rechenzentrumsbetrieb werden personenbezogenen Daten nur zu Abrechnungszwecken erhoben (z.B. Speichernutzung von Postfächern, verbrauchtes Datenvolumen, verbrauchte Gesprächsminuten). Abrechnungsrelevante Daten werden jeweils mit der zugehörigen Kundennummer als Referenz aufbewahrt. Stammdaten zu den Kundennummern sind nur durch Mitarbeiter mit Zugang zum internen ERP- oder Buchhaltungssystem abrufbar.

Mitarbeiterunterweisung

Wie stellt das Unternehmen sicher, dass Mitarbeiter personenbezogene Daten nicht ohne Anweisung oder gesetzliche Pflicht verarbeiten?

Alle Mitarbeiter sind auf Vertraulichkeit nach den Datenschutzbestimmungen hin verpflichtet und über ein Merkblatt über ihre Verpflichtungen im Umgang mit personenbezogenen Daten umfassend unterrichtet.

Eine IT-Nutzer-Richtlinie gibt Mitarbeitern Regeln für die Benutzung der Infrastruktur an die Hand.

Mitarbeiter erhalten konkrete Arbeitsanweisungen zum datenschutzkonformen Umgang mit Daten und regelmäßige, zumindest jährliche Schulungen oder Unterweisungen. Darüber hinaus werden sie über wesentliche Neuerungen informiert und in besonders anfälligen Bereichen sensibilisiert. Die Einhaltung der Vorgaben wird kontrolliert.

Regelmäßige Überprüfung, Bewertung und Evaluierung

Welches Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung wird eingesetzt?

Ein Datenschutzbeauftragter ist benannt. Eine Leitlinie sowie konkretisierende Richtlinien sind in Kraft gesetzt. Regelungen zu internen Verantwortlichkeiten und Zuständigkeiten sind getroffen. Prozesse sind definiert z.B. mit Blick auf Betroffenenrechte, Datenschutzverletzungen, Informationspflichten und Löschen.

Ein Verzeichnis aller Verarbeitungen ist erstellt und wird gepflegt.

Ein Prozess zur kontinuierlichen Verbesserung ist etabliert. In dessen Rahmen werden in der Regel jährlich auch die ergriffenen technischen und organisatorischen Maßnahmen einer Bewertung unterzogen.