Ministerium für Inneres, Bauen und Sport

SAARLAND

Vereinbarung zur Auftragsverarbeitung

gemäß Artikel 28 Absatz 3 DS-GVO

zwischen

dem Saarland,
vertreten durch das Ministerium für Inneres, Bauen und Sport

- nachfolgend Auftraggeber genannt -

und

_____

(Name, Anschrift, vertreten durch)

- nachfolgend Auftragnehmer genannt -

Inhaltsverzeichnis

Präambel
1. Gegenstand und Dauer
2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen
3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers
4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers
5. Pflichten des Auftragnehmers
6. Kontrollrechte des Auftraggebers und Nachweismöglichkeiten des Auftragnehmers
7. Mitteilungs- und Handlungspflichten des Auftragnehmers bei Störungen der Verarbeitung und Verletzungen des Schutzes personenbezogener Daten
8. Anfragen betroffener Personen
9. Zusammenarbeit mit der Aufsichtsbehörde und Beachtung der Vorschriften des Saarländischen Datenschutzgesetzes (SDSG)
10. Führen des Verzeichnisses von Verarbeitungstätigkeiten
11. Einsatz von Subunternehmern
12. Technische und organisatorische Maßnahmen nach Artikel 32 DS-GVO
13. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Artikel 28 Absatz 3 Satz 2 lit. g) DS-GVO
14. Haftung / Schadenersatz / Geldbuße
15. Schlussbestimmungen
16. Anlagen

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz in Bezug auf Auftragsverarbeitung, die sich aus der Vertragsbeziehung zwischen dem Auftraggeber und dem Auftragnehmer und allen dieser Vertragsbeziehung zugrundeliegenden Verträge inklusive aller Anlagen (im Folgenden „Vertrag“ genannt) ergibt. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte personenbezogene Daten („Daten“) des Auftraggebers verarbeiten („Auftragsverarbeitung“).

1. Gegenstand und Dauer

1.1 Gegenstand der Auftragsverarbeitung

Der Auftragnehmer erbringt für den Auftraggeber Leistungen auf Grundlage des Vertrags EVB-IT Systemvertrag über die Erstellung eines Gesamtsystems „Computer Aided Facility Management Software – System (CAFM–Software)“ vom _____ („Hauptvertrag“). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und der dazugehörigen Leistungsbeschreibung). Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.
Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

Diese Vereinbarung gilt auch, sofern die jeweiligen vertraglichen Vereinbarungen des Hauptvertrages nicht ausdrücklich Bezug nehmen auf diese Vereinbarung zur Auftragsverarbeitung.

1.2 Der Auftragnehmer verarbeitet dabei personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Artikel 4 Nummer 2 und Artikel 28 DS-GVO auf Grundlage dieser Vereinbarung.

Die Verarbeitung kann im Rahmen eines Rechenzentrumsbetriebs des Auftragnehmers, über Fernwartung oder durch sonstige Leistungen des Auftragnehmers beim Auftraggeber wie z.B. Installationen vor Ort stattfinden.

1.3 Die diesem Vertrag zugrundeliegenden Leistungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Leistungen oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artikel 44 ff. DS-GVO erfüllt sind. Die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitung bleiben unberührt.

Sofern die Datenverarbeitung nach dieser Vereinbarung und den gesetzlichen Vorgaben zur Verarbeitung personenbezogener Daten im Auftrag bzw. zur Übermittlung personenbezogener Daten in das Ausland zulässig außerhalb Deutschlands erbracht werden darf, wird der Auftragnehmer für die Einhaltung und Umsetzung der gesetzlichen Erfordernisse zur Sicherstellung eines adäquaten Datenschutzniveaus bei Standortverlagerungen und bei grenzüberschreitendem Datenverkehr Sorge tragen.

1.4 Dauer der Auftragsverarbeitung

Die Laufzeit dieser Vereinbarung richtet sich grundsätzlich nach der Laufzeit des zugrundeliegenden Hauptvertrages und gilt solange eine Vertragsbeziehung zwischen dem Auftraggeber und dem Auftragnehmer besteht. Spezifische Vorschriften dieser Vereinbarung, die nach Beendigung des Vertrages greifen, bleiben hiervon unberührt.

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus dieser Vereinbarung nicht nachkommt, Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

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

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben im Hauptvertrag vom _____ .

2.2 Art der personenbezogenen Daten:

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenarten (z. B.: Adressdaten, Personen-stammdaten, Vertragsstammdaten, Zahlungsdaten …))

☒ Personenstammdaten, Kommunikationsdaten (z.B. Telefon, E-Mail), Adressdaten
☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
☒ Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten
☒ Planungs- und Steuerungsdaten
☒ Beschäftigungs- und Karrieredaten von Externen (Lebensläufe, Qualifikationen, Beschäftigungsstatus, Zertifikate)
☒ Information über erfolgreich durchgeführte einfache Sicherheitsüberprüfung nach §8 SSÜG SL
☐ ….

vgl.: Artikel 4 Nummer 1, 13, 14 und 15 DS-GVO; der Fokus ist insbesondere auf die sensiblen Daten des Artikel 9 DS-GVO zu richten

2.3 Kategorien betroffener Personen:

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☒ Kunden
☒ Mieter
☒ Vermieter
☒ Beschäftigte des Landes und von Externen
☒ Lieferanten / Dienstleister
☒ Ansprechpartner
☒ Unternehmer / Handwerker
☐...

vgl. Artikel 4 Nummer 1 DS-GVO; gemeint sind bestimmte Personengruppen (z. B.: Kunden / Nichtkunden / Kreditnehmer / Beschäftigte)

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

3.1 Für die Beurteilung der Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte der betroffenen Personen nach den Artikeln 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 (Textform) festzulegen.

3.2 Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format (Textform). Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu (Textform) bestätigen.

Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt.

3.3 Der Auftraggeber ist berechtigt, sich - wie unter Punkt 6 festgelegt - 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.

3.4 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen 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 dieser Vereinbarung bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

4.1 Weisungsberechtigte Personen des Auftraggebers sind:

Ministerium für Inneres, Bauen und Sport, Abteilung OBB2, Referat OBB24, Frau ROR'in Sandra Kölle, 0681/501-84080, s.koelle@innen.saarland.de

(Vorname, Name bzw. Funktionsträger, Organisationseinheit, Telefon, E-Mail)

4.2 Der Auftragnehmer nennt dem Auftraggeber Ansprechpartner für im Rahmen dieser Vereinbarung anfallende Weisungen.

Weisungsempfänger beim Auftragnehmer sind:

Klicken oder tippen Sie hier, um Text einzugeben.

(Vorname, Name *bzw. Funktionsträger*, Organisationseinheit, Telefon, E-Mail)

4.3 Für Weisung zu nutzende Kommunikationskanäle sind neben dem üblichen Postweg die Telefonanschlüsse oder E-Mail-Adressen der Weisungsbefugten (4.1) und Weisungsempfänger:

Klicken oder tippen Sie hier, um Text einzugeben.

(genaue postalische Adresse/ E-Mail/ Telefonnummer)

4.4 Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch (Textform) die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragnehmers

5.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden, Artikel 29 DS-GVO); in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Weisungen des Auftraggebers sind beim Auftragnehmer zu dokumentieren (Artikel 28 Absatz 3 Satz 2 lit. a) DS-GVO).

5.2 Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

5.3 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, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

5.4 Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er ist verpflichtet, die personenbezogenen Daten nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

5.5 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird insbesondere technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen des Artikels 32 DSGVO genügen (Artikel 28 Absatz 3 Satz 2 lit. c) DS-GVO). Der Auftragnehmer wird diese technischen und organisatorischen Maßnahmen so treffen, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt sind. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer in dem unter Punkt 12 festgehaltenen Rahmen vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird. Das Ergebnis der Kontrollen ist zu dokumentieren und dem Auftraggeber auf Anforderung vorzulegen.

Bei der Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) sind die Maßnahmen nach Artikel 32 DS-GVO auch in diesem Fall sicherzustellen.

5.6 Bei der Erfüllung der Rechte der betroffenen Personen nach Artikel 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten (Artikel 30 DS-GVO) sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers (Artikel 35 und 36 DS-GVO) hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Artikel 28 Absatz 3 Satz 2 lite) und f) DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten:
Ministerium für Inneres, Bauen und Sport, Referat OBB24 Liegenschaften

5.7 Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Artikel 28 Absatz 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.

5.8 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.

5.9 Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf nur der Auftraggeber erteilen (vgl. Punkt 8).

5.10 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, auch alle relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen (z. B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse nach § 203 StGB etc.).

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.

5.11 Der Auftragnehmer stellt sicher, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und sich diese für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Artikel 28 Absatz 3 Satz 2 lit. b) und Artikel 29 DSGVO, § 13 Satz 2 SDSG). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb**.**

5.12 Datenschutzbeauftragter/Ansprechpartner für den Datenschutz:

Beim Auftragnehmer ist ein betrieblicher Datenschutzbeauftragter/ Ansprechpartner für den Datenschutz (sofern ein Datenschutzbeauftragter nach Art. 37 Abs. 1.DSGVO nicht bestellt werden muss) bestellt. Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung der Auftraggeberin in geeigneter Weise nach.

Klicken oder tippen Sie hier, um Text einzugeben.

(genaue postalische Adresse/ E-Mail/ Telefonnummer)

Ein Wechsel des Datenschutzbeauftragten/ Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

6. Kontrollrechte des Auftraggebers und Nachweismöglichkeiten des Auftragnehmers

6.1 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 – sofern diese nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen – 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 (Artikel 28 Absatz 3 Satz 2 lit. h) DS-GVO).

6.2 Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Er stellt insbesondere sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Artikel 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung innerhalb einer angemessenen Frist die erforderlichen Auskünfte zu

erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

6.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann gegenüber dem Auftraggeber erfolgen durch die Ergebnisse eines Selbstaudits, Zertifikate zu Datenschutz und/oder Informationssicherheit (z.B. ISO 27001), Zertifikate gemäß Artikel 42 DSGVO oder aktuelle Testate und/oder Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheits-abteilung, Datenschutzauditoren, Qualitätsauditoren), genehmigte Verhaltensregeln (Artikel 40 DSGVO) oder verbindliche interne Datenschutzvorschriften (Artikel 47 DSGVO). Ein Wegfall bzw. Änderung entsprechender Ergebnisse hat der Auftragnehmer dem Auftraggeber mitzuteilen.

6.4 Sofern einschlägig verpflichtet sich der Auftragnehmer, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Artikel 41 Absatz 4 DS-GVO und den Widerruf einer Zertifizierung nach Artikel 42 Absatz 7 DS-GVO unverzüglich zu informieren.

6.5 Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die dem Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

7. Mitteilungs- und Handlungspflichten des Auftragnehmers bei Störungen der Verarbeitung und Verletzungen des Schutzes personenbezogener Daten

7.1 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 Artikel 33 und Artikel 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Artikel 33 und 34 DS-GVO angemessen zu unterstützen (Artikel 28 Absatz 3 Satz 2 lit. f) DS-GVO). Meldungen aus dem Auftragsverhältnis nach Artikel 33 oder 34 DS-GVO darf nur der Auftraggeber durchführen.

7.2 Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7.3 Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber

und ersucht um weitere Weisungen. Über wesentliche Änderung der Sicherheitsmaßnahmen hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

7.4 Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten von einer Verletzung nach Punkt 7.1 betroffen sind.

8. Anfragen betroffener Personen

Soweit sich eine betroffene Person zwecks Geltendmachung der Betroffenenrechte unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer die betroffene Person über seine Unzuständigkeit informieren und an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber auf Basis der Angaben der betroffenen Person möglich ist. Gemäß Punkt 5 dieser Vereinbarung unterstützt der Auftragnehmer den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen.

9. Zusammenarbeit mit der Aufsichtsbehörde und Beachtung der Vorschriften des Saarländischen Datenschutzgesetzes (SDSG)

9.1 Auftraggeber und Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

9.2 Der Auftragnehmer gewährleistet die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt, anfragt oder sonstige Erkundigungen einzieht.

9.3 Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

9.4 Der Auftragnehmer verpflichtet sich zur Beachtung der Vorschriften des Saarländischen Datenschutzgesetzes in der jeweils geltenden Fassung (§ 4 Absatz 4 SDSG).

10. Führen des Verzeichnisses von Verarbeitungstätigkeiten

Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung. Der Auftragnehmer führt entsprechend den Vorgaben des Artikels 30 Absatz 2 DS-GVO ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

11. Einsatz von Subunternehmern

11.1 Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt.

Ein Subunternehmerverhältnis im Sinne dieser Vereinbarung liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der Verarbeitung personenbezogener Daten (im Auftrag des Verantwortlichen) ganz oder teilweise beauftragt.

11.2 Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

11.3 Kein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind (z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen) und keinen konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, haben.

11.4 Von der Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers setzt der Auftragnehmer den Auftraggeber vorab in Kenntnis. Vor Beginn der Verarbeitungstätigkeiten durch den Subunternehmer muss der Auftraggeber der Beauftragung schriftlich oder in dokumentiertem elektronischem Format zugestimmt haben.
Die Kommunikationswege entsprechen denen der Ziff. 4.

11.5 Der Auftragnehmer teilt dem Auftraggeber die bereits bei Abschluss der vorliegenden Vereinbarung bestehende Subunternehmerverhältnisse schriftlich oder elektronisch mit.

Die für den Auftragnehmer zurzeit mit der Verarbeitung von personenbezogenen Daten beschäftigten Subunternehmer sind in Anhang 2 mit Namen, Anschrift, Auftragsinhalt sowie Umfang mit der Verarbeitung von personenbezogenen Daten genannt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

11.6 Der Auftragnehmer trägt dafür Sorge, dass er Subunternehmern nach deren Eignung und Zuverlässigkeit und unter besonderer Berücksichtigung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Artikel 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

11.7 Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Artikel 44 ff. DS-GVO erfüllt sind.

11.8 Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) direkt gegenüber den Subunternehmern wahrnehmen kann. Das vereinbarte Datenschutzniveau soll mindestens der Vereinbarung zwischen Auftraggeber und Auftragnehmer entsprechen.

Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes

Datenschutzniveau gewährleistet ist (z.B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln).

Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

11.9 Der Vertrag über das Subunternehmerverhältnis müssen schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann.

Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind in diesem Vertrag deutlich voneinander abzugrenzen. Werden mehrere Subunternehmer eingesetzt, gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern.

11.10 Der Auftraggeber ist berechtigt, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den Inhalt des mit dem Subunternehmer geschlossenen Vertrages und die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmers zu erhalten. Der Auftragnehmer ist befugt diejenigen Informationen zu schwärzen, die Betriebs- und Geschäftsgeheimnisse darstellen, soweit diese für die vorliegende Vereinbarung nicht zwingend erforderlich sind.

11.11 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subunternehmer und dessen erstmaliges Tätigwerden ist erst mit Vorliegen aller Voraussetzungen für einer Datenverarbeitung durch Subunternehmer Unterauftragsverarbeitung gestattet.

11.12 Der Auftragsnehmer hat die Einhaltung der Pflichten des / der Subunternehmer/s zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

11.13 Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass die eingesetzten Subunternehmer den Datenschutzpflichten nachkommen, die ihnen durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

12. Technische und organisatorische Maßnahmen nach Artikel 32 DS-GVO

12.1 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers. Der Auftragnehmer stellt dem Auftraggeber auf dessen Anforderung ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

12.2 Der Auftragnehmer hat die Sicherheit gem. Artikel 28 Absatz 3 lit. c), Artikel 32 DS-GVO insbesondere in Verbindung mit Artikel 5 Absatz 1, Absatz 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. 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 Artikel 32 Absatz 1 DS-GVO zu berücksichtigen. Die in Anhang 1 beschriebenen technischen und organisatorischen Maßnahmen stellen das Datenschutzkonzept 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 dar. Anhang 1 ist Gegenstand dieser Vereinbarung.
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 DSGVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber unaufgefordert vorzulegen.

Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Mitarbeitern ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen.

12.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sowie wesentliche Änderungen sind zwischen Auftragnehmer und Auftraggeber abzustimmen und zu dokumentieren. Die Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

12.4 Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

13. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Artikel 28 Absatz 3 Satz 2 lit. g) DS-GVO

13.1 Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

13.2 Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Auftraggeber, jedoch spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragnehmer sämtliche im Auftrag des Verantwortlichen verarbeitete personenbezogene Daten dem Verantwortlichen zurückzugeben oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu löschen bzw. zu vernichten. Dies umfasst insbesondere dem Auftragsverarbeiter überlassene Daten, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen. Gleiches gilt für Test- und Ausschlussmaterial. Eine weitere Speicherung ist nur zulässig, wenn hierzu eine Verpflichtung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats besteht. Das Protokoll der Löschung bzw. Vernichtung ist auf Anforderung vorzulegen.

13.3 Der Auftragnehmer kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungs-fristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner

Entlastung bei Vertragsende dem Auftraggeber übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Punkt 13.2.

13.4 Entstehen zusätzliche Kosten durch abweichende Vorgaben durch den Auftraggeber bei der Rückgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

13.5 Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

13.6 Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus so lange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

14. Haftung / Schadenersatz / Geldbuße

14.1 Die Parteien haften bei Verstößen gegen die vorliegende Vereinbarung entsprechend den einschlägigen gesetzlichen Bestimmungen bzw. gegenüber betroffenen Personen gemäß Artikel 82 DS-GVO.

14.2 Im Falle einer Inanspruchnahme durch eine Person hinsichtlich etwaiger Schadenersatzansprüche nach Artikel 82 DSGVO verpflichten sich die Vertragsparteien, sich gegenseitig bei der Abwehr der Ansprüche im Rahmen ihrer jeweiligen Möglichkeiten zu unterstützen.

14.3 Der Auftragnehmer kann sich wegen der Verletzung von Verpflichtungen verhängten Geldbußen gegenüber dem Auftraggeber nicht schadlos halten.

15. Schlussbestimmungen

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

15.2 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 darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen und Beteiligten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber liegen.

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

15.4 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

15.5 Sollten einzelne Regelungen dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

15.6 Der Auftraggeber behält sich weitere inhaltlich bedeutsame Änderungen vor. Diese Änderungen werden einvernehmlich mit dem Auftragnehmer abgestimmt.

16. Anlagen

Anhang 1 - technische und organisatorische Maßnahmen
Anhang 2 - Subunternehmerverhältnisse

Ort, Datum	Ort, Datum
Unterschrift (Auftraggeber)	Unterschrift (Auftragnehmer)
(für den Auftraggeber)	Name, Vorname, Funktion

Anhang 1 - technische und organisatorische Maßnahmen

zur Vereinbarung zur Auftragsverarbeitung vom _____

(Datum)

zwischen dem Saarland,
vertreten durch das Ministerium für Inneres, Bauen und Sport

und

_____

(Vertragsparteien)

Punkt 12.2 des Vertrages verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang.

Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Artikels 32 DS-GVO dienen:

1.	**Zutrittskontrolle** Maßnahmen, die es Unbefugten verwehren, sich den IT-Systemen, Datenverarbeitungsanlagen sowie vertraulichen Akten und Datenträgern physisch zu nähern	1.1 Bauliche Absicherung (Gebäudesicherheitskonzept, Protokollierung Zu- und Abgänge, Zutrittskontrollsystem, Überwachungseinrichtung) - Schutz der Gebäude oder Geschäftsräume durch angemessene Zutrittskontrollsysteme - Abhängig von der Sicherheitseinstufung werden Grundstücke, Gebäude oder einzelne Bereiche durch zusätzliche Maßnahmen gesichert. - Entsprechend des Schutzbedarfs sind Zutrittsberechtigungen zu den Sicherheitsräumen nochmals auf das Personal der zuständigen Fachabteilung eingeschränkt. 1.2 Organisatorische Absicherung (Schlüsselordnung, -vergabe, Besucherausweise, Ausweisordnung) - Einsatz einer Schließanlage und Schlüssel mit Personen- und Zugangsidentifikation

		- Der Eingangsbereich ist durch einen Empfangsbereich überwacht, bei dem sich Gäste anmelden müssen. - Gäste werden durch die zu besuchende Person überwacht. 1.3 Rechnerräume (Aufstellungsort Server) - Die Server sind in geeigneten Räumen untergebracht, Schutz gegen Feuer-, Wasser- und ähnliche Schäden wurde berücksichtigt, strikte Zugangsregeln.
2.	**Benutzerkontrolle / Zugangskontrolle** Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können	2.1 Kontrollmaßnahmen (Regelwerk, Benutzerregistrierung) - Das Benutzerkonto muss zunächst beantragt und vom Vorgesetzten genehmigt werden. 2.2 Netzwerk (Freigabe von Netzzugängen) - Der Zugang über das LAN ist intern über anwendungsspezifische Kennwörter geschützt. - Der Zugang über das LAN von extern wird über eine Firewall geschützt. 2.3 Wartung (Verbindungsaufbau Fernwartung, Mitnahmen DV-Equipment zu Wartungszwecken) - Es gibt vertragliche Regelungen zur Wartung/Fernwartung. 2.4 Sonstiges (Kennwortverfahren, automatische Sperrung, Einrichtung eines Benutzerstammsatzes pro User, Verschlüsselung von (mobilen) Datenträgern und (mobiler) Systeme - Die technischen Systeme und Anwendungen der Auftragnehmer sind durch eine Benutzer-/Kennwort-Abfrage geschützt. - Arbeitsplätze werden bei Verlassen von den Benutzern gegen unberechtigte Nutzung gesichert (Abmeldung) und nach einem angemessenen Zeitintervall automatisch gesichert (automatische Abmeldung).

		- Fremde haben keinen Zugriff auf die Systeme des Auftragnehmers
3.	**Zugriffskontrolle** Maßnahmen, damit die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können	3.1 Zugriffsschutzmaßnahmen (Clean Desk, Sicherheitssoftware, Verschlüsselung, differenzierte Berechtigungen, Auswertungen, Kenntnisnahme, Veränderung, Löschung) - Die Systemzugänge der mit der Ausführung beauftragten Personen sind nur mit den Rechten ausgestattet, die für die Aufgabenerfüllung erforderlich sind. - Zur technischen Zugriffssicherung verwendet der Auftragnehmer anerkannte Sicherheitssysteme. Zugriffe werden technisch überwacht. - Eine Zugriffsberechtigung wird auf Basis des Berechtigungskonzepts beantragt und vom Vorgesetzten bzw. der Geschäftsleitung genehmigt. - Die Ausführung administrativer Zugriffe wird mit den Mitteln des Betriebssystems protokolliert. Auf die Anwendung bezogene Zugriffe werden mit den Mitteln und Möglichkeiten der Anwendung oder des Betriebssystems protokolliert und überwacht. 3.2 Sichere Entsorgung (Sichere Entsorgung von Papierdokumenten und digitalen Informationen, Beachtung von Aufbewahrungsfristen) - Datenschutzrelevante Papierdokumente werden über einen Shredder nach DIN 66399 vernichtet. - Hardware, die Daten enthält, wird datenschutzgerecht vernichtet.
4.	**Datenverarbeitungskontrolle / Weitergabekontrolle** Maßnahmen, die bei der Übermittlung oder beim Transport von personenbezogenen Daten eingesetzt werden, um unberechtigte Zugriffe, insbesondere zum Lesen, Kopieren, Verändern oder Entfernen dieser Daten vermeiden	4.1 Physische Datenübergabe (Weitergabe von Datenträgern, Belege, Datenübergabe, Richtigkeit Adressat, Datenklassifizierung) - Fremde Datenträger dürfen nicht genutzt werden. - Datenträger zur internen Datenweitergabe werden verschlüsselt.

		4.2 Elektronische Datenübermittlung (Protokollierung, Transportsicherung wie Verschlüsselung / Tunnelverbindung (VPN), elektronische Signatur, Datenverschlüsselung) - Firewallsysteme und ständig aktualisierte Virenschutzsoftware sichern neben einer Verschlüsselung und dem Einsatz von VPN Technologie die Kommunikation zum Internet. - Alle Datentransfers mit Dritten werden verschlüsselt oder im Ausnahmefall mit Passwortschutz durchgeführt. - Der Versand von personenbezogenen Daten erfolgt immer verschlüsselt.
5.	**Verantwortlichkeitskontrolle / Eingabekontrolle** Maßnahmen, damit es möglich ist, festzustellen, wer welche personenbezogenen Daten zu welcher Zeit verarbeitet hat und wohin sie übermittelt werden sollen oder übermittelt worden sind	Protokolle (Protokollierung(ssysteme), Auswertungsarten, Aufbewahrung) - Auf die Anwendung bezogene Dateneingaben werden mit den Mitteln und Möglichkeiten der Anwendung oder des Betriebssystems protokolliert und überwacht.
6.	**Auftragskontrolle** Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden	6.1 Vorherige dokumentierte Prüfung, vertragliche Verpflichtung und Genehmigung von Unterauftragsverarbeitern durch den Auftraggeber Weisungsgemäße Auftragsdatenverarbeitung (Kontrolle Einhaltung Weisung, Vereinbarung Subunternehmer, Identitätsprüfung) - Der Auftragnehmer wird sorgfältig ausgewählt. - Der Auftragnehmer bearbeitet die ihm überlassenen Daten nur aufgrund und anhand von vertraglich vereinbarten Weisungen des Auftraggebers. - Kompetenzen und Kontrollmaßnahmen werden in Abstimmung mit dem Auftraggeber definiert und technisch oder organisatorisch in die Betriebsabläufe eingebunden. - Sollten Dritte hinzugezogen werden, werden diese über entsprechende Auftragsdatenverarbeitungsvereinbarungen zur Einhaltung der Datenschutzmaßnahmen verpflichtet.

		- Die Mitarbeiter des Auftragnehmers müssen auf den Datenschutz verpflichtet werden. - Die Zugriffsberechtigten werden geschult und regelmäßig nachgeschult. - Alle Mitarbeiter und Dienstleister des Auftragnehmers mit Zugriff auf personenbezogene Daten werden verpflichtet, diese nur auf Anweisung und ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen zu verarbeiten. 6.2 Meldung Datenschutzverstöße (Meldesystem, Schulung) - Die fristgerechte Meldung von Datenschutzverstößen wird durch interne Regelungen (Datenschutzrichtlinie, Schulungen) sichergestellt.
7.	**Verfügbarkeitskontrolle** Maßnahmen, die sicherstellen, dass personenbezogene Daten nicht unbeabsichtigt zerstört werden oder verloren gehen Es soll sichergestellt werden, dass personenbezogene Daten und der Zugang zu diesen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können	7.1 Risiko und Schwachstellenanalyse (Existenz, Prozess Beseitigung von Schwachstellen, aktives Patchmanagement, Notfallplan) - Regelmäßige Risikoanalysen werden durchgeführt - Die Aktualität der Systeme wird von zentraler Stelle sichergestellt. - Es existieren Pläne für Notfälle 7.2 USV, Überspannungsschutz (Sicherheitsmaßnahmen, Dokumentation, Überwachung) - Die Serverräume sind mit USV ausgestattet 7.3 Branderkennung (Frühwarnsystem, Rufanlage, Aufbewahrung, Schlüssel im Alarmfall) - Die Serverräume sind mit Meldesystemen für Brand und Rauchentwicklung ausgerüstet. 7.4 Backupkonzept (Verantwortlichkeiten, Schutz vor Diebstahl, Funktionalitätstest) - Es existiert ein Backupkonzept / Back-Up von Daten auf Server - Diebstahlschutz

		7.5 Redundanz (Spiegeln von Informationen, z.B. RAID-Verfahren) - Daten werden vor versehentlichem sowie vorsätzlichem Ändern geschützt. 7.6 Sonstiges (Getrennte Aufbewahrung, Virenschutz / Firewall) - Alle Server sind durch eine Firewall geschützt und es sind aktuelle Virenscanner installiert. - Berechtigung zum Löschen (4-Augen-Prinzip)
8.	**Trennungskontrolle** Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden können	8.1 Mandantenfähigkeit (Durchgängigkeit, Dokumentation, Zweckbindung, klare Trennung) - Die Daten verschiedener Mandanten werden getrennt. 8.2 Trennung von Entwicklungs-, Test-, Produktivsystem (Netztrennung, Anonymisierung, Systemtrennung) - Test- und Produktivsysteme werden getrennt. - Testsysteme arbeiten mit Dummy-Daten.
9.	**Pseudonymisierung** Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern möglich und sinnvoll.	Pseudonymisierung (Ersetzen von Klardaten durch Pseudonyme) - Von den Möglichkeiten der Anonymisierung und der Pseudonymisierung wird wo immer möglich/erforderlich Gebrauch gemacht.
10.	**Wirksamkeitskontrolle** Maßnahmen, die gewährleisten, dass die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sicherzustellen, regelmäßig überprüft, bewertet und evaluiert wird	Regelmäßige interne Prüfungen (Dokumentation, Penetrationstests) Regelmäßige externe Prüfungen (Bspw. Zertifikate, Penetrationstests) - Notfallübungen

Anhang 2 - Subunternehmerverhältnisse i.S.v. Nr. 11

zur Vereinbarung zur Auftragsverarbeitung vom _____

(Datum)

Zwischen dem Saarland,
vertreten durch das Ministerium für Inneres, Bauen und Sport,
und

_____

(Vertragsparteien)

Liste der Subunternehmer gemäß Punkt 11 der Vereinbarung:

	Land	Name	Adresse	Auftragsinhalt
1				
2				
3				
4…				

oder:

☐ Erbringung der Leistung ohne die Zuhilfenahme eines Subunternehmers.