

Vereinbarung über Auftragsverarbeitung

zwischen

ReGe Hamburg Projektrealisierungsgesellschaft mbH
Überseeallee 1
D-20457 Hamburg

(nachfolgend „Auftraggeber“ genannt)

und

.....

(nachfolgend „Auftragnehmer“ genannt).

(Auftraggeber und Auftragnehmer nachfolgend gemeinsam auch „Parteien“ genannt.)

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Parteien zum Datenschutz, die sich aus der im Vertrag Bereitstellung und sicherheitskonformer Cloud-Betrieb eines Open-Source-basierten Geoinformationssystems (GIS) für KRITIS-nahe Anwendungsfälle in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Vor diesem Hintergrund schließen die Parteien folgende Vereinbarung über die Verarbeitung von personenbezogenen Daten im Auftrag des Auftraggebers. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten („Daten“) des Auftraggebers verarbeiten.

§ 1

Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

- 1.1 Der Gegenstand des Auftrags ergibt sich aus der Leistungsbeschreibung und dem Vertrag Bereitstellung und sicherheitskonformer Cloud-Betrieb eines Open-Source-basierten Geoinformationssystems (GIS) für KRITIS-nahe Anwendungsfälle, auf die hier verwiesen wird (im Folgenden: Leistungsvereinbarung).

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüberhinausgehende Verpflichtungen ergeben.

§ 2

Konkretisierung des Auftragsinhalts

- 2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

- ☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind beschrieben in dem Leistungsverzeichnis.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind. Der Auftragnehmer wird das angemessene Schutzniveau durch von ihm festzulegende Garantien nach Art. 46 Abs. 2 DSGVO sicherstellen. Das angemessene Schutzniveau

- ☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);
- ☒ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);
- ☐ wird hergestellt durch Standardvertragsklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);
- ☐ wird hergestellt durch genehmigte Verhaltensregeln (Artt. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);
- ☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).
- ☐ wird hergestellt durch sonstige Maßnahmen: (Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DS-GVO)

2.2 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☒ Personenstammdaten (z.B. Name, Vorname, Anschrift)
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail, Abteilung, Unternehmen)
- ☒ Vertragsstammdaten (z.B. Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☒ Vertragsabrechnungs- und Zahlungsdaten (z.B. Bankverbindung)
- ☐ Auskunftangaben (von Dritten, z.B. Auskunftgebern, oder aus öffentlichen Verzeichnissen)
- ☐ Videobilder
- ☐ [...]

2.3 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten

- ☒ Beschäftigte
- ☒ Lieferanten
- ☐ Handelsvertreter
- ☒ Ansprechpartner
- ☒ Besucher
- ☒ Mieter

§ 3

Datenschutzbeauftragter des Auftraggebers

- ☐ Der Auftraggeber hat folgende Person als Datenschutzbeauftragten bestellt:

Name:

Anschrift:

Kontaktdaten:

- ☐ Der Auftraggeber ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet.

§ 4

Technisch-organisatorische Maßnahmen

- 4.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung dokumentiert. Sie sind als Anlage 1 beigelegt. Der Auftraggeber bestätigt hiermit, dass das durch die technischen und organisatorischen Maßnahmen vermittelte Sicherheitsniveau im Verhältnis zum Risiko der Verarbeitung durch den Auftragnehmer angemessen ist.
- 4.2 Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 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 Art. 32 Abs. 1 DS-GVO zu berücksichtigen.
- 4.3 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. Wesentliche Änderungen sind zu dokumentieren.
- 4.4 Zurzeit umgesetzte Maßnahmen können der Anlage 1 entnommen werden. Die Parteien gehen dabei davon aus, dass damit ein angemessenes Schutzniveau gewährleistet ist. Sollte

sich später einen erforderlichen Anpassungsbedarf ergeben (bspw. durch eine Prüfung / Audit des Auftraggebers), ist dieser einvernehmlich umzusetzen.

§ 5

Berichtigung, Einschränkung und Löschung von Daten

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken, es sei denn, der Auftragnehmer ist hierzu durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

§ 6

Qualitätssicherung und sonstige Rechte und Pflichten des Auftragnehmers

- 6.1 Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:
 - 6.1.1 Soweit gesetzlich vorgeschrieben, eine schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
 - 6.1.2 Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie aufgrund eines Rechts der Europäischen Union oder eines Mitgliedstaates gesetzlich zur Verarbeitung verpflichtet sind.
 - 6.1.3 Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO, wie in Anlage 1 aufgeführt.
 - 6.1.4 Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
 - 6.1.5 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.

- 6.1.6 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.
- 6.1.7 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.
- 6.1.8 Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 8 dieser Vereinbarung.
- 6.2 Die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Rahmen von mobilem Arbeiten bzw. Telearbeit ist gestattet, wenn der Auftragnehmer gewährleistet, dass dafür ausschließlich sichere VPN-Verbindungen in sein Netzwerk genutzt werden und dass eine Kenntnisnahme der Daten durch Dritte ausgeschlossen ist. In jedem Fall ist die Einhaltung der Maßgaben des Art. 32 DS-GVO auch in diesem Fall sicherzustellen.

§ 7

Unterauftragsverhältnisse

- 7.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, wie z.B. Telekommunikationsleistungen und Post-/Transportdienstleistungen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
- 7.2 Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) beauftragen. Den in der **Anlage** zu dieser Vereinbarung benannten Unterauftragnehmern stimmt der Auftraggeber hiermit bereits zu.
- 7.3 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet; wie die vollständige Übertragung aller Datenschutzpflichten aus diesem Auftragsverarbeitungsvertrag sowie das Vorliegen hinreichender Garantien für die technischen und organisatorischen Maßnahmen.
- 7.4 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

- 7.5 Der Auftragnehmer ist ferner berechtigt, bestehende Unterauftragnehmer auszutauschen oder neue Unterauftragnehmer zu beauftragen. Für die Erteilung der Zustimmung vereinbaren die Parteien folgendes Verfahren:
- 7.5.1 Der Auftragnehmer benachrichtigt den Auftraggeber mindestens 14 Tage vor dem Einsatz des neuen Unterauftragnehmers.
- 7.5.2 Wenn der Auftraggeber in diesem Zeitraum nicht schriftlich oder in Textform, unter Angabe eines sachlichen Grundes, widerspricht, gilt die Zustimmung des Auftraggebers als erteilt, sofern der Auftragnehmer auf die Folge des widerspruchlosen Verstreichens hingewiesen hat.
- 7.5.3 Widerspricht der Auftraggeber gegenüber dem Auftragnehmer, ist der Auftragnehmer berechtigt, den
- 7.5.3.1 Vertrag und/oder diese Vereinbarung ohne den beanstandeten Unterauftragnehmer fortzusetzen,
- 7.5.3.2 die notwendigen Maßnahmen zu ergreifen, um die Bedenken des Auftraggebers aus dessen Widerspruch auszuräumen oder
- 7.5.3.3 mit Zustimmung des Auftraggebers, denjenigen Teil der Leistungen einzustellen, für den der entsprechende Unterauftragnehmer eingesetzt worden wäre.
- 7.6 Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der Zustimmung des Auftragnehmers.

§ 8

Kontrollrechte des Auftraggebers

- 8.1 Der Auftraggeber hat das Recht, Überprüfungen – einschließlich Inspektionen - durchzuführen oder durch zu benennende Prüfer durchführen zu lassen, sofern diese Prüfer nicht in einem unmittelbaren Wettbewerbsverhältnis zum Auftragnehmer stehen. In der Regel sind die Überprüfungen / Inspektionen rechtzeitig, vorzugsweise mindestens 14 Tage, vorher anzumelden, sofern nicht eine Kontrolle ohne vorherige Anmeldung erforderlich erscheint, weil andernfalls der Kontrollzweck gefährdet wäre.
- 8.2 Der Auftragnehmer ermöglicht und trägt dazu bei, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung alle erforderlichen Informationen zum Nachweis der Einhaltung der im Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung zu stellen.
- 8.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO oder Testate, Berichte oder Auszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren).

- 8.4 Der Auftragsverarbeiter gewährt das Kontrollrecht auch Auftraggebern des Auftraggebers, für die der in diesem Vertrag genannte Auftraggeber Auftragsverarbeiter und der Auftragsverarbeiter damit Subauftragsverarbeiter ist.
- 8.5 Für die Ermöglichung von Kontrollen durch den Auftraggeber gem. § 8.1 kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Der Vergütungsanspruch gilt nicht für erforderliche Kontrollen aufgrund eines vom Auftragnehmer verursachten Gesetzes- oder Vertragsverstoßes.

§ 9

Unterstützungspflichten des Auftragnehmers

- 9.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in Kapitel III sowie in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen, Betroffenenrechte und vorherige Konsultationen. Hierzu gehören u.a.
- 9.1.1 die Unterstützung zur Einhaltung der in den Artikeln 32 bis 36 DS-GVO genannten Pflichten unter Berücksichtigung der Art der Verarbeitung und dem Auftragnehmer zur Verfügung stehenden Informationen,
- 9.1.2 die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,
- 9.1.3 die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden, soweit Datensätze des Auftraggebers betroffen sind,
- 9.1.4 angesichts der Art der Verarbeitung den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,
- 9.1.5 die Unterstützung des Auftraggebers im Rahmen der vorherigen Konsultationen mit der Aufsichtsbehörde.
- 9.2 Für Unterstützungsleistungen, die nicht auf einen Gesetzes- oder Vertragsverstoß des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

§ 10

Weisungsbefugnis des Auftraggebers

- 10.1 Der Auftraggeber ist berechtigt, dem Auftragnehmer im Rahmen der Auftragsverarbeitung Weisungen zu erteilen. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Alle erteilten Weisungen, die der Auftraggeber dem Auftragnehmer erteilt, sind von dem Auftraggeber zu dokumentieren. Sofern eine Rechtsvorschrift der Europäischen Union oder der Mitgliedstaaten den Auftragnehmer zu einer Ausnahme der Weisungsgebundenheit

verpflichtet, informiert der Auftragnehmer zuvor den Auftraggeber über die auf der Grundlage von Rechtsvorschriften erfolgten oder unterlassenen Verarbeitungen, es sei denn die Rechtsvorschrift verbietet ihm wegen eines wichtigen öffentlichen Interesses eine Mitteilung.

- 10.2 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen die DSGVO oder andere Datenschutzbestimmungen der Europäischen Union oder der Mitgliedstaaten, es sei denn, es besteht eine Beschränkung durch das bestehende Recht wegen eines wichtigen öffentlichen Interesses. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Befolgt der Auftragnehmer rechtswidrige Weisungen des Auftraggebers, stellt der Auftraggeber diesen von etwaigen Schadensersatzansprüchen, Bußgeldern und Geldstrafen frei.
- 10.3 Offenkundig rechtswidrige Weisungen des Auftraggebers hat der Auftragnehmer nicht zu befolgen.

§ 11

Löschung und Rückgabe von personenbezogenen Daten

- 11.1 Kopien oder Duplikate der 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 nach dem Recht der Europäischen Union oder dem Recht der Mitgliedstaaten erforderlich sind.
- 11.2 Nach Abschluss der Erbringung der Verarbeitungsleistungen oder früher nach Aufforderung durch den Auftraggeber, werden nach Wahl des Auftraggebers entweder alle personenbezogenen Daten gelöscht oder an den Auftraggeber zurückgegeben und die vorhandenen Kopien gelöscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Auftragnehmer eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.
- 11.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen des Unionsrechts oder des Rechts eines Mitgliedstaates über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 12

Recht zur Offenlegung

Jede Partei ist berechtigt, zum Zwecke der Abwehr von Schadensersatzansprüchen, Geldbußen oder Geldstrafen die notwendigen Informationen und Unterlagen preiszugeben, soweit dies aufgrund des Unionsrechts oder des Rechts eines Mitgliedstaates zulässig ist. Die jeweils andere Partei wird über die Art und Weise der Offenbarung und deren Umfang informiert.

Ort, Datum

Ort, Datum

Unterschrift Auftraggeber

Unterschrift Auftragnehmer

Anlage 1: Technisch-organisatorische Maßnahmen

Anlage 2: Liste der eingesetzten Nachunternehmer

Anlage 1: Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

Die Dokumentation der technischen und organisatorischen Maßnahmen (nachfolgend TOM) ist eine wichtige und gemäß der Europäischen Datenschutz-Grundverordnung (nachfolgend DSGVO) verbindliche Datenschutzanforderung. Neben der Führung eines Verarbeitungsverzeichnisses und der Durchführung von Datenschutzfolgenabschätzungen (nachfolgend DSFA) bilden TOM ein zentrales Element des Datenschutzes.

Die TOM in der Unternehmensgruppe (nachfolgend UGG) unterstützen die Datensicherheit und den Datenschutz im Zusammenhang mit internen Verarbeitungstätigkeiten sowie Verarbeitungen im Auftrag unserer Kunden (Auftragsverarbeitungen). Ziel ist es, die Daten der Betroffenen (Kunden, Lieferanten, Mitarbeiter etc.) zu schützen und die Verarbeitungsprozesse entsprechend abzusichern.

Im Falle von „Datenpannen“ können angemessen dokumentierte und wirksam umgesetzte TOM helfen zu belegen, dass angemessene präventive und / oder aufklärende Maßnahmen zum Schutz personenbezogener Daten getroffen wurden.

Jede Verarbeitung von personenbezogenen Daten erfordert die Implementierung und Dokumentation angemessener TOM. Diese haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen zu treffen. Dabei kommen die folgenden zwei Grundsätze zur Anwendung:

- Je sensibler die Daten sind, die verarbeitet werden, desto höher ist deren Schutzbedarf.
- Je höher die Anzahl der bei der Verarbeitung betroffenen Personen ist, desto höher ist deren Schutzbedarf.

Die umzusetzenden TOM müssen diesen Dimensionen gerecht werden.

Die TOM sind von den jeweiligen Verantwortlichen in Zusammenarbeit mit dem zuständigen Datenschutzbeauftragten (nachfolgend DSB), sowie ggf. dem Corporate Center Organisation & IT zu definieren und zu implementieren. Die Angemessenheit und Wirksamkeit der TOM sind regelmäßig zu auditieren und bei Bedarf anzupassen.

Die folgende Darstellung der TOM betrifft die bei der UGG konzernweit einheitlich vorliegenden TOM.

Sofern durch die UGG personenbezogene Daten im Auftrag des Auftraggebers in den Räumlichkeiten des Auftraggebers verarbeitet und ggf. auch Arbeitsmittel (z.B. PC, Software) des Auftraggebers auf dessen Weisung genutzt werden, ist der Auftraggeber für die Gewährleistung der technischen und organisatorischen Maßnahmen in seinem Herrschaftsbereich insoweit verantwortlich.

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. b) DSGVO

Zutrittskontrollen sind Maßnahmen, die geeignet sind, Unbefugten den physischen Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verhindern.

Zentral durch die UGG genutzte Rechenzentren können nur durch autorisiertes Personal und nach Authentifizierung betreten werden. Darüber hinaus gibt es folgende Maßnahmen:

- Videoüberwachung
- Elektrische Zutrittskontrolle
- Redundante Stromversorgung mit USV und Diesel
- Geeignete Feuerlöschgeräte/Feuerlöschanlagen
- Brandmeldeanlage
- 24/7 Monitoring mit Alarmaufschaltung
- Differenzierte Sicherheitsbereiche/-zonen
- Protokollierung von Zutritten zum Serverraum

Gebäude und Büros der UGG werden mit personellen, maschinell und / oder mechanischem Zutrittskontrollsystem und / oder manuellem Schließsystem vor Zutritt unberechtigter Personen geschützt. Teils sind Gebäude der UGG auch videoüberwacht und/oder verfügen über eine Alarmanlage. Ferner regelt eine gruppenweit geltende Anweisung den Umgang mit Schlüsseln (General-, Gruppen-, Einzelschlüssel, Schließkarten und Transponder) inklusive der Schlüsselübergabe, Schlüsselmarken und Schlüsselrevision.

1.2. Zugangskontrolle

Zugangskontrollen sind Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Die Identifikation bzw. Authentifizierung an Unternehmensrechnern erfolgt mit einer Active Directory-Benutzerverwaltung, die wie folgt aufgebaut ist:

- Zentrale Anlage eines Benutzers sowie Identifikation über eindeutige Benutzer-ID
- Authentifizierung über Benutzernamen und persönlichem Passwort mit folgender Kennwortrichtlinie:
 - o Passwortvergabe durch den Benutzer
 - o Passwörter sind mindestens acht Zeichen lang und müssen drei Merkmale von Großbuchstaben, Kleinbuchstaben, Sonderzeichen oder Ziffern enthalten
 - o Die Gültigkeitsdauer von Passwörtern beträgt 90 Tage
 - o Die Chronik der Passwörter beträgt 18 Monate und beinhaltet eine Überprüfung der Passworthistorie mit Sperre für den Wechsel bei gleichem Passwort
 - o Passwörter werden verschlüsselt gespeichert
- Automatische Bildschirmsperre nach 10 Minuten Inaktivität
- Viren-Scanner für Server und Clients mit regelmäßigem Update
- Protokollierung von Zugängen zu DV-Systemen
- VPN für WAN-Verbindung
- Benutzerbezogener Zugang zum hauseigenen WLAN
- Schließvorrichtungen an den Serverschränken
- Vorrübergehend Zugangssperre nach 3 Fehlversuchen
- Anti-Virus-Software
- Firewall
- Intrusion Detection Systeme
- Intrusion Prevention System
- Smartphones / Tablets mit Mobile Device Management

- Protokollierung der Passwortnutzung
- Mobile Device Policy
- Zuordnung von Benutzerrechten (Berechtigungskonzept)
- Im Rahmen des Berechtigungsmanagements ist nachweisbar, wer und wann welche Berechtigungen innehatte Einsatz von zentraler Smartphone-Administrations-Software Protokolle über die Aktivitäten auf der Datenverarbeitungsanlage
- Aktualisierte Angriffsmuster und Signaturen von gängigen Einfallsmechanismen oder vorbereitender Maßnahmen werden zur Prävention angewandt
- Protokollierung von gescheiterten Zugriffsversuchen auf Datenverarbeitungssysteme

Hierneben gibt es eine unternehmensinterne Betriebsvereinbarung zum Umgang mit Kommunikationstechnik, welche unter anderem verbindliche Regelungen für die Themenbereiche Netzwerke, Bürokommunikation einschließlich E-Mail und Telekommunikationsmedien, Benutzerverwaltung und Passwortschutz sowie Internet und Intranet beschreibt.

1.3. Zugriffskontrolle

Zugriffskontrollen sind Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Der Zugriff auf das Datenverarbeitungssystem erfolgt mit differenzierten und abgestuften Berechtigungen in den jeweiligen Software-Systemen mit entsprechender Genehmigung durch den Vorgesetzten bzw. Prozessverantwortlichen. Antrag, Freigabe und Umsetzung werden dokumentiert. Siehe im Übrigen Abschnitt 1.2

1.4. Trennungskontrolle

Trennungskontrolle beschreibt Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Innerhalb der UGG gewährleisten spezifisch-aufgabenbezogene Datenverarbeitungssysteme eine angemessene Trennungskontrolle. Integrierte Systeme sind modular aufgebaut. Die wesentlichen innerhalb der UGG genutzten Datenverarbeitungssysteme gewährleisten zudem eine Trennung von Produktiv- und Testumgebung, um einen uneingeschränkten Systemablauf auch im Falle von Updates und Upgrades zu garantieren. Im Übrigen sind die wesentlichen Systeme mandantenfähig, um eine gesellschaftsbezogene Trennung von Daten sicherzustellen. Daten werden über eine entsprechende Mandanten- bzw. Ordnerstruktur getrennt. Mit differenzierten Berechtigungen können Daten zu unterschiedlichen Zwecken getrennt verarbeitet werden.

Hierneben sind die Beschäftigten unterwiesen, Daten nur für den vorgesehenen Zweck und auf vereinbarten IT-Systemen zu verwenden.

1.5. Pseudonymisierung gem. Art. 32 Abs. 1 lit. a) DSGVO; Art. 25 Abs. 1 DSGVO

Pseudonymisierung umfasst die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Die Beschäftigten der UGG sind sensibilisiert, personenbezogene Daten im Falle einer erforderlichen Weitergabe – soweit möglich - zu pseudonymisieren.

2. Integrität gem. Art. 32 Abs. 1 lit. b) DSGVO

2.1. Weitergabekontrolle

Weitergabekontrolle beschreibt Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Für die Übertragung von datenschutzrelevanten Daten per Email steht die Möglichkeit der Einrichtung einer S/MIME und TLS Verschlüsselung mit externen Kommunikationspartnern zur Verfügung.

Sonstige Maßnahmen sind:

- Deaktivierung der Windows Autowiederherstellung („Schattenkopie“)
- Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger
- Datenschutzgerechte Entsorgung von Papierdokumenten
- Protokolle über die Aktivitäten auf der DV-Anlage werden automatisch erstellt
- Firewall
- Intrusion Detection Systems
- Intrusion Prevention System
- VPN
- Content Filter
- Virenschutz
- Spamfilter
- Regelung zur Nutzung von privaten Endgeräten/Datenträgern
- Protokollierung von legitimen Fernzugriffen

Schließlich wird mittels unternehmensweit einheitlicher Übergabeprotokolle die Übermittlung von Dokumenten, Schlüsseln, Datenträgern etc., in dokumentierter Form festgehalten.

2.2. Eingabekontrolle

Eingabekontrollen umfassen Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Entsprechend einem differenzierten und abgestuften Berechtigungskonzept erfolgt die Eingabe der Daten gemäß der erteilten Berechtigung. Siehe hierzu Abschnitt 1.2 und 1.3. Darüber hinaus werden die weiteren Maßnahmen umgesetzt:

- Protokolle über die Aktivitäten auf der DV-Anlage werden automatisch erstellt
- Eine Protokollierung von Administratorentätigkeiten erfolgt

Darüber hinaus sind die Beschäftigten angewiesen, nur befugte, zweckgebundene Daten zu erheben.

3. Verfügbarkeit und Belastbarkeit gem. Art. 32 Abs. 1 lit. b) DSGVO

3.1. Verfügbarkeitskontrolle

Verfügbarkeitskontrolle beschreibt Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Elektronisch im System erfasste personenbezogene Daten und andere vertrauliche Informationen werden unternehmensweit in den IT-Systemen abgelegt. Um die Daten vor Verlust zu schützen bzw. im Fall eines Verlustes die Daten mit einem vertretbaren technisch-organisatorischen Aufwand wiederherzustellen, wurden die folgenden technisch-organisatorischen Sicherheitsmaßnahmen implementiert:

- Klimaanlage in den von der UGG genutzten Rechenzentren
- Schriftliches Datensicherungskonzept
- Sicherung von Stand-Alone-Systemen durch die Datensicherung
- Einsatz einer Virtualisierungstechnologie, um die Hardware besser auszulasten
- Datensicherung des Betriebssystems und der gesamten Konfiguration
- Sicherung der Datenbanken, Fileserver
- Mindestens einmal tägliche Sicherung der Daten auf Band bzw. Festplatte
- Festplattenspiegelung
- Kontrolle des Sicherungsvorgangs
- Lagerung der Datensicherungen in einem separaten Brandabschnitt
- Regelmäßige Kontrolle der Datensicherungen auf Datenvollständigkeit
- Regelmäßige Überprüfung einer möglichen Rekonstruktion der gesicherten Daten
- Virenschutz für Kommunikationswege (Mail und Internet), eine implementierte DMZ (Firewall etc.), Virenschutz auf Client und Serverbasis sowie Backupverfahren
- Serverräume sind mit Feuerlöschgeräten, Feuer- und Brandmeldeanlagen, Klimaanlage sowie redundanter Stromversorgung mit USV und Diesel ausgestattet
- Notfallkonzept
- Aufbewahrung der Datensicherung in zugriffsgeschützten Räumen oder Behältnissen
- Kapazitätsmanagement
- Zentrale Beschaffung und/oder Freigabe von Softwarekomponenten
- Einsatz von Superusern, zwecks Monitoring bzw. regelmäßiger Kontrolle von Fehlermeldungen

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO

4.1. Datenschutz-Management-System

Bestandteil eines wirksamen Datenschutz-Management-Systems ist die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der implementierten technisch-organisatorischen Maßnahmen.

Auch das unternehmensinterne Datenschutz-Management-System unterliegt einem stetigen Überprüfungs- und Verbesserungsprozess.

Zentrales Dokumentationsmedium des Datenschutz-Management-Systems der UGG ist eine Datenschutz-DV-Anwendung, welche regelmäßig mittels Updates bzw. Upgrades in automatisierter Form optimiert und an die jeweils aktuelle Rechtslage angepasst wird.

- Die Dokumentation der Verarbeitungsprozesse erfolgt in einer Datenschutz-DV-Anwendung. Prozessänderungen bzw. neu zu implementierende Prozesse sind gemäß Verfahrensanweisung auf ihre datenschutzrechtliche Relevanz zu überprüfen; Anpassungen, Ergänzungen, Streichungen werden innerhalb der Datenschutz-DV-Anwendung umgesetzt
- Im Übrigen unterliegen alle Datenschutzdokumente und -prozesse bzw. -anweisungen einem laufenden Überprüfungs- und Anpassungsprozess
- Alle Beschäftigten der UGG sind zur Wahrung der Vertraulichkeit personenbezogener Daten und der Verschwiegenheit nachweislich verpflichtet worden. Es finden regelmäßige Unterweisungen statt
- Schulungen sowie Sensibilisierungsmaßnahmen werden regelmäßig angeboten und bei Bedarf aktualisiert
- Es existieren diverse Verfahrensanweisungen zum Datenschutz. Beispielsweise existiert eine Verfahrensanweisung, welche detailliert den Prozess und die Verantwortlichkeiten im Zusammenhang mit der Erteilung von Auskünften an Betroffene über deren verarbeitete personenbezogene Daten regelt. Darüber hinaus eine Verfahrensanweisung zum detaillierten Prozess und die Verantwortlichkeiten im Zusammenhang mit der Meldung einer Verletzung des Schutzes personenbezogener Daten
- Für die Konzernunternehmen ist ein Datenschutzbeauftragter bestellt, sofern dies gesetzlich vorgeschrieben ist. Dieser verfügt über die notwendige Fachkunde und Zuverlässigkeit. Der bestellte Datenschutzbeauftragte ist unter [datenschutz@\[REDACTED\].de](mailto:datenschutz@[REDACTED].de) erreichbar. Bei Bedarf berät dieser die Konzernunternehmen bei der Durchführung einer DSFA
- Verarbeitungsverzeichnisse gemäß den datenschutzrechtlichen Vorgaben sind vorhanden und werden bei Bedarf aktualisiert
- Ein unternehmensweit geltendes Datenschutzmanagement-Handbuch ist vorhanden

4.2. Incident-Response-Management

Incident-Response-Management beschreibt den geregelten Umgang mit „Datenpannen“. Angemessen dokumentierte und wirksam umgesetzte TOM können in diesem Zusammenhang helfen zu belegen, dass angemessene präventive und / oder aufklärende Maßnahmen zum Schutz personenbezogener Daten getroffen wurden.

Zentrales Dokument des Incident-Response-Managements der UGG ist die Verfahrensanweisung zur Meldung von Datenschutzverstößen, welche detailliert die einzuleitenden Maßnahmen, die Verantwortlichkeiten sowie die Dokumentation im Falle von „Datenpannen“ beschreibt.

Im Rahmen eines 24/7 Monitorings durch ein Security Operations Center werden vorqualifizierte und sicherheitsrelevante Störungen nach einer definierten Meldekette zur UGG übermittelt.

4.3. Datenschutzfreundliche Voreinstellungen gem. Art. 25 Abs. 2 DSGVO

Datenschutzfreundliche Voreinstellungen bedeutet „Privacy by design“ / „Privacy by default“. Der Datenschutz innerhalb der UGG folgt diesem Ansatz.

Die Beschäftigten sind angewiesen nur befugte, zweckgebundene Daten zu erheben. Betroffene haben jederzeit die Möglichkeit, datenschutzrechtlich erteilte Einwilligungen zu widerrufen (auch mittels Fernkommunikation) und Löschung ihrer Daten zu verlangen. Siehe hierzu im Übrigen Abschnitt 2.2.

5. Auftragskontrolle (Outsourcing an Dritte)

Auftragskontrolle beschreibt Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Die Beschäftigten sind angewiesen, bei der Auswahl von Auftragnehmern bestimmte Sorgfaltskriterien einzuhalten und Aufträge, Weisungen und Vertragsgestaltungen stets in schriftlicher Form aufzusetzen. Auftragnehmer und deren Tätigkeiten werden in Abständen überprüft.

- Die Beschäftigten des Auftragnehmers und die Subunternehmer sind auf Vertraulichkeit / Datengeheimnis zu verpflichten
- Personenbezogene Daten sind datenschutzgerecht zu vernichten
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen einer Bestellpflicht
- Wirksame Kontrollrechte gegenüber dem Subunternehmer sind vereinbart
- Regelungen zum Einsatz weiterer Subunternehmer sind vorhanden
- Vernichtung von Daten nach Beendigung des Auftrags durch vertragliche Regelungen sichergestellt

Anlage 2: Liste der eingesetzten Unterauftragsverarbeiter:

Nachunternehmer	Leistung und Art der Daten	Drittstaatenübermittlung sowie Garantien (soweit einschlägig)	Weitere Empfänger der Daten (Empfänger/Staat/Art der Daten/ Drittstaatenübermittlung) (soweit einschlägig)