NUTZUNGSVERTRAG GEOVERIS

ZWISCHEN:

(1) **VdS Schadenverhütung GmbH**, Amsterdamer Str. 174, 50735 Köln

– "**VdS**" –

(2) der in der Annahmeerklärung von VdS bezeichneten natürlichen oder juristischen Person

– "**Kunde**" –

Die Parteien zu (1) bis (2) werden nachfolgend auch gemeinsam als die "**Parteien**" und einzeln als eine "**Partei**" bezeichnet.

VORBEMERKUNG

(A) VdS betreibt in ihrem Geschäftsbereich „GeoExpertise“ u.a. das Informationsangebot "GeoVeris", das die bislang unter den Bezeichnungen "ZÜRS Solutions" und "Meteo-Info" betriebenen Angebote zur Abfrage von Geoinformationen und meteorologischer Informationen ("GeoVeris-Informationen" oder "GVI") umfasst.

(B) Der Kunde ist ein Unternehmen / Einzelunternehmer, das/der im Rahmen seiner eigenen Geschäftstätigkeit in den Bereichen Finanzdienstleistungen, Versicherungen oder Immobilien auf Informationen zu orts- oder objektbezogenen Risiken angewiesen ist.

1. ABSCHLUSS DIESES VERTRAGES

1.1 Dieser Nutzungsvertrag kommt zustande, wenn

1.1.1 der Kunde auf einem von VdS angebotenen Weg, insbesondere über die Website www.vds.de/ (Neukundenregistrierung GeoVeris), unter Angabe der hierfür vorgegebenen Daten ein Angebot auf Abschluss dieses Nutzungsvertrages abgibt und

1.1.2 VdS dieses Angebot durch ausdrückliche Erklärung gegenüber dem Kunden bestätigt.

1.2 VdS ist berechtigt, ein auf den Abschluss dieses Nutzungsvertrages gerichtetes Angebot des Kunden ohne Angabe von Gründen abzulehnen.

2. VERTRAGSGEGENSTAND

2.1 Mit Abschluss dieses Nutzungsvertrages verpflichtet sich VdS gegenüber dem Kunden nach Maßgabe dieses Nutzungsvertrags und der Nutzungsbedingungen GeoVeris (**Anlage 1** zu diesem Nutzungsvertrag) zur Bereitstellung von GeoVeris und

zur Einräumung bestimmter Nutzungsrechte an den GeoVeris-Informationen. Die Parteien schließen ergänzend die als **Anlage 2** beigefügte Vereinbarung über Auftragsverarbeitung.

2.2 GeoVeris wird dem Kunden über das Web-Interface von VdS (unter www.geo-veris.de und/oder einer anderen von VdS mitgeteilten Adresse) zur Verfügung gestellt.

2.3 Nach Abschluss dieses Nutzungsvertrages richtet VdS einen Zugang für den Kunden ein und stellt dem Kunden die dazugehörigen Log-In-Daten zur Verfügung. Auf Anfrage des Kunden kann VdS für den Kunden weitere Zugänge (insbesondere für einzelne vom Kunden unter Berücksichtigung der Nutzungsbedingungen definiert und VdS mitgeteilte Berechtigte Nutzer) einrichten.

2.4 Wenn und soweit der Kunde einen für ihn eingerichteten Zugang als "Sammelzugang" verwendet (also einen solchen Zugang durch mehrere Berechtigte Nutzer nutzen lässt), ist eine personalisierte Kontrolle des Zugriffs auf GeoVeris und entsprechende Auswertungen nicht möglich. Jede Nutzung von GeoVeris über einen vom Kunden als solchen verwendeten Sammelzugang gilt als Nutzung von GeoVeris durch den Kunden.

2.5 Der Kunde hat die Möglichkeit, über GeoVeris die in der Leistungsbeschreibung spezifizierten GeoVeris-Informationen auszuwählen und abzurufen. Der Abruf von GeoVeris-Informationen ist kostenpflichtig; die Vergütung für den Abruf von GeoVeris-Informationen ergibt sich aus der Preisliste. Leistungsbeschreibung und Preisliste werden dem Kunden mit Annahme seines Angebots auf Abschluss des Nutzungsvertrages und über GeoVeris zur Verfügung gestellt.

2.6 Der Kunde verpflichtet zur Einhaltung des Nutzungsvertrages und der Nutzungsbedingungen sowie zur Zahlung der Vergütung für die von ihm abgerufenen GeoVeris-Informationen.

3. UMFANG DER ZULÄSSIGEN NUTZUNG DURCH DEN KUNDEN

3.1 Der Kunde wird GeoVeris-Informationen ausschließlich im Rahmen seiner eigenen Geschäftstätigkeit zur Vorbereitung oder Durchführung eines rechtlich zulässigen Geschäftsvorgangs mit Bezug zu dem durch die GeoVeris-Informationen beschriebenen orts- oder objektbezogenen Risiko und zur Prüfung oder Bewertung dieses Risikos abrufen ("**Berechtigte Nutzung**").

3.2 Der Kunde wird den Zugriff auf GeoVeris und den Abruf von GeoVeris-Informationen ausschließlich eigenen Mitarbeitern gestatten ("**Berechtigte Nutzer**"), die der Kunde über die Regelungen dieses Nutzungsvertrages und der Nutzungsbedingungen – insbesondere im Hinblick auf den Umfang der Berechtigten Nutzung und

der zulässigen Weitergabe an Berechtigte Empfänger – informiert und zu der Einhaltung dieser Vorgaben verpflichtet hat.

3.3 Der Kunde wird GeoVeris-Informationen außer in den in den Nutzungsbedingungen ausdrücklich genannten Fällen ausschließlich als notwendigen Bestandteil von Informationen und Unterlagen des Kunden an eigene Endkunden oder (potentielle) Geschäftspartner im Zusammenhang mit einem konkreten Geschäftsvorfall ("**Berechtigte Empfänger**") weitergeben oder diesen gegenüber offenlegen wird; eine separate Weitergabe oder Offenlegung von GeoVeris-Informationen außerhalb der Berechtigten Nutzung ist nicht zulässig.

4. NUTZUNGSBEDINGUNGEN, VEREINBARUNG ÜBER AUFTRAGSVERARBEITUNG

Für die Bereitstellung von GeoVeris durch VdS sowie für die Nutzung durch den Kunden gelten Nutzungsbedingungen GeoVeris in Anlage 1. Mit Abschluss dieses Nutzungsvertrages schließen die Parteien zudem die Vereinbarung über Auftragsverarbeitung GeoVeris in Anlage 2.

Anlage 1
Nutzungsbedingungen GeoVeris

1. Anwendungsbereich der Nutzungsbedingungen

1.1 Diese Nutzungsbedingungen gelten für die Nutzung von GeoVeris durch Unternehmen, soweit diese mit VdS einen Nutzungsvertrag über die Nutzung von GeoVeris (jeweils oder zusammen „**Nutzungsvertrag**“) abgeschlossen haben („**Kunde**“).

1.2 Abweichende oder ergänzende Bedingungen eines Kunden finden keine Anwendung. Dies gilt auch dann, wenn ein Kunde VdS auf solche abweichenden oder ergänzenden Bedingungen ausdrücklich hingewiesen hat.

2. Leistungen von VdS

2.1 VdS verpflichtet sich gegenüber dem Kunden, die in diesen Nutzungsbedingungen geregelten Nutzungsrechte an GeoVeris und den aus GeoVeris gemäß dem Nutzungsvertrag abrufbaren Daten einzuräumen und GeoVeris dem Kunden über das Internet zugänglich zu machen.

2.2 Funktionalitäten und Leistungsumfang von GeoVeris, die für GeoVeris verwendete Datenbasis sowie die vom Kunden zu schaffenden technischen Voraussetzungen ergeben sich aus der Leistungsbeschreibung.

2.3 Der Anspruch auf Nutzung von GeoVeris besteht nur im Rahmen des aktuellen Stands der Technik und der VdS von Dritten eingeräumten Nutzungsrechte an Daten und Funktionalitäten. VdS behält sich vor, den Zugang zu sowie die Funktionalitäten und Nutzung von GeoVeris zeitweilig zu beschränken, wenn dies im Hinblick auf Kapazitätsgrenzen, die Sicherheit oder Integrität der technischen Infrastruktur oder zur Durchführung technischer Maßnahmen oder aufgrund der Beendigung zeitlich beschränkter Nutzungsmöglichkeiten (etwa für Analyse- und Kartendienste) erforderlich ist. VdS wird den Kunden soweit möglich über geplante Beschränkungen des Zugangs, von Funktionalitäten und/oder der Nutzung innerhalb von GeoVeris oder durch Mitteilung per E-Mail informieren.

2.4 VdS weist ausdrücklich darauf hin, dass in GeoVeris eine Vielzahl von unterschiedlichen Ausgangsdaten verschiedener Datenlieferanten eingeflossen sind, die z.T. mit unterschiedlichen Datenmodellen und –formaten gearbeitet haben und dass Gutachten von Dritten im Auftrag von VdS für den Lizenznehmer erstellt werden. Aufgrund des erheblichen Umfanges unterschiedlicher Ausgangsdaten ist es nicht unwahrscheinlich, dass diese Daten und die über GeoVeris abgerufenen Informationen Ungenauigkeiten und Fehler enthalten. VdS hat die Dienstleister für die Bereitstellung der Ausgangsdaten und für die Erstellung von Gutachten sorgfältig ausgewählt, hat aber auf Erhebung bzw. Erstellung von Ausgangsdaten ebenso wenig

Einfluss wie auf die Vollständigkeit und Richtigkeit der VdS zur Verfügung gestellten Daten. Zudem können künftig in GeoVeris mathematische Verfahren einbezogen werden, mit denen versucht wird, bestimmte zukünftige Naturereignisse vorherzusagen; diese Verfahren gewährleisten gleichwohl – wie jede Prognosetätigkeit – nicht, dass die Prognose auch tatsächlich eintritt. Darüber hinaus weist VdS zusätzlich darauf hin, dass sich die für meteorologische Anfragen und Analysen verwendeten Ausgangsdaten nicht stets auf meteorologische Parameter an dem vom Lizenzgeber angegebenen Ort beziehen, sondern ggf. auf Ausgangsdaten der nächstgelegenen Wetterstation(en) oder sonstiger Erfassungseinrichtung(en). Es ist nach alledem nicht unwahrscheinlich, dass die von GeoVeris ausgegebenen GeoVeris-Informationen von den tatsächlichen Gegebenheiten und Risiken abweichen. GeoVeris bildet auch nicht die Wirklichkeit ab, sondern soll lediglich einen unverbindlichen Anhaltspunkt für eine erste Orientierung geben. Insoweit gewährleistet VdS nicht die Fehlerfreiheit der in GeoVeris verarbeiteten Daten und der GeoVeris-Informationen, die durch den Berechtigte Nutzer eigenständig zu prüfen sind.

2.5 VdS ist berechtigt, den Zugang des Kunden und/oder einzelner oder mehrerer Berechtigter Nutzer zu GeoVeris zu sperren, wenn bei VdS die berechtigte Annahme besteht, dass der Kunde gegen den Nutzungsvertrag verstößt oder die dem Kunden eingeräumte Nutzungsmöglichkeit missbräuchlich, z.B. durch unbefugte Dritte, genutzt wird. VdS informiert den Kunden über die Sperrung nach ihrer Wahl schriftlich, in Textform oder beim Zugriff auf GeoVeris. Bestätigt sich die Annahme von VdS nicht, wird VdS den gesperrten Zugang wieder freigeben. Dem Kunden bleibt der Nachweis vorbehalten, dass der angenommene Verstoß nicht vorliegt. Für die Dauer einer berechtigten Sperrung von Anwendungen wird VdS von ihrer Leistungspflicht frei. Dem Kunden stehen aufgrund einer berechtigten Sperrung keine Ansprüche gegen VdS zu.

3. Einräumung von Nutzungsrechten

3.1 VdS räumt dem Kunden während der Laufzeit des Nutzungsvertrages das zeitlich beschränkte, nicht ausschließliche, nicht übertragbare Recht ein, die über GeoVeris durch Berechtigte Nutzer abgerufenen GeoVeris-Informationen für Zwecke der Berechtigten Nutzung im Rahmen der in GeoVeris vorgesehenen Funktionalitäten und Nutzungsmöglichkeiten und unter Beachtung dieser Nutzungsbedingungen zu verarbeiten und zu nutzen.

3.2 Die gemäß Ziff. 3.1 eingeräumten Nutzungsrechte für GeoVeris schließen das nicht ausschließliche Recht des Kunden ein, die GeoVeris-Informationen im Rahmen der eigenen Geschäftstätigkeit für die Berechtigte Nutzung zu verwenden bzw. durch Berechtigte Nutzer verwenden zu lassen sowie sie Berechtigten Empfängern zugänglich zu machen, wenn und soweit für die Berechtigte Nutzung erforderlich ist.

3.3 Es ist ferner ausdrücklich untersagt, GeoVeris-Informationen außerhalb der Berechtigten Nutzung zu verarbeiten und zu nutzen oder GeoVeris-Informationen an andere als die im Nutzungsvertrag bezeichneten Berechtigten Empfänger weiterzugeben. Sind im Nutzungsvertrag keine Berechtigten Empfänger bezeichnet, ist die Weitergabe von GeoVeris-Informationen nicht zulässig. Unzulässig ist es insbesondere, die GeoVeris-Informationen zu veröffentlichen, öffentlich zugänglich zu machen oder unter Verwendung der GeoVeris-Informationen eigene Datenbanken, Informationsdienste oder vergleichbare Informationssammlungen anzulegen und/oder diese zu vervielfältigen, zu verbreiten, zu veröffentlichen oder öffentlich zugänglich zu machen.

3.4 VdS ist berechtigt, die Nutzung bestimmter Bestandteile der GeoVeris-Informationen mit ergänzenden Nutzungsbeschränkungen zu versehen, insbesondere aufgrund entsprechender Anforderungen von Lizenzgebern der für die GeoVeris-Informationen verwendeten Daten. Informationen zu ergänzenden Nutzungsbeschränkungen werden dem Kunden bzw. dem Berechtigten Nutzer in Schrift- oder Textform oder innerhalb von GeoVeris mitgeteilt.

3.5 Bei der Berechtigten Nutzung ist auf die Quelle hinzuweisen: (aus: GeoVeris, © VdS). Soweit innerhalb von GeoVeris und/oder auf ausgegebenen GeoVeris-Informationen darauf hingewiesen wird, dass auch weitere Quellenangaben anzubringen sind, ist dies zu beachten.

3.6 Sämtliche vorgenannten Nutzungsrechte werden zeitlich beschränkt eingeräumt.

3.7 Die Rechteeinräumung endet

3.7.1 mit Beendigung des Nutzungsvertrages (insbesondere durch eine Kündigung durch VdS oder dem Kunden);

3.7.2 wenn VdS gegenüber dem Kunden schriftlich oder in Textform anzeigt, dass die Nutzung aus rechtlichen Gründen (insbesondere aufgrund von Nutzungsbeschränkungen durch Inhaber von Rechten an den für GeoVeris verwendeten Daten und/oder an der Plattform oder anderen technischen Komponenten, die für den Betrieb von GeoVeris notwendig sind) nicht mehr erfolgen darf; dies kann sich auf einzelne oder alle Komponenten von GeoVeris und/oder der GeoVeris-Informationen beziehen; oder

3.7.3 wenn ergänzende Bedingungen für die zeitliche Beschränkung der Rechteeinräumung eintreten, über die VdS den Nutzer innerhalb von GeoVeris (v.a. vor dem Abruf von GeoVeris-Informationen) informiert hat.

3.8 Mit Beendigung der Rechteeinräumung ist der Kunde zur Deaktivierung der bei ihm eingerichteten Abrufmöglichkeit und zur Löschung der entsprechenden beim Kunden (einschließlich aller Berechtigten Nutzer) vorhandenen GeoVeris-Informa-

tionen und datenschutzkonformer Vernichtung sonstiger Produkte, Datenträger oder Dokumentationen (einschließlich etwaiger Sicherungskopien) verpflichtet. Hiervon ausgenommen sind bereits erstellten Vervielfältigungen, die aufgrund gesetzlicher oder vertraglicher Aufbewahrungspflichten (z.B. als Bestandteil einer Beratungsdokumentation) weiter aufzubewahren sind. Der Kunde ist auf Anfrage von VdS verpflichtet, die Löschung der GeoVeris-Informationen und der sonstigen Produkte, Datenträger oder Dokumentationen (einschließlich etwaiger Sicherungskopien) schriftlich zu bestätigen.

3.9 VdS behält sich vor, die Einhaltung der vorstehenden Nutzungsbeschränkungen durch geeignete Maßnahmen (insbesondere die Implementierung von Testdaten in den GeoVeris-Datenbestand) zu überprüfen.

4. Nutzung nur durch berechtigte Nutzer

4.1 Der Kunde stellt durch geeignete technische und organisatorische Maßnahmen sicher, dass die Nutzung von GeoVeris und der GeoVeris-Informationen nur durch Berechtigte Nutzer erfolgen kann.

4.2 Der Kunde wird insbesondere sicherstellen, dass jeder Berechtigte Nutzer GeoVeris nur nach Eingabe einer Benutzerkennung und eines Passwortes nutzen kann.

4.3 Darüber hinaus hat der Kunde Berechtigte Nutzer vor dem erstmaligen Zugang zu GeoVeris ausdrücklich auf die Einhaltung der Regelungen des Nutzungsvertrags zu verpflichten und VdS die Einhaltung dieser Verpflichtung auf Verlangen nachzuweisen. VdS behält sich ausdrücklich vor, den Kunden bzw. den Berechtigten Nutzern eine elektronische Lösung zur Abgabe der Erklärung (etwa im Rahmen des GeoVeris-Zugangs) zur Verfügung zu stellen.

5. Vergütung

5.1 Der Kunde ist verpflichtet, für die Nutzung von GeoVeris nach Maßgabe des Nutzungsvertrages das in der Preisliste festgelegte Entgelt an VdS zu zahlen. Sofern nicht anders angegeben, sind sämtliche Preisangaben Nettopreise ohne die gesetzliche Umsatzsteuer.

5.2 VdS ist berechtigt, die Preisliste anzupassen und wird den Kunden hierüber unter Beachtung einer Frist von drei Monaten schriftlich oder in Textform informieren. Der Kunde ist berechtigt, diesen Vertrag unter Beachtung einer Frist von zwei Wochen zu dem von VdS in der angepassten Preisliste genannten Anpassungstermin zu kündigen.

5.3 VdS ist berechtigt, die angefallenen Entgelte für jeden Abruf von GeoVeris-Informationen unmittelbar nach dem Abruf gegenüber dem Kunden in Rechnung zu stellen.

5.4 Entgelte sind innerhalb von 14 Tagen nach Rechnungseingang auf das in der Rechnung angegebene Konto zur Zahlung fällig, sofern in der Rechnung von VdS keine längere Zahlungsfrist angegeben wird.

6. Vertragsdauer, Kündigung

6.1 Der Nutzungsvertrag kommt mit Annahme des auf den Abschluss des Nutzungsvertrages gerichteten Angebots durch ausdrückliche Erklärung von VdS zustande und wird auf unbestimmte Zeit geschlossen. Während der Laufzeit kann der Nutzungsvertrag von jeder Partei unter Beachtung einer Kündigungsfrist von einem Monat zum Ende eines jeden Kalendermonats gekündigt werden.

6.2 Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere dann vor, wenn

6.2.1 der zwischen VdS und dem von VdS beauftragten Dienstleister für den Betrieb von GeoVeris abgeschlossene Vertrag, gekündigt, aufgehoben oder auf andere Weise beendet wird,

6.2.2 der zwischen VdS und dem Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) bestehende Vertrag über den Betrieb von GeoVeris gekündigt, aufgehoben oder auf andere Weise beendet wird,

6.2.3 eine staatliche Stelle die weitere Nutzung von für den Betrieb von GeoVeris relevanten Daten aus Gründen der öffentlichen Sicherheit mit sofortiger Wirkung untersagt,

6.2.4 die Nutzung der für den Betrieb von GeoVeris relevanten Daten (insbesondere aufgrund von Nutzungsbeschränkungen durch Inhaber von Rechten an den für GeoVeris verwendeten Daten) nicht mehr erfolgen darf,

6.2.5 eine der beiden Parteien den Vertrag schwerwiegend verletzt und diese Vertragsverletzung nicht innerhalb einer angemessenen Frist nach Abmahnung durch die andere Partei behebt, wobei § 323 Abs. 2 BGB für die Entbehrlichkeit der Abmahnung entsprechend gilt;

6.2.6 sich die Vermögensverhältnisse einer Partei so verschlechtern, dass die Erreichung des Vertragszwecks gefährdet ist;

6.2.7 oder über das Vermögen einer Partei ein Insolvenzverfahren eröffnet oder ein Antrag auf Eröffnung eines solchen gestellt wird und die offenbare Unbegründetheit des Antrags nicht unverzüglich nachgewiesen wird.

6.3 Die Kündigung hat schriftlich oder in Textform zu erfolgen.

6.4 Die durch diesen Vertrag übertragenen Nutzungsrechte fallen nach Ende der Vertragslaufzeit ohne weitere Rechtshandlung an VdS zurück. Dies gilt auch im Hinblick auf etwaige Rechte an Sicherungskopien. Ein Recht zur weiteren Nutzung von GeoVeris besteht ab dem Ende der Vertragslaufzeit nicht mehr.

7. Haftung

7.1 VdS haftet für Schäden, außer im Fall der Verletzung wesentlicher Vertragspflichten, nur, wenn und soweit VdS, ihren gesetzlichen Vertreter, leitenden Angestellten oder sonstigen Erfüllungsgehilfen Vorsatz oder grobe Fahrlässigkeit zur Last fällt. Im Fall der Verletzung wesentlicher Vertragspflichten haftet VdS für jedes schuldhafte Verhalten ihrer gesetzlichen Vertreter, leitender Angestellter oder sonstiger Erfüllungsgehilfen, wobei der Begriff der „wesentlichen Vertragspflichten“ solche Pflichten bezeichnet, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht, auf deren Einhaltung die Mitglieder regelmäßig vertrauen dürfen und deren Verletzung die Erreichung des Vertragszwecks gefährdet.

7.2 Außer bei Vorsatz oder grober Fahrlässigkeit gesetzlicher Vertreter, leitender Angestellter oder sonstiger Erfüllungsgehilfen, ist die Haftung von VdS der Höhe nach auf die bei Vertragsschluss typischerweise vorhersehbaren Schäden begrenzt.

7.3 Eine Haftung für den Ersatz mittelbarer Schäden, insbesondere für den entgangenen Gewinn, besteht nur bei Vorsatz oder grober Fahrlässigkeit gesetzlicher Vertreter, leitender Angestellter oder sonstiger Erfüllungsgehilfen von VdS.

7.4 Die vorgenannten Haftungsausschlüsse gelten nicht im Fall der Übernahme ausdrücklicher Garantien durch VdS und für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit sowie im Fall zwingender gesetzlicher Regelungen.

8. Datenschutz

8.1 Die Nutzung von GeoVeris (einschließlich der GeoVeris-Informationen) unterliegt datenschutzrechtlichen Beschränkungen. Die GeoVeris-Informationen werden nach Auffassung der Aufsichtsbehörden für den Datenschutz durch ihre Zuordnung zu einem bestimmten Objekt oder einem bestimmten Punkt zu personenbezogenen Daten im Sinne der DSGVO, spätestens, wenn sie darüber einer bestimmten Person zugeordnet werden können.

8.2 Vor diesem Hintergrund schließen die Parteien mit Abschluss des Nutzungsvertrages zugleich die dem Nutzungsvertrag als **Anlage 2** beigefügte Vereinbarung über Auftragsverarbeitung ab.

8.3 Der Kunde verpflichtet sich zudem, die datenschutzrechtlichen Bestimmungen bei seiner Nutzung von GeoVeris zu beachten. Danach dürfen nur die zur Wahrung

berechtigter Interessen (insbesondere zur Einschätzung und Kalkulation von objekt- oder ortsbezogenen Ereignissen und Risiken) erforderlichen Daten einem Objekt oder einer Fläche zugeordnet werden. Die GeoVeris-Informationen dürfen nicht zu anderen Zwecken genutzt werden, insbesondere nicht zur Erstellung georeferenzierter soziodemografischer Profile für den Rückschluss auf einzelne Personen. Der Kunde verpflichtet sich, die datenschutzrechtlichen Anforderungen in seinem Verantwortungsbereich insbesondere durch technische und organisatorische Maßnahmen sicherzustellen.

9. Schlussbestimmungen

9.1 Der Nutzungsvertrag und diese Nutzungsbedingungen unterliegen jeweils dem Recht der Bundesrepublik Deutschland unter Ausschluss des Kollisionsrechts. Gerichtsstand ist, soweit rechtlich zulässig, Köln.

9.2 Änderungen oder Ergänzungen dieses Nutzungsvertrages und dieser Nutzungsbedingungen– inklusive dieser Textformklausel – bedürfen zu ihrer Wirksamkeit der Textform. Mitteilungen können, soweit nicht ausdrücklich Abweichendes vereinbart ist, per E-Mail an die von den Parteien zu diesem Zweck zu benennenden E-Mail-Adressen übermittelt werden. Mündliche und telefonische Übermittlung sind hingegen nicht ausreichend.

9.3 Die Nichtigkeit einzelner Bestimmungen des Nutzungsvertrages oder dieser Nutzungs-bedingungen berührt die Wirksamkeit der anderen Bestimmungen nicht. Anstelle unwirksamer Bestimmungen treten in erster Linie solche, die den unwirksamen Bestimmungen in rechtswirksamer Weise wirtschaftlich am ehesten entsprechen. Gleiches gilt für eventuelle Regelungslücken.

Anlage 2
Vereinbarung über Auftragsverarbeitung GeoVeris

1. Gegenstand der Vereinbarung über Auftragsverarbeitung

Da die Erbringung der Vertragsleistungen unter dem Nutzungsvertrag durch VdS (nachfolgend auch "**Auftragnehmer**") auch die Verarbeitung personenbeziehbarer Daten im Auftrag und gemäß den Anweisungen des Kunden (nachfolgend auch "**Auftraggeber**") umfasst, schließen die Parteien ergänzend zum Nutzungsvertrag diese Vereinbarung zur Auftragsverarbeitung ("**AVV**"), um die Verpflichtungen beider Parteien zur Einhaltung des anwendbaren Datenschutzrechts (insbesondere der Anforderungen der EU Datenschutz-Grundverordnung („**DSGVO**“) näher zu spezifizieren.

2. Pflichten des Auftragnehmers

2.1 Weisungsbindung. Der Auftragnehmer darf die in **Anhang 1** zu dieser AVV aufgeführten und vom Auftraggeber zur Verfügung gestellten Kategorien personenbeziehbarer Daten nur für die in Anhang 1 beschriebenen Zwecke und nur in Übereinstimmung mit den vom Auftraggeber erteilten Weisungen verarbeiten.

2.2 Verarbeitung aufgrund zwingender gesetzlicher Regelungen. Falls der Auftragnehmer verpflichtet ist, personenbezogene Daten nach dem Recht der Union oder des Mitgliedstaates, dem der Auftragnehmer unterliegt, zu verarbeiten, wird der Auftragnehmer den Auftraggeber hierüber vor der jeweiligen Verarbeitung schriftlich informieren, es sei denn, das Gesetz verbietet solche Informationen aus wichtigen Gründen des öffentlichen Interesses. Im letztgenannten Fall wird der Auftragnehmer den Auftraggeber unverzüglich informieren, sobald ihm dies rechtlich möglich ist.

2.3 Technische/organisatorische Maßnahmen. Unter Berücksichtigung des Stands der Technik, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Auftragnehmer geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau für die im Auftrag des Auftraggeber durchgeführten Verarbeitungsvorgänge zu gewährleisten; einschließlich der als Mindeststandard in Anhang 2 näher beschriebenen Maßnahmen.

2.4 Laufende Bewertung und Verbesserung der technischen/organisatorischen Maßnahmen. Der Auftragnehmer prüft und bewertet die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung im erforderlichen Umfang fortlaufend. Im Falle einer Verbesserung der

technischen und organisatorischen Maßnahmen wird der Auftragnehmer dem Auftraggeber auf Verlangen den Entwurf einer entsprechend aktualisierten Anlage 2 zur Verfügung zu stellen.

2.5 Compliance-Unterstützung. Der Auftragnehmer unterstützt auf dessen Anfrage den Auftraggeber in dem Umfang, der erforderlich ist, um die Einhaltung der datenschutzrechtlichen Verpflichtungen des Auftraggebers zu gewährleisten, indem er diejenigen Informationen zur Verfügung stellt und Unterstützungsleistungen erbringt, die der Auftraggeber zur Einhaltung datenschutzrechtlicher Vorschriften benötigt.

2.6 Informations-, Auskunfts- und Kontrollrechte. Der Auftragnehmer gewährt dem Auftraggeber und seinen Beauftragten während der Laufzeit dieser AVV auf Anfrage innerhalb einer angemessenen Frist die erforderlichen Informationen, um die Einhaltung der AVV und des anwendbaren Datenschutzrechts durch den Auftragnehmer zu überprüfen. Grundsätzlich erfolgen Kontrollmaßnahmen durch Abgabe von Eigenerklärungen des Auftragnehmers (oder der ggf. von ihm nach Maßgabe dieser AVV eingeschalteten Subunternehmer) oder durch Vorlage von Prüfungsergebnissen unabhängiger Dritter. Soweit es für den Auftraggeber zur Erfüllung seiner gesetzlichen Verpflichtungen erforderlich ist, kann sich der Auftraggeber nach rechtzeitiger vorheriger Anmeldung zu Prüfzwecken in den Betriebsstätten zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen. Das Recht zur Durchführung der Kontrollmaßnahmen hat der Auftraggeber auch bereits vor Beginn der Datenverarbeitung. Die Kontrolle kann vom Datenschutzbeauftragten oder sonstigen Vertretern des Auftraggebers, welche zur Verschwiegenheit verpflichtet sind und gegen die der Auftragnehmer keine berechtigten Bedenken hat, durchgeführt werden. Umgehend im Anschluss an die Kontrolle der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen werden die Ergebnisse dieser Kontrolle vom Auftraggeber dokumentiert. Die Dokumentation ist dem Auftragnehmer im Anschluss zeitnah zur Verfügung zu stellen. Jede Partei trägt ihre im Zusammenhang mit den Kontrollmaßnahmen anfallenden Kosten.

2.7 Verletzung gesetzlicher / vertraglicher Bestimmungen durch Weisungen des Auftraggebers. Der Auftragnehmer wird den Auftraggeber benachrichtigen, wenn er der Ansicht ist, dass eine von ihm erhaltene Weisung gegen geltendes Datenschutzrecht und/oder gegen vertragliche Pflichten aus der AVV verstößt. Diese Hinweispflicht verpflichtet den Auftragnehmer nicht zu einer Prüfung etwaiger Weisungen. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung

solange auszusetzen, bis sie durch eine weisungsberechtigte Person des Auftraggebers bestätigt oder geändert wird.

2.8 Verletzung gesetzlicher / vertraglicher Bestimmungen durch den Auftragnehmer. Im Falle einer tatsächlichen oder vermuteten Verletzung des Schutzes personenbezogener Daten oder im Falle eines Verstoßes des Auftragnehmers, seiner Mitarbeiter oder sonstiger vom Auftragnehmer eingesetzter Dritter gegen datenschutzrechtlicher Vorschriften oder dieser AVV verpflichtet sich der Auftragnehmer

2.8.1 dem Auftraggeber unverzüglich (spätestens jedoch 36 Stunden nach Bekanntwerden des Ereignisses) über ein solches Ereignis beim Auftragnehmer oder einem Unterauftragnehmer zu informieren und dem Auftraggeber unverzüglich (wenn möglich, spätestens 36 Stunden nach Bekanntwerden des Ereignisses) angemessene Einzelheiten über das Ereignis mitzuteilen und

2.8.2 dem Auftraggeber auf Anfrage eine angemessene Zusammenarbeit und Unterstützung in Bezug auf alle Maßnahmen zu gewähren, die als Reaktion auf ein solches Ereignis im Rahmen der anwendbaren Datenschutzgesetze (v.a. nach Art. 33 (3), 34 (4) DSGVO) erforderlich sind.

2.9 Verzeichnis von Verarbeitungstätigkeiten. Der Auftragnehmer führt ein Verzeichnis über die im Auftrag des Auftraggebers durchgeführten Verarbeitungstätigkeit gemäß Art. 30 (2) GDPR und stellt dieses auf Anfrage dem Auftraggeber zur Verfügung.

2.10 Berichtigung, Löschung, Sperrung / Einschränkung der Verarbeitung. Aufzeichnungen, die vom Auftraggeber übermittelte personenbezogene Daten enthalten, dürfen nur gemäß den Anweisungen des Auftraggebers und der anwendbaren Datenschutzgesetze berichtigt, gelöscht und/oder gesperrt werden. Diese Verpflichtung bezieht sich nicht auf die vom Auftragnehmer zur Erbringung der Vertragsleistungen gespeicherten personenbeziehbaren Daten.

2.11 Aufsichtsbehörde. Der Auftragnehmer verpflichtet sich zur Zusammenarbeit und zur Einhaltung von Anweisungen, Richtlinien und Auflagen der zuständigen Aufsichtsbehörde.

2.12 Unterstützung bei Beschwerden oder Anfragen. Falls der Auftragnehmer Beschwerden, Anfragen oder Mitteilungen erhält, die sich auf die Verarbeitung personenbezogener Daten oder auf die Einhaltung der anwendbaren Datenschutzgesetze oder dieser AVV durch eine der Parteien beziehen, wird der Auftragnehmer den Auftraggeber unverzüglich benachrichtigen und dem Auftraggeber in Bezug auf solche Beschwerden, Anfragen oder Mitteilungen die erforderliche Mitwirkung, Informationen und Unterstützung (einschließlich der Berichtigung, Löschung und Sperrung personenbezogener Daten) gewähren.

2.13 Pflichten bei Beendigung der Auftragsverarbeitung. Bei Beendigung dieser AVV wird der Auftragnehmer auf Anweisung des Auftraggebers die vom Auftraggeber übermittelten personenbezogenen Daten entweder zurückgeben oder vernichten, wenn und soweit die weitere Speicherung dieser personenbezogenen Daten nicht zur Erfüllung von gesetzlichen Anforderungen erforderlich ist. Diese Verpflichtung bezieht sich nicht auf die vom Auftragnehmer zur Erbringung der Vertragsleistungen gespeicherten personenbeziehbaren Daten.

3. Datenverarbeitung außerhalb der EU/des EWR

Der Auftragnehmer kann die Verarbeitung personenbezogener Daten im Rahmen dieser AVV auch außerhalb der EU/des EWR durchführen, wenn er die erforderlichen Garantien zur Gewährleistung eines angemessenen Datenschutzniveaus umsetzt.

4. Pflichten des Auftraggebers

4.1 Verantwortlichkeit. Der Auftraggeber ist für die Rechtmäßigkeit der in Anlage 1 spezifizierten Verarbeitung personenbezogener Daten verantwortlich. Der Auftraggeber bleibt verantwortlich für alle Anforderungen des anwendbaren Datenschutzrechts in Bezug auf die betroffenen Personen, einschließlich, aber nicht beschränkt auf die Beantwortung von Auskunftsersuchen der betroffenen Personen.

4.2 Weisungen. Der Auftraggeber ist nach näherer Maßgabe von Anlage 1 berechtigt, Weisungen über den Umfang und die Art und Weise der Verarbeitung personenbezogener Daten zu erteilen. Weisungsberechtigt sind nur Personen, die befugt sind, den Auftraggeber im Geschäftsverkehr umfassend zu vertreten.

5. Personal

5.1 Der Auftragnehmer wird bei der Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers das Datengeheimnis beachten und die mit der Datenverarbeitung betrauten Personen zur Vertraulichkeit verpflichten. Auf Verlangen des Auftraggebers wird der Auftragnehmer die Verpflichtungen aller Personen, die an der Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers beteiligt sind, nachweisen.

5.2 Der Auftragnehmer wird dafür sorgen, dass alle an der Datenverarbeitung beteiligten Personen mit den einschlägigen Datenschutzbestimmungen vertraut gemacht werden. Der Auftragnehmer wird die Einhaltung dieser Datenschutzbestimmungen und dieser AVV durch diese Personen überwachen.

6. Unterauftragnehmer

6.1 Der Auftragnehmer ist berechtigt, die in diesem Vertrag geregelte Auftragsverarbeitung ganz oder teilweise durch andere Dritte erfüllen zu lassen. Dies gilt auch für Tätigkeiten, die mit der in diesem Vertrag geregelten Auftragsverarbeitung im

Zusammenhang stehen und bei denen nicht ausgeschlossen werden kann, dass Dritte auf die personenbezogenen Daten des Auftraggebers zugreifen kann. Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern informieren.

6.2 Der Auftragnehmer ist verpflichtet, mit seinen Unterauftragnehmern, die er mit der Verarbeitung personenbeziehbarer Objektdaten des Auftraggebers beauftragt, eine schriftliche Vereinbarung abzuschließen. Diese darf in Bezug auf die Interessen des Auftraggebers kein geringeres Schutzniveau als diese AVV aufweisen.

7. Freistellung

7.1 Wenn gegen eine Partei aufgrund einer Verletzung der Verpflichtungen der anderen Partei nach dem anwendbaren Datenschutzgesetz und/oder dieser AVV von Dritten Ansprüche geltend gemacht werden, wird die andere Partei die in Anspruch genommene Partei von allen durch die Verletzung entstandenen Kosten, Gebühren, Schäden, Aufwendungen oder Verluste freistellen.

7.2 Die Freistellung setzt voraus, dass

7.2.1 die in Anspruch genommene Partei die andere Partei unverzüglich über den geltend gemachten Anspruch informiert; und

7.2.2 der anderen Partei die Möglichkeit gegeben wird, gemeinsam mit der in Anspruch genommenen Partei den geltend gemachten Anspruch abzuwehren oder zu vergleichen.

8. Vertragsdauer und Kündigung

8.1 Diese AVV tritt mit Unterzeichnung durch beide Parteien in Kraft und ist auf unbestimmte Zeit abgeschlossen. Diese AVV kann von jeder Partei gegenüber der jeweils anderen Partei gekündigt werden, sobald der letzte Auftrag des Auftraggebers, der die Verarbeitung personenbezogener Daten umfasst, vollständig abgewickelt wurde.

8.2 Unbeschadet der vorstehenden Ziffer 8.1 kann jede Partei die AVV jederzeit aus wichtigem Grund gemäß § 314 BGB kündigen.

8.3 Kündigungen bedürfen der Schriftform.

9. Schlussbestimmungen

9.1 Diese AVV unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des Kollisionsrechts.

9.2 Diese AVV enthält zusammen mit dem Nutzungsvertrag die gesamte Vereinbarung der Parteien über den Gegenstand (Auftragsverarbeitung personenbezogener Daten). Im Falle von Widersprüchen zwischen dem Nutzungsvertrag und dieser AVV gehen die Regelungen der AVV vor. Änderungen und Ergänzungen dieser AVV

bedürfen zu ihrer Gültigkeit der Schriftform und der Unterschrift von bevollmächtigten Vertretern der Parteien. Dies gilt auch für eine Änderung dieses Schriftformerfordernisses.

9.3 Für den Fall, dass eine Klausel dieser AVV unwirksam sein sollte, oder die AVV in Bezug auf einen bestimmten Gegenstand eine Lücke aufweist, bleibt die Wirksamkeit der übrigen Klauseln hiervon unberührt. In diesem Fall haben die Parteien eine Vereinbarung zu treffen, die dem Zweck der unwirksamen Klausel, oder im Falle einer Lücke, der Systematik und dem Schutzzweck der gesamten AVV, am ehesten entspricht.

Anhang 1
Einzelheiten der Auftragsverarbeitung

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand des Auftrags

1.1.1 Der Auftraggeber stellt dem Auftragnehmer nach Maßgabe des Nutzungsvertrages einen Online-Zugriff auf GeoVeris zur Verfügung. Zur Nutzung von GeoVeris ist es erforderlich, dass der Auftraggeber dem Auftragnehmer Geo-Punktdaten übermittelt, damit Geoinformationen zu den vom Auftraggeber durch Geo-Punktdaten bezeichneten Objekten zugeordnet werden können. Eine weitere Verarbeitung oder Nutzung der Geo-Punktdaten durch den Auftraggeber findet nicht statt.

1.1.2 Der Auftraggeber wird nur Daten (insbesondere Geo-Punktdaten) an den Auftragnehmer übermitteln, bezüglich derer er selbst ausschließlich Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO ist und die er unter Beachtung der datenschutzrechtlichen Bestimmungen erhoben hat.

1.2 Dauer des Auftrags

Die Dauer des Auftrags entspricht der Laufzeit des Nutzungsvertrages.

2. Konkretisierung des Auftragsinhalts

2.1 Art der Auftragsverarbeitung von personenbeziehbaren Daten

2.1.1 Der Auftragnehmer verarbeitet bei Nutzung von GeoVeris durch den Auftraggeber Geo-Punktdaten, die nach Auffassung der Aufsichtsbehörden für den Datenschutz personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO sind.

2.1.2 Beim Auftragnehmer werden die vom Auftraggeber ausschließlich online übermittelten Geo-Punktdaten durch GeoVeris automatisch verarbeitet. Dabei können vom Auftraggeber zum Zweck der Abfragevorbereitung Klartext-Adressen der abzufragenden Orte an den Auftragnehmer übermittelt werden. Dort werden diese automatisch in Punktkoordinaten des Objekts (Objektkoordinaten) umgerechnet und diese Punktkoordinaten werden dem Auftraggeber online zurück übermittelt (Geocoder-Funktion). Bei einer sofort oder später erfolgenden Abfrage der Geoinformationen zu dem Objekt (den Objekten) aus GeoVeris werden diese Geoinformationen dann den Objektkoordinaten zugeordnet und mit diesen online an den Auftraggeber übermittelt. Dabei werden die vom Auftraggeber übermittelten Adressdaten und Geokoordinaten beim Auftragnehmer in automatisierten Dateien gespeichert. Diese Dateien werden vorbehaltlich abweichender

Vereinbarungen mit dem Auftraggeber im Einzelfall unter Beachtung der gesetzlichen Vorschriften (einschließlich der anwendbaren handels- und steuerrechtlichen Aufbewahrungspflichten) gespeichert.

2.2 Der Datenverarbeitungsvorgang gliedert sich in folgende Verarbeitungsschritte:

2.2.1 Ein Berechtigter Nutzer des Auftraggebers loggt sich mit Benutzernamen und Passwort auf der GeoVeris-Plattform ein.

2.2.2 Anschließend übermittelt er durch Eingabe in eine vorgegebene Maske an den Auftragnehmer Adressdaten oder Geokoordinaten (bei Ereignis-Abfragen zudem obligatorisch die Schadennummer und optional die Versicherungsscheinnummer; bei Risikoabfragen optional eine Projektnummer) und wählt die gewünschten Produkte aus.

2.2.3 Soweit Adressdaten übermittelt werden, rechnet der Auftragnehmer diese in Geokoordinaten um.

2.2.4 Die Geokoordinaten werden mit den beim Auftragnehmer verfügbaren Geoinformationen angereichert.

2.2.5 Die angereicherten Datensätze werden an den Auftraggeber zurückübermittelt.

2.2.6 Der Abschluss der Abfrage-Sitzung erfolgt durch ein Logout des Nutzers oder nach Timeout.

2.3 Zweck der Auftragsverarbeitung personenbeziehbarer Daten

Dem Auftraggeber soll es ermöglicht werden, einzelnen Adressen Geoinformationen zuzuordnen. Dies erfolgt nur im Zusammenhang mit der im Nutzungsvertrag vereinbarten zulässigen Nutzung von GeoVeris zur Beurteilung, Bearbeitung und Regulierung von Schadensfällen.

2.4 Arten personenbeziehbarer Daten

In GeoVeris werden neben den personenbeziehbaren Adressdaten oder Geokoordinaten ohne Namensangaben ausschließlich die in der jeweils geltenden Leistungsbeschreibung zum Nutzungsvertrag genannten Geoinformationen zur Verfügung gestellt.

2.5 Kategorien betroffener Personen

Die übermittelten Adressdaten oder Geokoordinaten können zu Objekten gehören, die bereits Gegenstand von Verträgen zwischen dem Auftraggeber und Dritten sind oder die im Rahmen der Bearbeitung von Geschäftsvorfällen mit Bezug zu bestimmten Risiken gegenüber dem Auftraggeber genannt wurden und für diese Bearbeitung erforderlich sind. Betroffene sind daher regelmäßig solche Personen, die mit dem Auftragnehmer in einer vertraglichen oder sonstigen geschäftlichen Beziehung stehen sowie Personen, die zu dem durch die Adresse oder Geokoordinate

bezeichneten Objekt in einer rechtlichen Beziehung stehen (wie Eigentümer und Inhaber sonstiger Rechte laut Grundbuch, Mieter, Pächter, Bewohner oder sonstige Personen, die das Objekt nicht nur vorübergehend nutzen, ebenso wie dort polizeilich gemeldete Personen).

3. Weisungen des Auftraggebers

3.1 Die Verarbeitung der personenbeziehbaren Daten erfolgt im Rahmen von GeoVeris überwiegend automatisiert nach den Eingaben des Auftraggebers im Rahmen der vom Auftragnehmer definierten Funktionalitäten und Einsatzbedingungen von GeoVeris. Eine manuelle Steuerung oder Eingriffsmöglichkeit des Auftragnehmers in einen laufenden Datenverarbeitungsprozess ist nicht vorgesehen. Auf die automatisierte Datenverarbeitung kann durch Weisungen des Auftraggebers an den Auftragnehmer in der Regel kein sofortiger Einfluss genommen werden. Vor diesem Hintergrund gelten vom Auftragnehmer definierte Maßgaben und die vom Auftraggeber an den Auftragnehmer erteilten Aufträge zugleich auch als Weisungen des Auftraggebers an den Auftragnehmer im Hinblick auf Art und Umfang der Verarbeitung und Nutzung personenbezogener Daten.

3.2 Soweit im Rahmen von GeoVeris (z.B. bei der manuellen Zusammenstellung von Geo-Daten durch den Auftragnehmer oder einen vom Auftragnehmer beauftragten Dritten) Aufträge erteilt werden können, gelten die vom Auftraggeber an den Auftragnehmer erteilten Aufträge zugleich auch als Weisungen des Auftraggebers an den Auftragnehmer im Hinblick auf Art und Umfang der Verarbeitung und Nutzung personenbezogener Daten

3.3 Soweit dies möglich ist, ist der Auftragnehmer verpflichtet, Weisungen des Auftraggebers im Hinblick auf seine Daten Folge zu leisten, z. B. durch veränderte Programmierungen der zukünftigen Verarbeitungen seiner Objektdaten. Etwaige hierdurch verursachte Kosten sind vom Auftraggeber zu tragen. Die Weisungen sind schriftlich zu erteilen; mündliche Weisungen sind unwirksam.

3.4 Der Auftragnehmer wird den Auftraggeber darauf hinweisen, wenn er der Ansicht ist, dass eine Weisung gegen Datenschutzvorschriften verstößt. Diese Hinweispflicht verpflichtet den Auftragnehmer nicht zu einer Prüfung etwaiger Weisungen. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch eine weisungsberechtigte Person des Auftraggebers bestätigt oder geändert wird.

Anhang 2
Technische und organisatorische Maßnahmen

GeoVeris wird im Auftrag des Auftragnehmers durch die con terra GmbH unter Einbindung ausgewählter Unterauftragnehmer betrieben. Die hierbei von con terra GmbH bzw. den Unterauftragnehmern getroffenen technischen und organisatorischen Maßnahmen sind in dem beigefügten Dokument beschrieben.

con terra GmbH

Technische und Organisatorische Maßnahmen

Stand: 13.02.2020

Inhalt

Vorwort

Das Dokument beschreibt die als verbindlich festgelegten technischen und organisatorischen Maßnahmen im Zusammenhang mit durchgeführten Auftragsverarbeitungsvorgängen zwischen Auftraggeber und Auftragnehmer. Die dargestellten Maßnahmen stellen somit ein Abbild des gelebten Datenschutz- und Datensicherheitskonzept des Standortes dar.

Datenschutz- und Datensicherheitskonzept

Der folgende Maßnahmenkatalog beschreibt die im Rahmen der Auftragsverarbeitung zu treffenden technischen und organisatorischen Einzelmaßnahmen nach Art. 24 Abs. 1 EU-DS-GVO. Die EU-DS-GVO verpflichtet Unternehmen die Datenverarbeitung personenbezogener Daten durch angemessene, technische und organisatorische Maßnahmen abzusichern und personenbezogene Daten nach Möglichkeit zu pseudonymisieren. Die getroffenen Maßnahmen müssen dabei dem Risiko des jeweiligen Datenverarbeitungsvorgangs Rechnung tragen und dem derzeitigen Stand der Technik entsprechen. Diese Anforderungen erfüllt der Auftragnehmer durch ein wirksames Zusammenspiel aus Datenschutzmanagement und Informationssicherheitsmanagement und hat angemessene Maßnahmen zur Absicherung der Datenverarbeitungsvorgänge getroffen. Insbesondere die Schutzwerte: Verfügbarkeit, Vertraulichkeit, Integrität und Belastbarkeit. Den Schutzwerten werden dabei folgende informationssicherheitsrelevanten Definitionen zugrunde gelegt:

- Vertraulichkeit: Daten, Informationen und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen.
- Integrität: Der Begriff Integrität bezieht sich auf die Korrektheit der verarbeiteten Informationen und Daten.
- Verfügbarkeit: Der Begriff der Verfügbarkeit bezieht sich auf Informationen, Daten, Applikationen sowie Systeme und betrifft deren Funktionsfähigkeit bzw. Abrufbarkeit.
- Belastbarkeit: Die Belastbarkeit stellt als besonderen Aspekt der Verfügbarkeit die Anforderung, dass Systeme auch im Störfall, Fehlerfall oder bei hoher Belastung möglichst widerstandsfähig ausgestaltet sein müssen.

Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Zutrittskontrollsystem - Abschließbare Räume:

Im Unternehmen sind sämtliche Räume, in denen ein Zugriff auf personenbezogene Daten möglich ist, abschließbar.

Zutrittskontrollsystem:

Im Unternehmen wird ein zentral verwaltetes Zutrittskontrollsystem eingesetzt.

Server - Externer Einsatz:

Im Unternehmen werden keine externen Server (z.B. in einem Rechenzentrum) angemietet.

Sicherung des Unternehmensgeländes - Pförtner/Wachschutz:

Das Unternehmensgelände und ggfs. Teile davon werden durch einen Pförtner oder Wachschutz bewacht.

Server - Interner Einsatz:

In den Unternehmensräumlichkeiten werden keine Server eingesetzt.

Sicherung des Unternehmensgeländes - Abgrenzung:

Das Unternehmensgelände / die Unternehmensräumlichkeiten werden vom öffentlichen Bereich abgegrenzt durch:

- Abschließbare Tür

Zutrittskontrollsystem - Technisches Mittel:

Das Zutrittskontrollsystem basiert auf folgenden technischen Mitteln:

- Token/Transponder

Zutrittskontrollsystem - Verwaltung:

Das Zutrittskontrollsystem wird folgendermaßen verwaltet:

- Elektronisch

Sicherung des Unternehmensgeländes - Zeitraum:

Das Unternehmensgelände und ggfs. Teile davon werden durch einen Pförtner oder Wachschutz zu folgenden Zeiten bewacht:

- Sporadische Rundgänge außerhalb der Betriebszeiten

Zugangskontrolle

Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Tragbare Endgeräte - Zugangssperren:

Im Unternehmen verfügen tragbare Endgeräte über Zugangssperren (Passwort, PIN, Muster o. A.).

Fernwartung - VPN:

Im Unternehmen wird zur Fernwartung ein VPN-Tunnel eingesetzt.

Fernwartung - Regelungen zur Kontrolle von Fernwartung:

Im Unternehmen wurden Regelungen und Kontrollen hinsichtlich Fernwartung definiert.

Im Unternehmen werden folgende Regelungen und Kontrollen zur Fernwartung umgesetzt:

- User erstellt Ticket bei Comparex, Mitarbeiter ruft User an und frag auf Freischaltung, User muss dies bestätigen

Fernwartung - Sicherheitsmaßnahmen:

Im Unternehmen wird die Fernwartung unter angemessenen Sicherheitsmaßnahmen durchgeführt.

Fernwartung - Zugangsmöglichkeiten:

Im Unternehmen werden Fernwartungszugänge individuell freigegeben.

Passwort-Manager:

Im Unternehmen wird ein Passwort-Manager eingesetzt.

Passwort-Manager:

Passwort-Manager - Zugangskontrolle:

Der eingesetzte Passwort-Manager bietet eine ausreichende Zugangskontrolle und eine verschlüsselte Speicherung.

Tragbare Endgeräte - Passwortkomplexität:

Im Unternehmen werden ausreichend komplexe Passwörter und PINs, für die Nutzung von tragbaren Endgeräten gefordert.

Administratoren - Protokollierung:

Im Unternehmen werden die Aktivitäten innerhalb der Administratorenkonten protokolliert.

Authentifizierung - Zwei-Faktor-Authentifizierung:

Im Unternehmen wird eine Zwei-Faktor-Authentifizierung eingesetzt.

Authentifizierung - Single Sign-On Verfahren:

Im Unternehmen wird ein Single Sign-On Verfahren eingesetzt.

Authentifizierung - Single Sign-On-Verfahren mit Zwei-Faktor-Authentifizierung:

Im Unternehmen wird zur Anmeldung mittels Single Sign-On eine Zwei-Faktor-Authentifizierung eingesetzt.

Zugang zu personenbezogenen Daten in Bereichen mit Publikumsverkehr:

Im Unternehmen wird dafür gesorgt, dass personenbezogene Daten in Bereichen mit Publikumsverkehr nicht frei zugänglich sind.

Fernwartung - Tools:

Im Unternehmen werden folgende Tools zur Fernwartung eingesetzt:

- TeamViewer

Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

IT-Sicherheit - Firewall:

Im Unternehmen wird eine bzw. mehrere Firewalls gegen unerwünschte Netzwerkzugriffe eingesetzt.

Im Unternehmen werden folgende Firewalls eingesetzt:

- Meraki

Dokumentation - Berechtigungen:

Im Unternehmen wird die Vergabe sowie der Entzug von Zugangs- und Zugriffsberechtigungen für IT-Systeme dokumentiert.

Dokumentation - Digitale Verwaltung:

Im Unternehmen wird die Dokumentation über die Vergabe sowie den Entzug von Zugangs- und Zugriffsberechtigungen für IT-Systeme digital aufgezeichnet.

Dokumentation - Zugriffsschutz:

Im Unternehmen ist die Dokumentation der zugelassenen Benutzer, Benutzergruppen und Rechteprofile vor unbefugtem Zugriff geschützt.

Administratoren - Vergabe von Zugangs- und Zugriffsberechtigungen:

Im Unternehmen erfolgt die Vergabe von Zugangs- und Zugriffsberechtigungen anhand der Funktion der Zugangs- bzw. Zugriffsberechtigten.

Ausgeschiedene Personen - Entzug von Berechtigungen:

Im Unternehmen wird sichergestellt, dass sämtliche Zugangsberechtigungen und Zugriffsberechtigungen einer ausscheidenden Person zeitnah gesperrt und ggf. gelöscht werden.

Datenträgerkontrolle

Es ist zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Tragbare Endgeräte - Sicherheitsrichtlinie:

Im Unternehmen existiert eine aktuelle Sicherheitsrichtlinie für tragbare Endgeräte, in der alle umzusetzenden Sicherheitsmechanismen beschrieben sind.

Datenträgermanagement - Zugriffsschutz:

Im Unternehmen werden zur Entsorgung gesammelte schutzbedürftige Datenträger vor unberechtigtem Zugriff geschützt.

Tragbare Datenträger - Verschließbare Behältnisse:

Im Unternehmen stehen an allen Arbeitsplätzen verschließbare Behältnisse zur Verfügung, um Unterlagen und Datenträger sicher aufbewahren zu können.

Tragbare Endgeräte - Geeignete Aufbewahrung:

Im Unternehmen werden Benutzer von tragbaren Endgeräten auf die Einhaltung einer geeigneten Aufbewahrung verpflichtet.

Tragbare Endgeräte - Diebstahlsicherung:

Im Unternehmen werden tragbare Endgeräte außerhalb der Nutzungszeiten gegen Diebstahl gesichert.

Tragbare Endgeräte - Verwendungsrichtlinie:

Im Unternehmen wurde eine Verwendungsrichtlinie für tragbare Endgeräte definiert.

Datenträgermanagement - Ordnungsgemäßer Umgang:

Im Unternehmen wurde eine Richtlinie für den Umgang mit Datenträgern definiert.

Datenträgermanagement - Sichere Löschung:

Im Unternehmen werden elektronische Datenträger sicher gelöscht.

Tragbare Endgeräte - Freigabeverfahren für Applikationen:

Im Unternehmen gibt es ein Test- und Freigabeverfahren für Applikationen auf tragbaren Endgeräten.

Tragbare Endgeräte - Fernlöschung:

Im Unternehmen ist die Fernlöschung von Daten auf tragbaren Endgeräten möglich.

Tragbare Datenträger - Sichere Aufbewahrung:

Im Unternehmen existieren Richtlinien zur sicheren und sachgerechten Aufbewahrung von tragbaren Datenträgern und Endgeräten.

Datenträgermanagement - Verschlüsselung:

Im Unternehmen werden elektronische Datenträger verschlüsselt.

Datenträgermanagement - Schutzbedarfsstufen:

Im Unternehmen werden Datenträger hinsichtlich ihrer Vertraulichkeit in verschiedene Schutzbedarfsstufen eingeteilt.

Datenträgermanagement - Bestandsverzeichnis:

Im Unternehmen wird für folgende elektronischen Datenträger ein Bestandsverzeichnis geführt:

- Mobiltelefone
- Laptops
- Tabletcomputer

Datenträgermanagement - Verschlüsselungsverfahren:

Im Unternehmen werden folgende Verschlüsselungsverfahren für Datenträger verwendet:

- Bitlocker kommt zum Verschlüsseln der Notebooks zum Einsatz.In der Cloud werden die Storage Accounts verschlüsselt, auf denen die virtuellen Festplatten liegen

Datenträgermanagement - Klassifizierung der Schutzbedarfsstufen:

Im Unternehmen wurden folgende Schutzbedarfsstufen für Datenträger definiert:

- vertraulich, nicht vertraulich

Datenintegrität

Es ist zu gewährleisten, dass gespeicherte personenbezogene Daten nicht unautorisiert geändert werden.

IT-Sicherheitskonzept:

Im Unternehmen existiert ein IT-Sicherheitskonzept, welches die grundlegenden technischen und organisatorischen Maßnahmen darstellt, die im Unternehmen zur Gewährleistung von Datenschutz und Datensicherheit getroffen werden.

Technische und organisatorische Maßnahmen - Aktualität:

Im Unternehmen wird die Aktualität der technischen und organisatorischen Maßnahmen regelmäßig überprüft.

Übertragungskontrolle

Es ist zu gewährleisten, dass überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können.

VPN-Tunnel:

Im Unternehmen wird ein VPN-Tunnel zur Datenübertragung eingesetzt.

VPN-Tunnel - Firewall:

Im Unternehmen wird zusätzlich eine Firewall für den VPN-Tunnel eingesetzt.

Telekommunikation - Verbindung zum Telekommunikationsprovider:

Zur Verbindung mit dem Telekommunikationsprovider wird folgende Methode verwendet:

- Reguläre DSL/Glasfaserverbindung

VPN-Tunnel - Endpunkt Platzierung:

Der VPN-Tunnel Endpunkt ist an folgender Stelle platziert:

- In der Firewall

Transportkontrolle

Es ist zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

Datenübertragung - Datenträger:

Im Unternehmen werden keine Datenträger mit personenbezogenen Daten übermittelt.

Datenübertragung - Verschlüsselung:

Daten werden bei der Übertragung mit den folgenden Verfahren/Protokollen verschlüsselt:

- SSL/TLS
- WPA2
- IPSEC
- SSH

Benutzerkontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können.

Schulungen für Beschäftigte - Regelmäßigkeit:

Im Unternehmen finden regelmäßig Schulungen zum Thema Datenschutz statt.

Ausgeschiedene Personen - Rückforderung unternehmenseigener Gegenstände:

Im Unternehmen wird sichergestellt, dass sämtliche unternehmenseigene Gegenstände mit Bezug zu personenbezogenen Daten von einer ausscheidenden Person zurückgefordert werden.

Telekommunikation - Datenschutz für Telearbeiter:

Telearbeiter wurden auf die Einhaltung einschlägiger Datenschutzvorschriften hingewiesen.

Administratoren:

Im Unternehmen wurde für alle IT-Systeme und IT-Netze Administratoren sowie deren Stellvertreter bestimmt.

Administratoren - Spezielle Konten:

Im Unternehmen werden spezielle Administratorenkonten eingesetzt.

IT-Sicherheit - Administratoren Qualifikation:

Im Unternehmen wird sichergestellt, dass IT-Administratoren über ausreichende Qualifikation zur Ausübung ihrer Tätigkeit besitzen.

Mitarbeiter - Maßnahmen:

Um im Unternehmen die Beschäftigten auf die Wichtigkeit des Datenschutzes hinzuweisen und diese gemäß den Erfordernissen zu verpflichten, werden folgende Maßnahmen getroffen:

- Verpflichtung der Beschäftigten zu Verhaltensregeln
- Unternehmensinterne Datenschutz-Richtlinien
- Verpflichtung der Beschäftigten auf das Datengeheimnis
- Information der Mitarbeiter über Neuerungen zum Thema Datenschutz

Administratoren - Ebenen:

Im Unternehmen werden die Administratorenkonten auf folgender Ebene eingesetzt:

- Betriebssystem
- Datenbank
- Netzwerk
- Applikation

Mitarbeiter - Schulungen:

Um die Mitarbeiter auf die Wichtigkeit des Datenschutzes hinzuweisen und diese gemäß den Erfordernissen zu verpflichten, werden folgende Maßnahmen getroffen:

- Schulung aller zugriffsberechtigten Beschäftigten

Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Externe Dienstleister:

Das Unternehmen arbeitet mit externen Dienstleistern zusammen.

Externe Dienstleister - Weisungen zur Verarbeitung:

Im Unternehmen werden Weisungen zur Verarbeitung personenbezogener Daten ausschließlich schriftlich an Auftragsverarbeiter erteilt.

Externe Dienstleister - Auftragsverarbeitungsvertrag:

Im Unternehmen wurde mit allen Dienstleistern ein Auftragsverarbeitungsvertrag geschlossen.

Dienstleister Datenträgerentsorgung:

Es wird ein externer Dienstleister zur Entsorgung von Datenträgern genutzt.

Dienstleister Datenträgerentsorgung - Zertifizierung:

Der externe Dienstleister besitzt folgende Zertifizierung:

- Rhenus Data Office GmbH Zertifizierung Entsorgungsfachbetrieb Zertifizierung Datenschutz-Gütesiegel Zertifizierung DIN 66399 Zertifizierung Energiemanagement DIN EN ISO 50001 Zertifizierung Qualitätsmanagement DIN EN ISO 9001

Speicherkontrolle

Die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter, personenbezogener Daten ist zu verhindern.

Passwortschutz - Überprüfung der Passwortvorgaben:

Im Unternehmen wird die Einhaltung der Passwortvorgaben technisch überprüft.

Passwortschutz - Passwort-Wechsel-Intervalle:

Im Unternehmen werden Passwörter in regelmäßigen Abständen gewechselt.

Mitarbeiter - Fachgerechte Entsorgung personenbezogener Daten:

Im Unternehmen sind die Beschäftigten angehalten personenbezogene Daten fachgerecht zu entsorgen.

Passwortschutz - Passwortliste:

Es wird keine unverschlüsselte Passwortliste geführt.

Passwortschutz - Initialpasswörter:

Initialpasswörter müssen beim ersten Login geändert werden.

Passwortschutz - Passwortkomplexität:

Im Unternehmen gibt es eine Vorgabe für die Passwortkomplexität.

Passwortschutz - Vorgabe für die Passwortlänge:

Es gibt eine Vorgabe für die Passwortlänge.

Kamerabilder/Videoüberwachung - Passwortlänge:

Bitte machen Sie Angaben zur Passwortlänge

Passwortschutz - Protokollierung von Falscheingaben:

Falscheingaben des Passworts werden protokolliert.

Passwortschutz - Sperrung nach Falschanmeldungen:

Benutzer werden nach einer definierten Zahl von Falschanmeldungen automatisch gesperrt

Die Sperrung erfolgt nach der folgenden Anzahl von Falschanmeldungen:

- 5

Automatische Bildschirmsperre:

Im Unternehmen wird eine automatische Bildschirmsperre eingesetzt.

Automatische Bildschirmsperre - Zeitraum:

Im Unternehmen wird die automatische Bildschirmsperre nach maximal 10 Minuten aktiviert.

Verschlüsselung der Übertragung:

Daten werden bei der Übertragung mit den folgenden Verfahren/Protokollen verschlüsselt:

- SSL/TLS

Authentifizierung - Benutzerauthentifizierung IT-Systeme:

Zur Benutzerauthentifizierung in IT-Systemen werden folgende Verfahren verwendet:

- Passwort

Passwortschutz - Passwortbestandteile:

Die Passwörter bestehen aus folgenden Bestandteilen:

- Buchstaben
- Zahlen
- Sonderzeichen

Kamerabilder/Videoüberwachung - Wechselintervalle:

Folgende Wechselintervalle sind implementiert:

- 3 Monate

Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten jederzeit verfügbar sind und besonders gegen zufällige Zerstörung oder Verlust geschützt sind.

IT-Sicherheit - Schadsoftware in verschlüsselten Daten:

Im Unternehmen werden auch verschlüsselte Daten auf Schadsoftware geprüft.

Archivierungskonzept:

Im Unternehmen wurde ein Archivierungskonzept definiert, welches regelt, wie und wie lange Dokumente archiviert werden.

Archivierungskonzept - Gesetzliche Aufbewahrungspflicht:

Es liegt eine gesetzliche Aufbewahrungspflicht für die archivierten Dokumente vor.

Zuverlässigkeit

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust abgesichert sind.

IT-Sicherheit - Redundanz kritischer Systeme:

Im Unternehmen sind kritische Systeme und ggf. die Infrastruktur redundant ausgelegt.

Kamerasoftware - Updates:

Es werden regelmäßig Updates der Kamerasoftware durchgeführt.

IT-Sicherheit - Software zur Netzwerküberwachung:

Im Unternehmen wird eine Software zur Überwachung des Netzwerks bzw. der Anwendungen verwendet.

Im Unternehmen wird folgende Software zur Überwachung des Netzwerks bzw. der Anwendungen eingesetzt:

- Vom Anbieter Solarwinds die Produkte SAM und NPM

IT-Sicherheit - Software Aktualisierungen:

Aktualisierungen werden zeitnah wie folgt umgesetzt:

- Automatisiert

IT-Sicherheit - Trennung der Netzwerke:

Das Netzwerk zur Videoüberwachung ist wie folgt in verschiedene Segmente aufgeteilt:

- Virtuell getrennt

Wiederherstellbarkeit

Es ist zu gewährleisten, dass personenbezogene Daten bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

Notfallsituationen - Berechtigungskonzept:

Im Unternehmen gibt es ein Berechtigungskonzept für Notfallsituationen.

Sicherungen - Unternehmensweite Richtlinie:

Im Unternehmen gibt es eine unternehmensweite Richtlinie zu Sicherungen.

Sicherungen - Schriftliche unternehmensweite Richtlinie:

Im Unternehmen gibt es eine schriftlich definierte unternehmensweite Richtlinie zu Sicherungen.

Sicherungen - Umsetzung:

Im Unternehmen wird die Richtlinie zu Sicherungen auch in der Praxis umgesetzt.

Sicherungen - Wiederherstellungsmöglichkeiten:

Im Unternehmen können folgende Bereiche wiederhergestellt werden:

- Installationen
- Systemdateien- und Datencontainer
- Log-Daten
- Benutzerkonten
- Daten
- Konfigurationen (Einstellungen und Freigaben)

Sicherungen - Sicherungsarten:

Im Unternehmen werden folgende Sicherungsarten eingesetzt:

- Inkrementelle Sicherung
- Komplett-/Vollsicherung
- Differenzielle Sicherung
- Speicherabbildsicherung (Image Backup)

Sicherungen - Sicherungsmedien:

Im Unternehmen werden die folgenden Speichermedien für Sicherungen verwendet:

- Netzwerk- und Online-Datensicherung
- Optische Speicher

Sicherungen:

Im Unternehmen werden die Sicherungen durchgeführt von:

- Cloud-Anbieter
- Eigenständige Backups (z. B. durch NAS-System)

Trennbarkeit

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Trennung von Arbeitsplätzen:

Im Unternehmen werden Arbeitsplätze zur Verarbeitung besonderer Kategorien personenbezogener Daten räumlich von anderen Arbeitsplätzen getrennt.

Betriebssystem

Es ist zu verhindern, dass Unbefugte Zugriff auf Betriebssysteme erhalten können.

Passwortschutz - Wechselintervalle:

Auf Betriebssystemebene wird in folgendem Intervall das Passwort gewechselt:

- 3 Monate

Auf Betriebssystemebene werden Passwörter in regelmäßigen Abständen gewechselt.

Passwortschutz - Benutzerkonten:

Auf Betriebssystemebene wird jedes Benutzerkonto des Betriebssystems durch ein Passwort geschützt.

Passwortschutz - Passwortkomplexität:

Auf Betriebssystemebene gibt es eine Vorgabe für die Passwortkomplexität.

Passwortschutz - Überprüfung der Passwortvorgaben:

Auf Betriebssystemebene wird die Einhaltung der Passwortvorgaben technisch überprüft.

Passwortschutz - Passwortlänge:

Auf Betriebssystemebene gibt es eine Vorgabe für die Passwortlänge.

Auf Betriebssystemebene hat das Passwort eine Länge von mindestens 8 Zeichen.

Passwortschutz - Initialpasswörter:

Auf Betriebssystemebene müssen Initialpasswörter bei der ersten Anmeldung geändert werden.

Administration - Berechtigungskonzept in Test- und Entwicklungsumgebung:

Auf Betriebssystemebene wurde ein Berechtigungskonzept in den Test- und Entwicklungsumgebungen umgesetzt.

Protokoll - Protokollierung von Falscheingaben:

Auf Betriebssystemebene werden Falscheingaben von Benutzern protokolliert.

Passwortschutz - Sperrung nach Falscheingaben:

Auf Betriebssystemebene werden Benutzerkonten nach einer definierten Anzahl von Falschanmeldungen gesperrt.

Auf Betriebssystemebene erfolgt die Sperrung nach der folgenden Anzahl von Falschanmeldungen:

- 5

Passwortschutz - Passwortbestandteile:

Auf Betriebssystemebene bestehen die Passwörter mindestens aus folgenden Bestandteilen:

- Buchstaben
- Zahlen
- Sonderzeichen

Anwendungen

Es ist zu verhindern, dass Unbefugte Zugriff auf jegliche Anwendungen erhalten können.

Software - Trennung zwischen Umgebungen:

Im Unternehmen gibt es eine Trennung zwischen Produktiv-, Test-, und Entwicklungsumgebungen inkl. der Datenbanken.