ALLGEMEINE GESCHÄFTSBEDINGUNG ZUR AUFTRAGSVERARBEITUNG DER TERRA CLOUD GMBH

1. Präambel
Diese Bedingung beschreibt die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus den Verträgen der Parteien ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit einem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1 Anwendungsbereich und Verantwortlichkeit
Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im jeweiligen Vertrag und ggf. in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen jedes Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).
Die datenschutzrechtlichen Pflichten des Auftragnehmers sind durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.
Die Art der zu verarbeitenden Daten und die Kategorien der betroffenen Personen ergeben sich aus den Leistungsbeschreibungen der jeweils vom Kunden beauftragten TERRA CLOUD Leistungen und den dazugehörigen SLA. Diese sind unter https://downloads.terracloud.de abrufbar.

§ 2 Pflichten des Auftragnehmers
(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.
Die Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass ein angemessenes oder vertraglich vereinbartes Schutzniveau nicht unterschritten wird.
Eine Beschreibung der technisch-organisatorischen Maßnahmen des Auftragnehmers findet sich im Anschluss an diese Bedingungen.

(3) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Artt. 33 bis 36 DS-GVO genannten Pflichten. Dieser Aufwand wird dem Auftragnehmer vom Auftraggeber zu den jeweils geltenden Stundensätzen des Auftragnehmers vergütet.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisungen zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.
Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen und ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.
In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

(11) Die vorstehend geschilderten Aufwände sind vom Auftraggeber an den Auftragnehmer zu dessen jeweils gültigen Preisen gemäß Preisliste zu vergüten.

§ 3 Pflichten des Auftraggebers
(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. daten- schutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 4 Anfragen betroffener Personen
Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 5 Nachweismöglichkeiten
(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.
Für die Unterstützung bei der Durchführung einer Inspektion mit dem Auftraggeber wird dem Auftragnehmer sein Aufwand zu seinen jeweiligen gültigen Stundensätzen vergütet.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 6 Subunternehmer (weitere Auftragsverarbeiter)
(1) Der Auftragnehmer bedient sich zur Erfüllung seiner vertraglichen Verpflichtungen in bestimmten Fällen Subunternehmer. Diese sind unter https://downloads.terracloud.de abrufbar.

(2) Ein solches Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten. Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber mit einer Frist von drei Wochen. Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als gegeben.

(3) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 7 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Bedingungen und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Bedingungen unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(3) Es gilt deutsches Recht.

Anhang über technische und organisatorische Maßnahmen nach Art. 32 DSGVO (vgl. auch § 2 Abs. 2)

Die hier beschriebenen Informationen befinden sich in Zukunft auf der Webseite unter https://downloads.terracloud.de

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:
Das Gelände und das Gebäude sind rund um die Uhr kameraüberwacht. Es gibt Bewegungsmelder die außen das Licht einschalten und innen einen Alarm auslösen. Außerhalb der Betriebsstunden ist ein Wachschutz für Gebäude durch externe Dienstleister engagiert. Fenster und Türen sind alarmgesichert. Die Alarmanlage hat eine Aufschaltung zur Polizei. Der Zutritt zu dem Unternehmen erfolgt für die Besucher (inklusive Techniker und Kunden) ausschließlich über die Zentrale. Die Türen zur Lieferantenanfahrt werden von hier zum Zutritt berechtigter und angemeldeter Personen freigeschaltet. Laut Dienstanweisung bewegen sich Besucher nie alleine im Gebäude und tragen dauerhaft einen Besucherausweis. Jeder Besucher muss sich am Empfang anmelden. Der Zutritt betriebsfremder Personen wird an dieser Stelle protokolliert. Alle Techniker und Kunden müssen Ihren Besuch im Voraus anmelden, damit die Legitimation des Besuches überprüft werden kann. Der unbeaufsichtigte Zugang zum Gebäude (nur für Mitarbeiter) erfolgt über RFID Token in Kombination mit einem Passwort / PIN.

Zutritt zu den einzelnen Cubes

Unter einem Cube versteht man einen organisatorischen Bereich innerhalb des Rechenzentrums in dem die Server untergebracht sind. Der Zugang zum Treppenhaus (zu den Cubes) ist vergittert. Bewegungsmelder und Kameras sichern diesen Bereich zusätzlich ab. Der Zugang zu den Fluren der Cubes erfolgt über Token, die zentral gemanagt werden. (Mitarbeiter der Terra Cloud haben einen Master-Key für Notfälle). Alle Türen innerhalb des Rechenzentrums geben Alarm, wenn sie länger als der erlaubte Zeitraum (wenige Sekunden) offenstehen. Dieser Zustand wird auf der Videowand überwacht. Die Serverräume haben keine Fenster oder Verbindung zur Außenhaut des Gebäudes. Der Zugang in alle Serverräume wird automatisch protokolliert. In der gesamten Terra Cloud finden mindestens zweimal täglich Kontrollgänge statt (hierbei wird auf mögliche Probleme und Veränderung geachtet).

Zutritt Cube 1, 3 & 4 (Hosting, Iaas & SaaS)
Zu Cube 1, 3 und 4 haben nur Mitarbeiter der Terra Cloud Zutritt. Zutritt über RFID & PIN. Die Zutritte werden protokolliert.

Zutritt Cube 2 (Housing, Hosting)

Zutritt über RFID & PIN. Die Zutritte werden protokolliert. Die einzelnen Serverschränke sind durch Käfige voneinander getrennt. Durch die Anmeldung werden die entsprechenden Käfigtüren freigeschaltet. Jeder Kunde hat nur Zugang zu seinem gemieteten Bereich.

Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

Alle internen Systeme sind an ein Active Directory angeschlossen. Zu den Hosting Systemen existiert kein administrativer und direkter Zugang. Der Administrations-Zugang wird indirekt über Jump Server hergestellt. Diese Zugänge sind besonders gesichert und haben besondere Anforderungen an die Passwörter: - min. 16 Zeichen - Bestehend aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen - Wechsel alle 7 Tage - Die Passwörter dürfen nicht aus Namen, Wörtern oder Tastaturmustern bestehen. Alle Systeme sind über redundante Internet Leitungen (die aus 2 Bundesländern zugeführt werden) mit der Außenwelt verbunden. Diese Verbindungen werden durch mehrere zentrale Firewall Systeme abgesichert. Die Regelwerke dieser Firewall werden in kurzen Abständen überarbeitet. Die Firewalls werden extern von einem professionellen Anbieter gepflegt und sowohl intern als auch extern überwacht. Hierdurch wird eine frühzeitige automatische Angriffserkennung gewährleistet. Alle Kundennetzte sind über VLAN voneinander getrennt. Jedes Kundennetz (im Bereich Housing optional) erhält zudem eine professionelle Firewall als persönliche Zugangskontrolle zur Selbstverwaltung.

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:
Es liegt ein anwenderbezogenes Berechtigungskonzept vor, dass im Active Directory umgesetzt wird. Die realisierte Berechtigungsstruktur bezieht sich auf das gesamte System des Unternehmens: Die Berechtigungen können auf Dateien, auf Datensätze, auf Anwendungsprogramme und das Betriebssystem differenziert werden und die Lese-, Änderungs- und Löschrechte einschränken. Es wird sichergestellt, dass jeder Benutzer nur auf die Daten zugreifen kann, zu denen er zugriffsberechtigt ist. Das Berechtigungskonzept, dass sich an den Stellungen der Mitarbeiter orientiert, ist schriftlich festgehalten (Dokumentation über das Active Directory). Verschiedene Zugriffsrechte werden durch vorgefertigte Benutzerprofile zusammengefasst. Weiterhin ist das Berechtigungskonzept programmtechnisch in der Anwendung, im Active Directory hinterlegt. Sämtliche Zugriffe der Benutzer werden protokolliert. Es gibt eine durchgängige physikalische Trennung zwischen Management (Administrator) System und Produktivnetz (Kundennetze). Bei den Management-Systemen wird sehr differenziert auf die Notwendigkeit des Zugriffs durch die Mitarbeiter geachtet. Jeder Zugriff eines Mitarbeiters wird protokolliert. Kundenpasswörter zum Zugriff auf die Verwaltungsoberflächen werden automatisch als kryptisches Passwort generiert und in einer eigenen Datenbank verschlüsselt abgelegt. Die Passwörter sind den Mitarbeitern der Terra Cloud unbekannt.

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Das Trennungsgebot wird zur Trennung von Cube 1, Cube 2 und dem Backup-System (extra Leitung) umgesetzt. Beim Cube 1 werden für jeden Kunden ein eigenes VLAN und eine eigene Firewall eingesetzt. Beim Cube 2 werden einzelne Schränke und einzelne Käfige installiert. Das Backup-System verfügt über eine eigene Versorgung und ist durch eine 256 Bit AES Verschlüsselung gesichert. Das verwendete Passwort kann durch Terra Cloud nicht zurückgesetzt oder ausgelesen werden.

Pseudonymisierung

Die zur Bereitstellung und Betrieb von Cloud Leistungen erhobenen Daten werden verschlüsselt abgespeichert. Aus diesem Datensatz wird ein kryptischer Wert (sogenannter Token) erzeugt mit dessen Hilfe eine weitere Verarbeitung wie z.B. Ausführung von Bestellungen oder Installationen möglich ist.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

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.
Die Kunden-Netze sind durch VLAN voneinander getrennt. Diese VLANs werden automatisch verwaltet. Eine Doppelvergabe ist nicht möglich. Auch werden die VLANs nur von speziell geschulten Mitarbeitern gepflegt. Die öffentlichen IP Adressen werden von speziell geschulten Mitarbeitern gepflegt und vergeben. Beim Cube 1 hat jeder Kunde sein eigenes VLAN. Die Pflege der Systeme wird durch einen Admin der Terra Cloud gewährleistet. Es existiert eine virtuelle Firewall vor jedem Kunden aus dem Bereichen

Hosting, IaaS und/oder SaaS. Auch kann der Kunde kostenpflichtig die Erstellung von regelmäßigen Backups hinzubuchen: Dabei werden physikalische Backups als verschlüsselter Stream erstellt und in anderen Brandabschnitt Bereichen oder auf Wunsch in einem Partner Rechenzentrum für den Kunden elektronisch zugänglich aufbewahrt. Die Verschlüsselung der Backup Datensätze ist obligatorisch und erfolgt kundenseitig. Diese Passwörter sind der Terra Cloud nicht bekannt und können auch nicht ausgelesen oder zurückgesetzt werden. Beim Cube 2 wird ebenfalls ein eigenes VLAN umgesetzt. Die Pflege des Systems liegt jedoch vollkommen in den Händen des Kunden (Colocation/ Housing Konzept). Damit liegen auch alle Sicherungsmaßnahmen in den Händen des Kunden. Für Cube 1 & 2 gibt es optional die Möglichkeit einen Schadsoftwareschutz für die Firewall zu buchen. Jedoch wird per Default keine End Point Protektion umgesetzt. Das Management Netz ist vom öffentlichen Netz abgekapselt. In diesem Netz sind alle USB-Geräte verboten und alle USB-Ports deaktiviert. Das indirekte Patchen erfolgt über WSUS. Zugriff auf die Systeme kann nur über den Jump Server erfolgen. Weiterhin ist ein zentraler Virenscanner im Einsatz. Beim Office System ist ein Virenschutz auf allen Rechnern, zentral in der Firewall, auf dem Mailserver und auf den internen Servern umgesetzt. Der gesamte Virenscanner und die gesamte Konfiguration werden zentral gepflegt.

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind. Alle Zugriffe auf die Management Systeme werden protokolliert. Alle Konfigurationsänderungen werden protokolliert und gespeichert. Zur Gewährleistung der Eingabekontrolle sind die vom Softwarehersteller mitgebrachen Log Mechanismen und Transaktionsprotokolle, zur Protokollierung aller Eingaben für alle Anwendungen, vorhanden. Zusätzlich werden Änderungen mittels eines ticketbasierenden Change Management Software System durchgeführt, protokoliert und archiviert.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
Für das interne Management und das interne Office werden Backups nach einem Backup-Plan durchgeführt. Darüber hinaus werden die Backups in georedundanter Form aufbewahrt. Für die beiden Cubes wird standardmäßig kein Backup vorgenommen. Die Stromversorgung zur Terra Cloud erfolgt über eine Ringeinspeisung. Diese ist dem Unternehmen vertraglich zugesichert. Das Unternehmen setzt eine redundante unterbrechungsfreie Stromversorgung (USV) ein, in der Blitz- und Überspannungseinrichtungen integriert sind. Die unterbrechungsfreie Stromversorgung wird automatisch einmal pro Quartal hinsichtlich ihrer Wirksamkeit getestet. Die USV kann das gesamte Rechenzentrum 20 Minuten mit Strom versorgen. Für die weitere Stromversorgung bei Stromausfall steht ein Notstromaggregat, versorgt über einen Dieseltank mit einem Volumen von fünf Tagen, zur Verfügung. Das Notstromaggregat wird hinsichtlich der Wirksamkeit einmal im Monat getestet. Die Verbindung zum Internet wird über zwei verschiedene, physikalisch getrennte Leitungen aus zwei verschiedenen Bundesländern realisiert. Die beiden Leitungen sind nicht gekreuzt. Die Kühlung der Serverräume wird bis zu 90 % des Jahres über eine Luftkühlung umgesetzt. Hierzu werden zwei Klimaanlagen redundant betrieben. Beide Anlagen sind verschaltet, somit stehen beide passiven Kühlflächen der Chiller zur Verfügung. Zum Schutz gegen Wasser sind Feuchtigkeits- und Leckage Sensoren im gesamten Gebäude verbaut. Auch verfügt das Unternehmen über Wasser-Auffangwannen an allen notwendigen Stellen und über Entwässerungs-Anlagen und Drainagen auf dem Grundstück. Weiterhin besteht in den Serverbereichen ein 60 cm hoher Doppelboden. Bei der Löschanlage handelt es sich um eine N2 Löschanlage mit Brandmeldeanlage und Brandfrüherkennung. Die Brandmeldeanlage verfügt über eine direkte Aufschaltung zur Feuerwehr. Auch gibt es spezielle Feuerlöscher vor Ort. Für den weiteren Brandschutz werden regelmäßige Begehungen durch die Feuerwehr durchgeführt. Auch führt die Feuerwehr regelmäßige Schulungen zu Löscheinsätzen im Rechenzentrum durch. Es wird ein zentrales Patch-Management mit physikalisch getrennter Testumgebung eingesetzt. Für das Patch-Management werden regelmäßige Notfallübungen und regelmäßige Wartungsintervalle aller Technik (protokolliert) umgesetzt.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management

Das Datenschutzmanagement wurde in die bestehenden Qualitätsicherungssysteme, sowie in das Changemanagement und Ticketing System integriert und orientiert sich an den in den Systemen bereits etablierten Berechtigungsstrukturen.

Incident-Response-Management

Innerhalb der TERRA CLOUD wurden zwei unabhängige Incident Systeme eingeführt. Die Teilung dient einer erhöhten Sicherheit. Das „externe" System wird ausschließlich für Kundenanfragen als Incident Plattform genutzt wird. Anfragen sind ausschließlich über diese Plattform zu stellen und werden innerhalb des Systems entsprechend verwaltet und archiviert. Telefonische Anfragen werden von den Mitarbeitern in eine schriftliche Anfrage verwandelt.
Für die internen Prozesse zur Qualitätssicherung, Installationsüberwachung und zum Zwecke des Change-Managements wird eine weitere, unabhängige „interne" Plattform betrieben. Zu diesem System haben nur autorisierte Mitarbeiter Zugriff.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Die zur Eingabe von Daten bestehenden Portale sind so konzipiert, dass ausschließlich Daten erhoben werden, die zur Ausführung der bestellten Leistung entweder für den Bestellprozess selbst, zur Installation oder zur Durchführung von Wartungsarbeiten benötigt werden. Auf eine Speicherung von Passwörtern für einen automatischen „Log In" wird verzichtet.

Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass die Verarbeitung personenbezogener Daten durch einen Dritten im Auftrag Ihres Unternehmens (Auftragsdatenverarbeitung) nur entsprechend den Weisungen des Auftraggebers erfolgt.
Zur Auftragskontrolle wird ein definierter Prozess verwendet, der insbesondere folgende Inhalte betrachtet: Aufträge werden nur nach einer vorherigen Überprüfung der Zulässigkeit bei Auftragsdatenverarbeitungen schriftlich getroffen. Zusätzliche Vereinbarungen bedürfen ebenfalls der Schriftform. Der Auftrag enthält eine klare Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber. Unterauftragsverhältnisse sind offen zu legen und entsprechend zu überprüfen.
Vor der Vergabe erfolgt eine Überprüfung der technisch- organisatorischen Maßnahmen des Auftragnehmers. Wenn erforderlich, werden zusätzliche Sicherheitsmaßnahmen definiert und umgesetzt. Zur Überwachung der ordnungsgemäßen Vertragsausführung erfolgt mindestens einmal im Jahr eine Kontrolle des Auftragnehmers. Diese kann auch durch einen entsprechenden Nachweis erbracht werden (z.B. TÜV Audit).