Rahmenbedingungen für Connected Services der Robert Aebi GmbH

Diese Rahmenbedingungen für die Bereitstellung von Connected Services der Robert Aebi GmbH legen die Bedingungen fest, gemäß derer die Connected Services dem Kunden erbracht werden (Teil I) und gemäß derer die Daten über die Baumaschine verarbeitet werden (Teil II).

Teil I. Allgemeine Geschäftsbedingungen für Connected Services

1. Geltungsbereich, Form

1.1. Diese Allgemeinen Geschäftsbedingungen für Connected Services (im Folgenden: **AGB Connected Services**) gelten für alle unsere Geschäftsbeziehungen mit unseren Kunden (im Folgenden: **Kunden**). Die AGB Connected Services gelten nur, wenn der Kunde Unternehmer (§ 14 BGB), eine juristische Person des öffentlichen Rechts oder ein öffentlich-rechtliches Sondervermögen ist.

1.2. Die AGB Connected Service gelten für Verträge über die Erbringung von Connected Services (im Folgenden: **Connected Services** oder **Services**). Sofern nichts anderes vereinbart, gelten die AGB Connected Services in der zum Zeitpunkt der Bestellung des Kunden gültigen bzw. jedenfalls in der ihm zuletzt in Textform mitgeteilten Fassung als Rahmenbedingungen auch für gleichartige künftige Verträge, ohne dass wir in jedem Einzelfall wieder auf sie hinweisen müssten.

1.3. Unsere AGB Connected Services gelten ausschließlich. Abweichende, entgegenstehende oder ergänzende Allgemeine Geschäftsbedingungen des Kunden werden nur dann und insoweit Vertragsbestandteil, als wir ihrer Geltung ausdrücklich zugestimmt haben. Dieses Zustimmungserfordernis gilt in jedem Fall, beispielsweise auch dann, wenn wir in Kenntnis der Allgemeinen Geschäftsbedingungen des Kunden die Leistung an ihn vorbehaltlos ausführen.

2. Vertragsschluss, Erfassung, Speicherung und Austausch der Daten

2.1. Unsere Angebote sind freibleibend und unverbindlich. Dies gilt auch, wenn wir dem Kunden Kataloge, technische Dokumentationen (z. B. Zeichnungen, Pläne, Berechnungen, Kalkulationen, Verweisungen auf DIN-Normen), sonstige Produktbeschreibungen oder Unterlagen - auch in elektronischer Form - überlassen haben, an denen wir uns Eigentums- und Urheberrechte vorbehalten.

2.2. Die Bestellung der Connected Services durch den Kunden gilt als verbindliches Vertragsangebot. Sofern sich aus der Bestellung nichts anderes ergibt, sind wir berechtigt, dieses Vertragsangebot innerhalb von 2 Wochen nach seinem Zugang bei uns anzunehmen.

2.3. Die Annahme kann entweder schriftlich (z. B. durch Auftragsbestätigung) oder durch Bereitstellung der Connected Services an den Kunden erklärt werden.

2.4. Zur Erbringung der Connected Services, können bestimmte Daten (wie in dieser Ziffer 2 nachfolgend beschrieben) erfasst, gespeichert und erhalten werden durch: (1) das Telematik-System, (2) die Diagnose-Tools, (3) den Co-Piloten und (4) durch uns, den Kunden oder Dritte.
Die betreffenden Daten beinhalten insbesondere Informationen zur Leistung der Baumaschinen, Daten zu Geopositionierung, Betriebsstunden, Geschwindigkeit, Kraftstofffüllstand, Kraftstoffverbrauch, Fehlercodes (Fehler) und Alarmmeldungen, baumaschinentypspezifische Informationen (Ladegewicht, Betriebs-/Standzeiten, Hardware-/Softwarekonfiguration, Arbeitsmodus etc.) sowie die Seriennummer und sonstige Identifikationsdaten. Einige Funktionen der Connected Services kombinieren gegebenenfalls Daten mehrerer Drittanbieter.

2.5. Das Telematik-System ist ein von den Lizenzgebern der Volvo CE entwickeltes auf Telematik basierendes System. Es besteht aus einem On-Board-Zugang (im Folgenden: **Telematik-Hardware**), einem Telekommunikationsnetzwerk und einem zentralen Backoffice-System sowie „Software-as-a-Service“ (SaaS)-Lösungen, welche von uns angeboten und von den Unternehmen der Volvo Group als Drittanbieter genutzt werden. Zu diesen Systemen haben die Kunden über das entsprechende Internetportal (im Folgenden: **Schnittstelle**) Zugang oder können diese anderweitig erhalten. Die Telematik-Hardware ist entweder ein Bestandteil der Baumaschine oder wird vom Kunden separat erworben. Sie erfasst, verarbeitet, überwacht, analysiert und sendet interaktiv bestimmte Daten über das Kommunikationsnetzwerk von der Baumaschine an den Händler, um die Daten weiterzuverarbeiten. Die Telematik-Hardware kommuniziert mit (einer) bestimmten Generation(en) von Telekommunikationsnetzwerken. Sollte(n) die entsprechende(n) Generation(en) von Telekommunikationsnetzwerken dem Kunden nicht mehr zur Verfügung stehen, ist der Kunde für die Aktualisierung der Telematik-Hardware verantwortlich, um die Connected Services weiterhin nutzen zu können. Der Kunde trägt die Kosten für die entsprechenden Aktualisierungen.

2.6. Wir können bestimmte Daten auch durch den Einsatz von Diagnosewerkzeugen (z. B. TechTool, MATRIS) erhalten, wenn wir uns mit der Baumaschine verbinden.

2.7. Wir können bestimmte Daten auch durch den Einsatz des Co-Pilots erhalten, wenn wir uns mit der Baumaschine verbinden. Der Co-Pilot ist ein von Lizenzgebern von Volvo CE entwickeltes System. Es besteht aus einem Computer mit Touchscreen, mobiler Konnektivität und sonstigen Bauteilen (**„Co-Pilot-Hardware“**) vom Händler angebotenen und durch Drittanbieter betriebene Software-as-a-Service (SaaS)-Lösungen, auf die der Kunde über die Schnittstelle oder anderweitig zugreifen kann.

2.8. Bestimmte Daten können auch von uns, dem Kunden oder von Dritten bereitgestellt werden.

2.9. Der Betrieb des Telematik-Systems, der Diagnosewerkzeuge und des Co-Piloten sowie die Bereitstellung der Connected Services beinhalten die Datenübermittlung an Unternehmen der Volvo Group und an Drittanbieter von Services, insbesondere andere Händler und Werkstätten sowie IT-Lieferanten, die von den Unternehmen der Volvo Group beauftragt sind. Dies erfolgt zum Zwecke der Erbringung der Connected Services sowie neuer Services und für andere Zwecke, beispielsweise zur Überwachung kritischer Bauteile und Fehlercodes für proaktive Wartung. Weitere Informationen diesbezüglich befinden sich in den Handbüchern der Baumaschinen, den Servicebeschreibungen und den zusätzlichen Bedingungen für die Connected Services.

2.10. Der Kunde ist Inhaber der Rechte und Rechtsansprüche in Bezug auf die hierin beschriebenen und die in Ziffer 2.4 Bezug genommenen Daten (im Folgenden: **Baumaschinendaten**). Der Kunde räumt uns und der Volvo CE hiermit ein weltweites kosten- und gebührenfreies, übertragbares, abtretbares, unterlizenzierbares, unbefristetes und unwiderrufliches Nutzungsrecht ein, um Baumaschinendaten zu erfassen, zu analysieren, zu nutzen, zu modifizieren oder anderweitige Kontrolle über die Baumaschinendaten auszuüben einschließlich dem Recht, die Baumaschinendaten mit entsprechenden verbundenen Unternehmen und sonstigen, durch uns oder Volvo CE autorisierten Personen zu teilen. Dies dient der Weiterentwicklung der angebotenen Connected Services sowie der Verbesserung der Volvo-Produkte.

3. Umfang der Connected Services

3.1. Der Umfang der vertragsgemäßen Connected Services umfasst diejenigen Connected Services, für die sich der Kunde gemäß der Schnittstelle oder etwaig anderen Verfahren registriert hat. Eine vollständige Produktbeschreibung (technische Spezifikation) der Connected Services ist in den Schnittstellen für die vom Kunden gewählten Services aufgeführt oder bei uns erhältlich. Soweit die Connected Services einschließlich der Nutzung ihrer Schnittstellen die Geltung zusätzlicher Bedingungen nach sich ziehen, so finden diese zusätzlichen Bedingungen jeweils Anwendung. Die aktuelle Version dieser AGB Connected Services ist unter www.robert-aebi.de abrufbar oder bei uns erhältlich.

3.2. Es ist den Connected Services immanent, dass wir oder Drittanbieter von Services (insbesondere Werkstätten, die von den Unternehmen der Volvo Group für diese Zwecke beauftragt sind) Kundeninformationen über die Instandhaltungs-, Reparatur- und Wartungsergebnisse sowie Leistungsergebnisse der Baumaschinen des Kunden erhalten.

4. Verfügbarkeit des Telematik-Systems und des Co-Piloten

4.1. Die Nutzung des Telematik-Systems und/oder des Co-Piloten unterliegt der technischen Verfügbarkeit gemäß der technischen Spezifikation.

4.2. Die Verfügbarkeit hängt u.a. von der Verfügbarkeit des Netzwerks, der Generation des verfügbaren Telekommunikationsnetzwerks und der Satellitenabdeckung ab und kann durch lokale Hindernisse (z. B. Brücken, Gebäude etc.), atmosphärische oder topografische Bedingungen und technische Einschränkungen gestört werden.

4.3. Wir übernehmen keine Gewährleistung und/oder Garantie für die Sicherheit der mobilen und schnurlosen Netzwerkkommunikation, die für die Übertragung der Daten und Informationen genutzt werden.

4.4. Das Telematik-System und/oder der Co-Pilot können aufgrund von Wartungsarbeiten oder der Fehlerbehebung an technischen Komponenten des Systems nicht verfügbar sein. Geplante Wartungsarbeiten werden, falls möglich, dem Kunden auf der Schnittstelle des Services oder anderweitig mitgeteilt. Die vom Kunden zu entrichtende Gebühr für den jeweiligen Service ist nachträglich zu reduzieren, wenn der Umfang der Connected Services während des festgelegten Zeitraums, für den der Kunde für den jeweiligen Service Vorauszahlungen geleistet hat, wesentlich reduziert ist. Die Reduzierung erfolgt in diesen Fällen in Relation zur verringerten Nutzung des betreffenden Services während der verbleibenden Zeit.

4.5. Der Online-Zugriff ist üblicherweise auf einen bestimmten Zeitraum beschränkt, der auf der Service-Schnittstelle für den bestimmten Service festgelegt ist. Der Kunde ist allein dafür verantwortlich, dass er über die erforderliche technische Ausrüstung verfügt, um auf die Connected Services zuzugreifen, z.B. die IT-Ausstattung und den Online-Zugang.

5. Nutzung des Telematik-Systems und/oder des Co-Piloten

5.1. Die Nutzung von Telematik-System und/oder den Co-Piloten steht unter dem Vorbehalt der Einhaltung der spezifischen Bedingungen der jeweiligen Services und der Einhaltung aller Bestimmungen dieser AGB Connected Services und etwaig weiterer vertraglicher Bestimmungen durch den Kunden und der technischen Verfügbarkeit von Telematik-System und/oder des Co-Piloten.

5.2. Mit Zustandekommen des Vertrages stellen wir dem Kunden die Login-Informationen bereit, damit der Kunde Zugang zu den Schnittstellen hat, seine Baumaschine bei den Schnittstellen anmelden/deren Bedingungen akzeptieren und mit der Nutzung der abonnierten Connected Services beginnen kann. Der Kunde sorgt jederzeit für die Sicherheit von Telematik-System und/oder Co-Pilot durch die sichere und geschützte Aufbewahrung der Zugangs- und Anmeldedaten.

5.3. Der Kunde ist für die Einhaltung der Benutzerrichtlinien und Bedienungsanleitungen der Baumaschine verantwortlich und stellt diese sicher.

5.4. Das Telematik-System und/oder der Co-Pilot ist nicht in allen Ländern / Gebieten verfügbar. Informationen zu den Ländern / Gebieten, in denen die Nutzung des Telematik-Systems und/oder des Co-Piloten und/oder der Connected Services nicht verfügbar sind, sind bei uns zu erfragen.

Der Kunde erhält die Connected Services nur für diejenigen Baumaschinen, für die er die notwendige Hardware für das Telematik-System und/oder den Co-Piloten erworben und sich für die Connected Services registriert hat. Dies beinhaltet alle notwendigen Aktualisierungen aufgrund veralteter Generationen / einer veralteten Generation des Telekommunikationsnetzwerks.

5.5. Das Telematik-System und der Co-Pilot sind urheberrechtlich geschützt und die Volvo Group erhebt Anspruch auf alle ausschließlichen Rechte diesbezüglich. Dies gilt vorbehaltlich der Einräumung von Nutzungsrechten an den Kunden gemäß den Regelungen dieser AGB Connected Services und der Einhaltung derselben durch den Kunden. Alle Urheberrechte und sonstigen Eigentumsrechte an den gewerblichen Schutzrechten an dem Telematik-System, der Telematik-Hardware, dem Co-Piloten und der Co-Piloten-Hardware bleiben vorbehalten. Der Kunde erwirbt keine Eigentumsrechte betreffend die gewerblichen Schutzrechte an dem Telematik-System, der Telematik-Hardware, dem Co-Piloten und/oder der Co-Pilot-Hardware.

5.6. Der Kunde wird die durch die Connected Services, den Co-Piloten oder das Telematik-System bereitgestellten Informationen oder Inhalte nicht verbreiten, rückübertragen, vervielfältigen, veröffentlichen, modifizieren, weiterentwickeln, nachkonstruieren oder anderweitig verändern, soweit zwingende gesetzliche Vorschriften dem nicht entgegenstehen.

5.7. Der Kunde darf die Nutzung der Connected Services ohne unsere Erlaubnis nicht einem Dritten gewähren.

5.8. Wir behalten uns das Recht vor, Detailinformationen des bzw. der Computer oder sonstiger Geräte, mit denen der Kunde die Schnittstelle nutzt, per Fernzugriff aufzuzeichnen. Dies erfolgt vor allem zur Verhütung von Datenpiraterie und um die Kunden über alle wichtigen Updates für die Schnittstelle und bezüglich anderer Produkte von uns, die mit den Connected Services und der Nutzung der Schnittstelle in Zusammenhang stehen, zu informieren. Wir bewahren derlei gesammelte Daten in Übereinstimmung mit den anwendbaren Gesetzen auf.

5.9. Wir kommen jederzeit Anfragen öffentlicher Stellen zur Offenlegung von Daten nach, einschließlich auf Basis oder im Rahmen der unter dem Vertrag verarbeiteten Daten, wenn wir hierzu gesetzlich verpflichtet ist.

5.10. Der Kunde ist verantwortlich für die Bereitstellung korrekter Informationen, die für alle Registrierungen, Abmeldungen oder sonstigen Vorgänge im Zusammenhang mit den Connected Services und/oder des Co-Piloten für die jeweilige Baumaschine erforderlich sind. Insbesondere muss der Kunde:

(i) alle erforderlichen Maßnahmen zur Erfassung, Verarbeitung und Nutzung der Daten im Zusammenhang mit den Connected Services ergreifen;

(ii) uns informieren, falls der Kunde nicht länger Eigentümer der entsprechenden Baumaschine ist oder sie ihm nicht mehr zur Verfügung steht.

(iii) sicherstellen, dass seine Passwörter und Zugangsinformationen zur Nutzung der Connected Services nur berechtigten Nutzern zur Verfügung stehen.
(iv) sicherstellen, dass die Nutzer der Baumaschine und der Services vollständig über die Anweisungen zur Nutzung der Connected Services informiert sind und diese einhalten.
(v) sicherstellen, dass der Kunde und die Nutzer der Baumaschine das Telematik-System und/oder den Co-Piloten nicht unter Verletzung von Gesetzen oder für rechtswidrige oder missbräuchliche Zwecke nutzen.

5.11. Der Kunde sichert zu, dass er während der gesamten Laufzeit des Vertrags jederzeit über alle notwendigen Einwilligungen, Genehmigungen, Rechte und Berechtigungen verfügt, um sicherzustellen, dass der Kunde das Telematik-System, den Co-Piloten und die Schnittstelle in voller Übereinstimmung mit allen geltenden Gesetzen und Vorschriften, einschließlich der datenschutzrechtlichen Bestimmungen, nutzt. Der Kunde stellt uns und Volvo CE von allen Ansprüchen, Verlusten, jeglicher Haftung, Schäden, Gebühren, Aufwendungen und Kosten (einschließlich angemessener Anwaltshonorare) frei, die sich daraus ergeben, dass der Kunde sich nicht an geltende Gesetze und Vorschriften gehalten hat.

5.12. Wir dürfen die Erbringung der Connected Services verweigern oder das Telematik-System zur Ortung einer registrierten Baumaschine nutzen, wenn wir vernünftigerweise annehmen durften, dass die Baumaschine nicht vom Kunden als rechtmäßigen Eigentümer betrieben wird oder der Kunde geltende Gesetze oder Regelungen des Vertrags bzw. dieser AGB Connected Services nicht einhält.

5.13. Sofern und soweit personenbezogene Daten betroffen sind, gilt Abschnitt II der Rahmenbedingungen.

6. Besondere Bedingungen für die Connected Services

6.1. Individuelle Connected Services können besonderen Bedingungen unterliegen, die sodann ergänzend Anwendung finden. Bei Abschluss des Abonnements für die entsprechenden individuellen Connected Services gelten die entsprechenden besonderen Bedingungen (in ihrer jeweils gültigen Fassung, wie in den entsprechenden besonderen Bedingungen dargelegt). Im Falle eines Widerspruchs zwischen den jeweiligen besonderen Bedingungen und diesen AGB Connected Services haben die besonderen Bedingungen in Bezug auf die individuellen Services Vorrang.

6.2. Die Connected Services können Daten oder Services beinhalten, die wir oder die Volvo CE unter Einräumung entsprechender Nutzungsrechte von Drittparteien erhalten. Es gelten daher die Nutzungsbedingungen der jeweiligen Drittparteien.

7. Preise und Zahlungsmodalitäten

7.1. Der Kunde zahlt die Abonnementsgebühren für die Connected Services gemäß Bestellung oder die ggf. in den besonderen Bedingungen der Services festgelegt sind.

7.2. Sofern nicht anderweitig ausdrücklich geregelt, verstehen sich alle Preise netto (ohne Mehrwertsteuer und sonstige geltende Verkaufssteuern, Entgelte, Gebühren oder Abgaben, die auf die entsprechenden Beträge aufgeschlagen werden).

7.3. Alle gemäß Vertrag vom Kunden zu leistenden Zahlungen erfolgen in vollem Umfang ohne Abzug. Eine Aufrechnung ist nur mit unbestrittenen oder rechtskräftigen Forderungen möglich. Ein Zurückbehaltungsrecht besteht nicht.

7.4. Gerät der Kunde mit der Zahlung in Verzug, ist der Betrag unbeschadet unserer sonstigen Rechte ab dem Fälligkeitsdatum bis zur vollständigen Zahlung mit dem gesetzlichen Verzugszins zu verzinsen.

7.5. Wir dürfen eine Drittpartei damit beauftragen, in unserem Namen die Rechnung zu stellen und die Zahlungen einzuziehen.

7.6. Soweit nichts anderes vereinbart wurde, beinhalten alle Connected Services alle entsprechenden Telekommunikationsabonnements zur Übermittlung der Daten an die und von der Baumaschine.

8. Besondere Bedingungen für im Voraus bezahlte Abonnements

8.1. Für Connected Services, für die eine Vorauszahlung für einen festen Zeitraum vereinbart wurde, gelten die folgenden Bedingungen:

Der Abonnementzeitraum beginnt ab Registrierung der Baumaschine bei uns. Gebühren, die sich auf andere Services oder eine andere Nutzung als die von den Abonnementsgebühren abgedeckten Gebühren beziehen (z. B. zusätzliche

Services) werden dem Kunden gemäß der geltenden Preisliste belastet und in Rechnung gestellt. Während des Zeitraums der Vorauszahlung erhält der Kunde keine Rückerstattung, falls er die Services kündigt.

9. Haftung

9.1. Wir haften – unberührt von den nachfolgenden Bestimmungen dieses Abschnitts – stets unbeschränkt für vorsätzlich oder grob fahrlässig verursachte Schäden, für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit und soweit wir nach dem Produkthaftungsgesetz zur Haftung verpflichtet sind.

9.2. In Fällen einfacher Fahrlässigkeit haften wir dem Kunden gegenüber nur, soweit wir eine wesentliche Vertragspflicht, mithin eine Pflicht deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Kunde als Vertragspartner regelmäßig vertraut und vertrauen darf, verletzt haben. In diesen Fällen ist die Haftung auf den Ersatz des vorhersehbaren, typischerweise eintretenden Schadens beschränkt.

9.3. Die verschuldensunabhängige Haftung auf Schadensersatz (§ 536a Abs. 1 Satz 1 Alt. 1 BGB) für bei Vertragsschluss vorhandene Mängel ist ausgeschlossen.

10. Gewährleistung

10.1. Die Gewährleistung für die Telematik-Hardware und/oder Co-Piloten-Hardware, die durch den Kunden separat gekauft werden, richten sich ausschließlich nach den für den jeweiligen Kaufvertrag zugrundeliegenden vertraglichen Regelungen.

10.2. Im Falle von dienstvertraglichen Leistungen gewährleisten wir, dass diese mit angemessener Sorgfalt und sachgerecht durchgeführt werden. Für die Verletzung dieser Pflicht haften wir im Rahmen der Haftungsregelung gemäß Ziffer 9. Jegliche weitere Gewährleistung ist aufgrund der Rechtsnatur von Dienstleistungen ausgeschlossen.

10.3. Im Falle von mietvertraglichen Leistungen gelten grundsätzlich die gesetzlichen Regelungen zur Gewährleistung in Mietverträgen. Wir gewährleisten nur, dass die Connected Services während der vertraglichen Laufzeit der technischen Spezifikation entsprechen. Wir werden etwaige Mängel innerhalb einer angemessenen Frist beheben. Die Anwendung des § 536a Abs. 2 BGB (Selbstvornahmerecht) ist jedoch ausgeschlossen. Der Kunde zeigt uns auftretende Mängel unverzüglich schriftlich mit Beschreibung des Auftretens des Mangels und der näheren Umstände an. Der Kunde unterstützt uns bei der Beseitigung der Mängel unentgeltlich und stellt insbesondere alle notwendigen Unterlagen, Daten etc. zur Verfügung, die wir zur Analyse und Beseitigung des Mangels benötigen.

11. Deaktivierung der Telematik-Systemeinheit

Wir können die Telematik-Systemeinheit auf Ersuchen und Kosten des Kunden deaktivieren. Die vom Kunden gewünschte Deaktivierung muss durch uns oder durch eine andere von Volvo autorisierte Person erfolgen.

Sobald das Telematik-System deaktiviert ist, können die Daten nicht wiedererlangt werden und bestimmte Services können nicht verfügbar sein. Die Reaktivierung kann durch uns oder eine andere, von Volvo autorisierte Person auf Verlangen und Kosten des Kunden erfolgen.

12. Laufzeit und Kündigung

12.1. Die Laufzeit der Nutzung der Connected Services ergibt sich aus der Bestellung des Kunden. Sofern der Vertrag auf unbestimmte Zeit geschlossen wurde, kann dieser von uns oder vom Kunden jederzeit durch eine schriftliche Kündigung unter Einhaltung einer Frist von 60 Tage gekündigt werden.

12.2. Mit der Beendigung des Vertrages enden automatisch alle Abonnements für Connected Services aus dem Vertrag, ohne dass für die Connected Services bereits gezahlte Beträge erstattet werden.

12.3. Der Kunde kann bestimmte Services innerhalb der in Ziffer 12.1 genannten Frist (sofern nichts anderes bestimmt ist) kündigen, indem er uns mitteilt, die Registrierung des Kunden und der Maschine diesbezüglich rückgängig zu machen. Die Kündigung einzelner Services wirkt sich nicht auf das Fortbestehen des Vertrages insgesamt aus.

12.4. Die Parteien können den Vertrag schriftlich außerordentlich aus wichtigem Grund insbesondere dann kündigen, wenn die andere Partei eine wesentliche Vertragspflicht verletzt wird. Die außerordentliche Kündigung aus weiteren wichtigen Gründen bleibt unberührt. Im Falle der Verletzung einer wesentlichen Vertragspflicht ist die außerordentliche Kündigung erst nach dem erfolglosen Ablauf einer zur Abhilfe bestimmten Frist oder nach erfolgloser Abmahnung möglich. Die Fristsetzung und die Abmahnung sind entbehrlich, wenn der Schuldner die Leistung ernsthaft

und endgültig verweigert oder besondere Umstände vorliegen, die unter Abwägung der beiderseitigen Interessen die sofortige Kündigung rechtfertigen.

12.5. Ist der Kunde mit fälligen Beträgen in Höhe von zwei aufeinander folgenden Monatsbeträgen oder mit Teilbeträgen mindestens in Höhe von zwei Monatsbeträgen länger als vierzehn (14) Tage in Verzug ist, so stellt dies eine wesentliche Vertragsverletzung dar, die uns berechtigt, den Vertrag außerordentlich zu kündigen und/oder den betreffenden Service mit sofortiger Wirkung einzustellen. Ziffer 12.4, Satz 3 und 4 gelten entsprechend.

12.6. Wir sind berechtigt, den Vertrag und/oder einen bestimmten Service außerordentlich zu kündigen, wenn der Kunde sich nicht an die anwendbaren Datenschutzgesetze hält (Ziffer 12.4, Satz 3 und 4 gelten entsprechend) oder das Eigentum der Baumaschine auf Dritte überträgt. Wird die Maschine auf einen nachfolgenden Eigentümer / Nutzer übertragen, bleibt der Kunde für die Connected Services haftbar, einschließlich der Gebühren, Beträge, Abgaben, die entstanden sind, bis die Connected Services gekündigt werden oder der Käufer/Nutzer neue Connected Services bestellt. Das Recht des Kunden, das Eigentum an der Baumaschine zu übertragen, bleibt unberührt.

12.7. Wenn der Vertrag endet oder gekündigt wird, behalten wir uns das Recht vor, das Kundenprofil auf der Schnittstelle zu deaktivieren.

12.8. Die Beendigung des Vertrages gleich aus welchem Grund erfolgt unbeschadet von Rechten und Pflichten, die vor der Beendigung entstanden sind. Bestimmungen des Vertrages oder dieser AGB Connected Services, die ihrer Natur nach über die Beendigung des Vertrages hinaus ihre Gültigkeit behalten, bleiben ungeachtet der Beendigung in Kraft.

12.9. Bei Beendigung des Vertrags gleich aus welchem Grund hat der Kunde keinen Anspruch auf Erstattung der unter diesem Vertrag gezahlten Beträge. Die Beendigung dieses Vertrages erfolgt unbeschadet aller Ansprüche, die wir gegenüber dem Kunden bezüglich aller Beträge haben, die aus diesem Vertrag entstanden sind.

13. Höhere Gewalt

Solange wir durch ein unvorhergesehenes Ereignis, das wir auch bei Beachtung zumutbarer Sorgfalt nicht abwenden können, insbesondere bei Ereignissen wie Naturkatastrophen, Bränden/Explosionen, behördlichen Eingreifen, gesetzlichen Verboten, Pandemien/Epidemien, Quarantäneanordnungen, gesetzlichen Notständen oder sonstigen Fällen höherer Gewalt, an der Leistungserbringung ganz oder teilweise gehindert ist, gelten die Leistungsfristen um die Dauer der Behinderung als verlängert. Für die Dauer der Behinderung liegt keine Pflichtverletzung vor. Wir zeigen dem Kunden derartige Behinderungen und ihre voraussichtliche Dauer unverzüglich an. Dauert die höhere Gewalt ununterbrochen länger als zwei Monate oder wird uns die Leistungserbringung in den Fällen der höheren Gewalt unmöglich oder teilweise unmöglich, werden wir von den jeweils geschuldeten Leistungspflichten frei.

14. Sonstiges

14.1. Der Kunde kann seine Rechte und Pflichten aus dem Vertrag, den AGB Connected Services oder den besonderen Bedingungen und Bestimmungen für die Services nur nach unserer vorherigen schriftlichen Zustimmung vollständig oder teilweise abtreten oder übertragen.

14.2. Wir sind berechtigt, den Vertrag jederzeit auf eine Gesellschaft der Volvo Group zu übertragen. Der Kunde genehmigt eine solche Vertragsübernahme und wird uns aus dem Vertrag entlassen, ohne weitere Ansprüche zu stellen.

14.3. Die für die Erfüllung unserer Verpflichtungen bestimmten Termine sind keine Fixtermine.

14.4. Sollte eine Bestimmung dieser AGB Connected Services unwirksam sein oder werden, bleibt die Rechtswirksamkeit der übrigen Bestimmungen hiervon unberührt. Die Parteien sind im Falle einer unwirksamen Bestimmung dieser AGB Connected Services verpflichtet, über eine wirksame und zumutbare Ersatzregelung zu verhandeln, die dem von der unwirksamen Bestimmung verfolgten wirtschaftlichen Zweck möglichst nahekommt; das Gleiche gilt im Falle einer Lücke.

14.5. Wir behalten uns das Recht vor, diese AGB Connected Services jederzeit zu ändern. Der Kunde wird sechs Wochen vor Inkrafttreten der Änderungen schriftlich über die Änderungen informiert. Im Rahmen dieser Information werden dem Kunden die neuen AGB Connected Services mitgeteilt. Er ist berechtigt, der Geltung der neuen AGB Connected Services innerhalb von vier Wochen nach Zugang dieser Mitteilung zu widersprechen. Unterlässt der Kunde einen Widerspruch, werden die geänderten AGB Connected Services nach Ablauf der sechswöchigen Frist Vertragsbestandteil. Auf diese Frist werden wir den Kunden im Rahmen der Änderungsmitteilung ausdrücklich hinweisen.

14.6. Ausgeschlossen vom Recht zur Änderung dieser AGB Connected Services nach vorstehender Ziffer 14.5 sind Regelungen, welche die Hauptleistungspflichten der Vertragsparteien betreffen und die somit das Verhältnis zwischen Haupt- und Gegenleistungspflichten maßgeblich verändern, sowie sonstige grundlegende Änderungen der vertraglichen Pflichten, die dem Abschluss eines neuen Vertrags gleichkommen. Für solche Änderungen ist eine ausdrückliche vertragliche Vereinbarung erforderlich.

14.7. Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des internationalen Privatrechts und unter Ausschluss des UN-Kaufrechts, sofern und soweit kein anderweitiges Recht zwingend gilt.

14.8. Ist der Kunde Kaufmann i. S. d. Handelsgesetzbuchs, juristische Person des öffentlichen Rechts oder ein öffentlich-rechtliches Sondervermögen, ist ausschließlicher - auch internationaler - Gerichtsstand für alle sich aus dem Vertragsverhältnis unmittelbar oder mittelbar ergebenden Streitigkeiten der Geschäftssitz des Händlers in 88480 Achstetten. Entsprechendes gilt, wenn der Kunde Unternehmer i. S. v § 14 BGB ist. Der Händler ist jedoch in allen Fällen auch berechtigt, Klage am Erfüllungsort einer Lieferverpflichtung gemäß diesem Vertrag bzw. einer vorrangigen Individualabrede oder am allgemeinen Gerichtsstand des Käufers zu erheben.

Teil II. Vertrag über die Auftragsverarbeitung personenbezogener Daten für Connected Services

1. Gegenstand und Details

1.1. Gemäß diesem Vertrag über die Auftragsverarbeitung personenbezogener Daten (im Folgenden „**AVV**“) verarbeiten wir personenbezogene Daten im Auftrag des Kunden. Wir sind der Auftragsverarbeiter der in Ziffer 2 dieses AVV aufgeführten Arten von personenbezogenen Daten, die sich auf die Kategorien von betroffenen Personen beziehen. Der Kunde trägt die volle Verantwortung für die personenbezogenen Daten inklusive der Tatsache, dass die entsprechenden Daten keine Rechte Dritter und geltendes Recht in sonstiger Weise verletzen. Daher muss der Kunde sicherstellen, dass alle personenbezogenen Daten des Kunden, die im Telematik-System und/oder im Co-Piloten gespeichert sind, gesetzeskonform gespeichert und genutzt werden. Wir dürfen im Auftrag des Kunden die in Ziffer 2 zu diesem AVV genannten personenbezogenen Daten nur für Zwecke, die für die ordnungsgemäße Erfüllung des Hauptvertrags notwendig sind und nur gemäß den dokumentierten Anweisungen des Kunden verarbeiten. Ungeachtet des Vorstehenden haben wir und die Volvo CE als Unterauftragsverarbeiter das Recht, Daten (sowohl personenbezogene Daten als auch anderweitige Daten) von Baumaschinen und den Connected Services für eigene Zwecke zu nutzen und zu verarbeiten. Soweit die entsprechende Verarbeitung personenbezogene Daten beinhaltet, gelten wir bzw. die Volvo CE jeweils entsprechend als „Verantwortlicher“. Falls gewünscht, stimmt der Kunde zu, uns und/oder die Volvo CE bei der Bereitstellung von Informationen oder der Erlangung von Einwilligungen von betroffenen Personen in Bezug auf die Verarbeitungsaktivitäten durch uns und/oder die Volvo CE als Verantwortlicher zu unterstützen. Über den Vertragszweck hinaus, der die Erbringung automatisierter Services beinhaltet, sind einzelne Anweisungen des Kunden nur in Ausnahmefällen und nur gemäß den Bedingungen des Hauptvertrags (einschließlich diesem AVV) zulässig. Berichtigungen, Löschungen und Sperrungen personenbezogener Daten dürfen aus diesem Grund vom Kunden nur über seinen Onlinezugang erfolgen; wir nehmen keine Berichtigungen, Löschungen oder Sperrungen personenbezogener Daten vor. Im Falle technischer Probleme kann sich der Kunde an den Händler-Support wenden (welcher ggf. durch unsere Unterauftragnehmer erbracht wird).

1.2. Dieser AVV gilt als schriftlicher Datenverarbeitungsvertrag zwischen dem Kunden und uns gemäß den geltenden Gesetzen für personenbezogenen Daten und ist als solcher auszulegen.

1.3. Bei der Verarbeitung personenbezogener Daten sind wir verpflichtet, die für den Schutz personenbezogener Daten geltenden Bestimmungen einzuhalten und alle technischen, sicherheitsrelevanten und organisatorischen Maßnahmen zu ergreifen, die durch die entsprechenden geltenden Gesetze zum Schutz personenbezogener Daten vorgeschrieben sind. Dies beinhaltet die Maßnahmen, die in Teil III. festgelegt sind.

1.4. Der Kunde ermächtigt uns Unterauftragsverarbeiter einzusetzen. Alle Unterauftragsverarbeiter müssen die entsprechenden Anforderungen dieses AVV einhalten. Beim Einsatz von Unterauftragsverarbeitern werden wir sicherstellen, dass alle Rechte, die der Kunde uns gegenüber gemäß diesem AVV in Bezug auf die Auftragsverarbeitung von Daten hat, dem Kunden - über uns - auch gegenüber den Unterauftragsverarbeitern gewährt werden. Wir werden den Kunden in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragsverarbeitern informieren. Dem Kunden steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potentiellen Unterauftragsverarbeiters zu erheben. Ein Einspruch darf vom Kunden nur aus wichtigem, uns nachzuweisenden Grund erhoben werden. Soweit der Kunde nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Kunde Einspruch, sind wir berechtigt, den Hauptvertrag und den AVV mit einer Frist von 60 Tagen zu kündigen.

1.5. Sofern und in dem Maße, in dem wir Unterauftragsverarbeiter einsetzen, einschließlich des Umstandes, dass die entsprechenden Unterauftragsverarbeiter wiederum Unterauftragsverarbeiter einsetzen und dies die Verarbeitung personenbezogener Daten im Namen des Kunden zur Folge hat, erteilt der Kunde uns hiermit die Vollmacht,

(a) mit allen Unterauftragsverarbeitern einen schriftlichen Unterauftragsverarbeiter-Vertrag, Datentransfer-Vertrag (einschließlich der entsprechenden durch die EU-Kommission verabschiedeten EU-Standardvertragsklauseln, im Sinne derer der Kunde als Datenexporteur und wir oder der Unterauftragsverarbeiter (je nachdem, was zutrifft) als Datenimporteur gelten) bzw. sonstige gesetzlich vorgeschriebene Verträge zur Verarbeitung personenbezogener Daten einzugehen; und

(b) allen entsprechenden Unterauftragsverarbeitern zu erlauben, mit allen nachfolgenden Unterauftragsverarbeitern einen schriftlichen Unterauftragsverarbeiter-Vertrag, Datentransfer-Vertrag (einschließlich der entsprechenden durch die EU-Kommission verabschiedeten EU-Standardvertragsklauseln, im Sinne derer der Kunde als Datenexporteur und wir oder der Unterauftragsverarbeiter (je nachdem, was zutrifft) als Datenimporteur gelten) bzw. sonstige gesetzlich vorgeschriebene Verträge zur Verarbeitung personenbezogener Daten einzugehen.

1.6. Wir dürfen personenbezogene Daten in ein anderes Land oder andere Länder übermitteln (vorsorglich wird angemerkt, dass dies auch die Gewährung auf Zugriff auf die personenbezogenen Daten beinhaltet). Die Parteien ergreifen gemeinsam alle angemessenen und erforderlichen Maßnahmen, die notwendig sind um sicherzustellen, dass die Übermittlung gemäß geltendem Recht erfolgt. Dies beinhaltet, dass ein entsprechender Vertrag unter Einbeziehung der EU-Standardvertragsklauseln für die Datenübermittlung in Länder außerhalb des Europäischen Wirtschaftsraums (EWR) abgeschlossen wird.

1.7. Falls und in dem Maße, in dem eine andere Rechtsperson als der Kunde Verantwortlicher für alle oder einen Teil der personenbezogenen Daten ist, die durch uns im Auftrag des Kunden gemäß diesem AVV verarbeitet werden, bestätigt der Kunde, dass er über die notwendige Befugnis und Vollmacht verfügt, um diesen Datenverarbeitungsvertrag im Auftrag der entsprechenden Rechtsperson abzuschließen.

1.8. Wir verpflichten uns, sicherzustellen, dass derjenige Personenkreis, der berechtigt ist, Zugang zu den personenbezogenen Daten zu haben, die personenbezogenen Daten gemäß den Anweisungen des Kunden verarbeitet, und dass - im Hinblick auf die Verarbeitung personenbezogener Daten - sich dieser Personenkreis zur Geheimhaltung verpflichtet hat.

1.9. Wir werden den Kunden mit technischen und organisatorischen Maßnahmen im Rahmen des Zumutbaren dabei unterstützen, der Pflicht des Kunden zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte der betroffenen Personen nachzukommen.

1.10. Unter Berücksichtigung der Art der Verarbeitung und der für uns zugängigen Informationen unterstützen wir den Kunden bei der Einhaltung der datenschutzrechtlichen Bestimmungen bezüglich der Sicherheit der Verarbeitung, der Meldung einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde, der Mitteilung einer Verletzung des Schutzes personenbezogener Daten an die betroffenen Personen, der Datenschutz-Folgenabschätzung und einer vorherigen Konsultation mit der Aufsichtsbehörde.

1.11. Wir stellen dem Kunden auf dessen Anforderung alle erforderlichen und bei uns vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem AVV und unseren Verpflichtungen als Auftragsverarbeiter nach der DSGVO zur Verfügung.

1.12. Der Kunde ist berechtigt, einmal pro Kalenderjahr und mit mindestens dreißig (30) Tagen schriftlicher Vorankündigung durch den Kunden, während unserer üblichen Geschäftszeiten ein Audit durchzuführen oder durch einen unabhängigen Drittauditor durchführen zu lassen, um die Einhaltung der datenschutzrechtlichen Bestimmungen gemäß diesem AVV durch uns zu überprüfen. Die Kosten des gemäß dieser Ziffer 1.12 durchgeführten Audits trägt der Kunde.

1.13. Im Rahmen des Audits arbeiten wir mit dem Kunden in angemessener Weise zusammen. Das Audit ist in Art, Umfang und Dauer auf das beschränkt, was für die Erreichung des Zwecks angemessen und erforderlich ist, und darf zu keiner unnötigen Störung unseres Geschäftsbetriebs führen.

1.14. Ein vom Kunden bestellter unabhängiger Drittauditor darf nicht im Wettbewerb zu uns stehen und muss vor dem Zugang zu jeglichen Informationen oder unseren Geschäftsräumen eine Geheimhaltungsverpflichtung unterschreiben auf Basis der von uns zuvor genehmigten Bedingungen.

1.15. Mit Ausnahme der oben genannten Verpflichtungen, ist der Kunde für die Rechtmäßigkeit der Verarbeitung der vom Kunden zur Verarbeitung zur Verfügung gestellten personenbezogenen Daten verantwortlich. Dies beinhaltet unter anderem die Einholung etwaig notwendiger Nutzungsrechte, Genehmigungen oder Zustimmungen für die Verarbeitung und die Benachrichtigung zuständiger Behörden oder Datenschutzbeauftragen über die Verarbeitung.

1.16. Hinsichtlich unserer Haftung nach diesem AVV wird auf Ziffer 9 des Teils I. verwiesen, welche auch für diesen AVV Anwendung findet. Soweit Dritte Ansprüche aufgrund einer rechtswidrigen Verarbeitung der personenbezogenen Daten gegen uns geltend machen, stellt der Kunde uns von diesen Ansprüchen frei, es sei denn der Anspruch beruht auf einer schuldhaften Nichterfüllung einer unserer Verpflichtung aus diesem AVV. Eine Freistellung von Ansprüchen Dritter durch den Kunden erfolgt auch dann, wenn der Anspruch auf einer Weisung des Kunden beruht, die im Widerspruch zu geltenden datenschutzrechtlichen Bestimmungen steht und wir den Kunden gemäß Ziffer 1.17 darauf hingewiesen haben. Der Kunde verpflichtet sich ferner, uns auch von allen etwaigen Geldbußen, die gegen uns verhängt werden, in dem Umfang freizustellen, in dem der Kunde Anteil an der Verantwortung für den durch die Geldbuße sanktionieren Verstoß trägt.

1.17. Wir informieren den Kunden umgehend schriftlich, falls eine Weisung des Kunden nach unserer Meinung die geltenden datenschutzrechtlichen Bestimmungen verletzt.

1.18. Mit Beendigung dieses AVV werden wir gemäß den Weisungen des Kunden entweder alle personenbezogenen Daten löschen oder dem Kunden zurückgeben und sicherstellen, dass keine personenbezogenen Daten bei uns oder bei einem Unterauftragsverarbeiter verbleiben. Falls der Kunde innerhalb von 90 Tagen nach Beendigung dieses AVV keine Weisungen erteilt, werden wir alle den Kunden betreffenden Daten in der Schnittstelle löschen (einschließlich aller personenbezogenen Daten, die gemäß diesem AVV verarbeitet wurden) und werden dies dem Kunden auf Anfrage bestätigen. Unser Recht und das Recht der Unternehmen der Volvo Group, die während der Laufzeit dieses AVV erfassten Daten für eigene Zwecke verarbeiten, bleibt unberührt.

2. Arten personenbezogener Daten, Kategorien betroffener Personen, Art und Zweck der Verarbeitung

2.1 Arten personenbezogener Daten und Kategorien betroffener Personen

Die folgenden Arten personenbezogener Daten, die die angegebenen Kategorien betroffener Personen betreffen, werden von uns im Auftrag des Kunden gemäß diesem AVV verarbeitet:

- Baumaschinendaten, die erfasst, gespeichert und erhalten werden durch: (1) das Telematik-System, (2) den Co-Piloten, (3) die Diagnose-Tools und (4) uns, den Kunden oder Dritte. Die entsprechenden Daten beinhalten, ohne darauf beschränkt zu sein, Informationen zur Leistung der Baumaschinen, Daten zu Geopositionierung, Betriebsstunden, Kraftstofffüllstand, Kraftstoffverbrauch, Fehlercodes (Fehler) und Alarmmeldungen, baumaschinentypspezifische Informationen (Lastenmessung, Betriebs-/Standzeiten, Hardware-/Softwarekonfiguration, Arbeitsmodus etc.) sowie die Seriennummer und sonstige Identifikationsdaten. Einige Funktionen der Services kombinieren gegebenenfalls Daten mehrerer Drittanbieter von Services. Die Daten können an einen bestimmten Baumaschinenführer gekoppelt sein und daher personenbezogene Daten darstellen.

- Sonstige personenbezogene Daten, die uns durch den Kunden durch seine Nutzung der Services bereitgestellt werden, wie z. B. Kontaktdaten. Diese personenbezogenen Daten könnten z. B. Mitarbeiter des Kunden betreffen. Hierbei handelt es sich um Vor- und Nachnamen, Funktion/Titel, E-Mail-Adresse, Telefonnummern und Debitorennummern.

2.2 Art und Zweck der Verarbeitung

Wir verarbeiten die personenbezogenen Daten im Auftrag des Kunden zum Zweck der Erbringung der Services. Wir dürfen die personenbezogenen Daten gemäß diesem AVV und seinen Anhängen im Auftrag des Kunden nicht für andere Zwecke verarbeiten, es sei denn, es ist etwas anderes vereinbart.

Anhang 1 zu Teil II. – Technische und organisatorische Maßnahmen der Unterauftragsverarbeiter (Volvo IT/HCL/HCL Sweden im Auftrag des Händlers

1. Zugangskontrolle

Alle IT-Standorte, die zur Bereitstellung von Services genutzt werden, sind in verschiedene Sicherheitszonen unterteilt, wobei Computerräumen die höchste Sicherheitsklassifizierung zuteil wird. Eintritts- und Zugangssysteme sind hochmodern mit Zugangskontrollprüfungen zwischen den Zonen und Bereichen der Einrichtungen, so dass lediglich autorisiertes Personal Zugang hat. Die Computerräume und Eingänge werden von Sicherheitspersonal videoüberwacht, sind alarmgesichert und mit Überwachungssystemen ausgestattet.

2. Zugangskontrolle zu den Systemen

Der Zugang zu den Systemen und Anwendungen ist durch zahlreiche Anweisungen aufgebaut, die eine individuelle und persönliche Nutzeridentifizierung und Authentifizierung, Zugangskontrolle, Protokollierungen und Nachverfolgungen bieten. Zugang zu den Systemen erfolgt durch Kerberos-Sitzungstickets. Der Fernzugriff auf die Netzwerkressourcen macht ergänzende Ausrüstung in Form von Token (Generierung eines einmaligen Passwortes) erforderlich, Passwörter werden automatisch dahingehend überprüft, ob sie bestimmte Buchstaben und sonstige Merkmale aufweisen, und müssen regelmäßig geändert werden. Die Nutzer-IDs / Passwörter werden nach einer vorgegebenen Anzahl fehlerhaften Versuche automatisch gesperrt und Clients werden nach einem vorgegebenen Zeitraum der Inaktivität auf Stand-by gesetzt. Portable Clients sind standardmäßig verschlüsselt. Stationäre Clients, Server und Disk-Arrays werden bei Bedarf verschlüsselt.

3. Zugangskontrolle zu den Daten

Das System verhindert Aktivitäten, die nicht durch die zugewiesenen Zugangsberechtigungen entsprechen. Das Kontrollsystem für Datenzugriff und Autorisierung basiert auf einem kundenspezifischen In-house-System, in dem Nutzer den Zugang beantragen können und eine differenzierte Zugangskontrolle gewährleistet ist. Der Zugang muss durch mindestens zwei Parteien genehmigt werden - die verantwortliche Führungskraft und dem System-/Anwendungs-/Informationsverantwortlichen. In einigen Fällen ist die detaillierte Zugangsberechtigung (wie z. B. die Berechtigung zur Erstellung, Änderung oder Löschung von Aufzeichnungen) innerhalb der Anwendung definiert. In diesen Fällen wird der Systemverantwortliche nach wie vor auf die Anwendung zugreifen, bearbeitet den Vertrieb jedoch selbst oder durch Delegieren an einen Systemadministrator delegieren.

4. Offenlegungskontrolle

Durch den anwendbaren Sicherheitsrahmen ist vorgegeben, dass sowohl internationale als auch nationale Gesetzgebung eingehalten werden muss, unabhängig davon, wo die Tätigkeit durchgeführt werden. Die Vorschriften bezüglich persönlicher Integrität basieren auf der DSGVO und allen entsprechend anwendbaren Vorschriften, die durch nationale Gesetzgebung ergänzt werden. Ein höherer Schutz der Information, wie Verschlüsselung wird vom Kunden, je nach Klassifizierung der Information, angeordnet. Fernzugriff auf die anwendbaren Netzwerke ist grundsätzlich geschützt (VPN) und die Verschlüsselung innerhalb des Netzwerks hängt von den Kundenanforderungen ab. Die verschlüsselte Speicherung wird lediglich bei mobilen Clients als Standardleistung angeboten. Die Verschlüsselung kommt als zusätzlicher Service zum Einsatz, wenn die Kundennachfrage dies erfordert.

5. Eingabekontrolle

Jeder Unterauftragsverarbeiter hat die Möglichkeit, alle in Systemen und Anwendungen vorgenommenen Tätigkeiten zu protokollieren. Ob diese Möglichkeit zum Einsatz kommt oder nicht, basiert auf der Vereinbarung mit dem Kunden, dem die Klassifizierung der Informationen bezüglich Integrität der (personenbezogenen) Daten bekannt sein muss. Es gibt keine automatische Funktion, die eigenständig bewerten kann, ob die Integrität personenbezogener Daten durch Nutzung, Änderung, Verschiebung oder Löschung beeinträchtigt wurde.

6. Kontrolle der Tätigkeit

Die Volvo IT ist eine hundertprozentige Tochtergesellschaft der AB Volvo, und die Volvo IT ist seit Jahrzehnten der Hauptlieferant von IT-Dienstleistungen für Händler der Volvo Group, HCL und HCL Sweden sind strategische Partner der Volvo Group und die Hauptinfrastrukturlieferanten für die Infrastruktur von Volvo IT. Jedoch sind Volvo IT, HCL und HCL Sweden als Lieferanten nicht vorgeschrieben und der Händler kann sich für andere Anbieter entscheiden. Das Auswahlkriterium für einen IT-Anbieter innerhalb oder außerhalb der Volvo Group ist hauptsächlich durch Wirtschaftlichkeit, Verfügbarkeit, Sicherheit und Serviceniveau geprägt.

Serviceniveaus und die Sicherheit basieren üblicherweise auf den grundlegenden Sicherheitsniveaus von Volvo IT, die im Handbuch zu Unternehmenssicherheit von Volvo IT aufgeführt sind. Sollten zusätzliche Sicherheitsmaßnahmen basierend auf der Klassifizierung der Information erforderlich sein, wird dies zwischen dem Kunden und dem Händler ausgehandelt und die erforderlichen Maßnahmen werden ergriffen. Volvo IT verfügt über eine eigene Prüfungsorganisation, die die Organisation und die Erbringung von Dienstleitungen regelmäßig überprüft. Außerdem wird Volvo IT sowohl von PricewaterhouseCoopers (im Auftrag der AB Volvo) und vom Bureau Veritas (Zertifizierungsstelle für das ISO 27001-Zertifikat, das die Volvo IT besitzt) auditiert. Das VINST-System, in dem alle

Kundenanforderungen (oder Anforderungen von Volvo IT) erfasst werden, wird sichergestellt, dass Volvo IT die Vertragserfüllung nachverfolgt. Falls der Händler nicht der regelmäßigen in dieser Klausel 6 festgestellten Prüfung unterliegt, ist der Kunde berechtigt, Prüfungen beim Händler durchzuführen.

7. Verfügbarkeitskontrolle

Der Kundenvertrag beinhaltet Maßnahmen für die Verfahren der Volvo IT, der Spiegelung von Festplatten (falls notwendig zwischen verschiedenen Computerzentren), unterbrechungsfreie Stromversorgung (USV) und ist für alle unsere Computerzentren erforderlich. In einem Dritt-Computerzentrum werden die Backups gespeichert. Dieses Computerzentrum ist unabhängig von den anderen beiden Zentren, die die Primärdaten verwalten. Alle Standorte, Plattformen und Systeme sind verpflichtet, sich an die Richtlinie des Business Continuity Managements der Volvo IT zu halten, die besagt, dass komplette Wiederherstellungspläne vorliegen und in regelmäßigen Abständen getestet werden müssen.

Die Volvo IT verfügt über eine fortschrittliche Umsetzung von Maßnahmen gegen Schadsoftware. Dies orientiert sich an den Regelungen der IT-Richtlinie für Virenschutz. Ebenso besteht die physische Umsetzung, die auf Basis dieser Richtlinie erfolgt, aus einer mehrstufigen Schutzsoftware gegen Malware unterschiedlicher Lieferanten. Dies erfolgt, um die möglichen Schwächen eines Produkts zu kompensieren. Dies schließt sowohl die Server als auch die Endgeräte ein und wird durch persönliche Firewalls und Informationsverarbeitungssysteme / Angrifferkennungssysteme (IPS / IDS) auf allen Endgeräten sowie auf Netzwerkebene ergänzt.

Die Anordnung beinhaltet auch eine zentrale Funktion für die Kontrolle der Sicherheitsanfälligkeit und die Umsetzung von Sicherheitspatches für die Betriebssysteme und die Anwendungen, die als Garant dafür dienen, dass das System so fehlerfrei wie möglich funktioniert.

8. Kontrolle der getrennten Datenaufbewahrung

Personenbezogene Daten, die für unterschiedliche Zwecke erfasst wurden, werden gemäß der schwedischen Gesetzgebung und den Sicherheitsbestimmungen von Volvo getrennt voneinander verarbeitet.

Die Test- und die Produktionsumgebungen werden gemäß den Regelungen des Händlers strikt voneinander getrennt, und ein Entwickler kann niemals eine Aktualisierung der Produktionsumgebung vornehmen. Dies sorgt für eine Sicherstellung der Aufgabentrennung.

Daten unterschiedlicher Kunden werden in den meisten Fällen an getrennten physischen Orten gespeichert. Dennoch setzt die Volvo IT bei der Anwendung ihrer Speicher-Philosophie auf Zersplitterung der Daten. Dies bedeutet, dass alle Informationen auf verschiedene Medien aufgeteilt werden, was wiederum bedeutet, dass die Informationen nicht mehr hergestellt werden können, falls ein physisches Medium kompromittiert ist

Die Client-Daten werden für interne Kunden durch die Nutzung einer ACL (Zugriffskontrollliste) im AD (Active Directory) über ein CIFS-Netzwerkprotokoll gespeichert. Für externe Kunden verfügt die Volvo IT über dedizierte logische Speichersysteme. NFS ist ein Speichersystem, das über Exportrechte verfügt.

Die Server/Datenbanken, welche über eine FCP-Schnittstelle angeschlossen sind, nutzen LUN-Sicherheit (Logical Unit Number) im Speichersystem und Zoning im SAN-Netzwerk, um den Zugang zu den Server-Festplatten sicherzustellen.

Bitte beachten Sie: Alle Anforderungen weitergehender Informationen und alle weiteren Anfragen sind schriftlich an den Händler zu richten. Für alle Teile dieses Vertrags, für die der Händler oder sein Unterauftragnehmer der Volvo IT, HCL, HCL Sweden oder einen jeglichen sonstigen Unterauftragnehmer außerhalb der Volvo Group beauftragt, stellt der Händler sicher, dass der entsprechende Unterauftragnehmer Verpflichtungen und Routineabläufe einhält, die mindestens genauso restriktiv oder schützend sind wie die in diesem Anhang 3 dargelegten Verpflichtungen und Routineabläufe.

Anhang 2 zu Teil II. – Technische und organisatorische Maßnahmen der Robert Aebi GmbH

Anforderungen

Der Auftragsverarbeiter stellt die Umsetzung und Einhaltung der geforderten technischen und organisatorischen Maßnahmen gemäß § 32 DSGVO sicher. Dazu gehören Maßnahmen, die dazu dienen, für die fortlaufende Vertraulichkeit, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und Dienste zu sorgen. Zu den geeigneten technischen und organisatorischen Maßnahmen zählen beispielsweise Pseudonymisierung und Verschlüsselung der personenbezogenen Daten. Der Auftragsverarbeiter verwendet Verfahren und Dokumentationen, die eine regelmäßige Prüfung, Beurteilung und Bewertung der Wirksamkeit der eingeführten technischen und organisatorischen Maßnahmen vorsehen, damit die Sicherheit der Verarbeitung gewährleistet wird.

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

Zutrittskontrolle

Das Ziel einer Zutrittskontrolle ist es, Unbefugten den Zutritt (z.B. zu Datenverarbeitungsanlagen) zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden. Der Begriff des Zutritts ist dabei räumlich zu verstehen.

- Der Zugang zu Standorten, an denen Server oder Endgeräte untergebracht sind, wird nur befugtem Personal gewährt.
- Die Zugangsberechtigung von Personal, das nicht länger befugt ist, wird unverzüglich widerrufen.
- Die Befugnis wird nach dem Prinzip der Notwendigkeit vergeben.
- Das Grundstück ist in komplett umzäunt und wird außerhalb der Geschäftszeiten verschlossen. Der Außenbereich und der Empfangsbereich sind videoüberwacht.
- Zutritt des Geländes sowie des Gebäudes erfolgt über ein zentral verwaltetes Tokensystem. Diese werden individuell und dokumentiert an Mitarbeiter vergeben. Diese Token sind mit diversen Berechtigungen ausgestattet, je nach Funktion und Befugnis. Bei Verlust können die betroffenen Token sofort gesperrt werden.

Zugangskontrolle

Das Ziel einer Zugangskontrolle ist es, mithilfe geeigneter Maßnahmen zu verhindern, dass Unbefugte in Datenverarbeitungsanlagen und -systeme, mit denen personenbezogene Daten verarbeitet oder genutzt werden, eindringen oder diese nutzen können.

- Der Zugang zu den technischen Systemen der Aebi GmbH erfolgt nach Beantragung und Genehmigung durch den Vorgesetzten.
- Es erfolgt eine zentrale Benutzerverwaltung in einer geschützten Datenbank (LDAP).
- Der Zugriff auf die Systeme, Netzlaufwerke und Ablagesysteme erfolgt personalisiert.
- Der Datenaustausch zwischen Standorten und Rechenzentren erfolgt verschlüsselt (VPN-MPLS).
- Es gibt eine automatische, kennwortgeschützte Sperrung des Bildschirms.
- Es ist ein komplexes Kennwort erforderlich mit einer Mindestlänge von 8 Zeichen, Kennwort-wechsel alle 42 Tage mit Kennwortchronik.
- IT-Richtlinien im Umgang mit Hard- und Software existieren und werden regelmäßig überarbeitet.
- Es existiert eine Clean-Desktop-Policy.
- Die Vernichtung von Dokumenten erfolgt mittels Shredder (Sicherheitsstufe P4),
- Die Vernichtung von Datenträgern erfolgt physikalisch und wird schriftlich protokolliert (AV-Vertrag).
- Sorgfältige Auswahl von Dienstleistern
- Es werden nur Reinigungsdienste in Anspruch genommen, die die Mitarbeiter auf das Datenschutzgeheimnis verpflichtet haben.
- Einsatz von Antiviren-Software sowie Firewall

Zugriffskontrolle

Das Ziel einer Zugriffskontrolle ist es, zu gewährleisten, dass ausschließlich die zur Benutzung der Daten-verarbeitungssysteme Berechtigten auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung und Nutzung und nach der Speicherung nicht unbefugt gelesen, vervielfältigt, verändert oder entfernt werden können.

- Der Zugriff erfolgt nach einem Rollen- und Berechtigungskonzept mit Benutzerkennung und Passwort, welches gewährleistet, dass die Mitarbeiter nur die notwendigen Zugriffe erhalten.
- Ein Rollenkonzept regelt die Zugriffsberechtigung nach Beantragung und Genehmigung durch den Vorgesetzten.
- Die Zugriffe werden technisch überwacht. Die Ausführung administrativer Zugriffe wird protokolliert und kontrolliert. Auf die Anwendung bezogene Zugriffe werden mit den Mitteln und Möglichkeiten der Anwendung protokolliert und überwacht.
- Generell sind Systeme und Anwendungen, die zur Verarbeitung von personenbezogenen Daten verwendet werden, durch Passwortverfahren gesichert.
- Die Anzahl der Administratoren ist auf das notwendige reduziert
- Einsatz von Aktenvernichtern Sicherheitsstufe mind. P4.
- Physische Löschung von Datenträgern.

Trennungskontrolle

Das Ziel des Trennungsgebots ist es, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten ebenfalls getrennt voneinander verarbeitet werden.

- Die Robert Aebi GmbH greift auf die Rechenzentren der Aebi AG Schweiz zu: Alle Systeme und Anwendungen sind speziell auf eine zweckgebundene und mandantengetrennte Verarbeitung ausgerichtet.
- Steuerung über Berechtigungskonzept

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

Weitergabekontrolle

Das Ziel einer Weitergabekontrolle ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, vervielfältigt, verändert oder entfernt werden können und dass überprüft sowie festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Der Zugriff auf die Systeme von außerhalb erfolgt per VPN und MFA.
- Zum Schutz vor Weitergabe von Daten werden an die jeweiligen Erfordernisse angepasste und abgestufte Sicherheits- und oder Verschlüsselungsverfahren verwendet. Dazu gehören Firewall-Systeme und ständig aktualisierte Virensoftware sowie einer Secure Socket Layer (SSL) Verschlüsselung für die Kommunikation im Internet.
    - Saveguard private crypto für Passwortvergabe bei Dateiversand
    - DTA Dateien verschlüsselt über eCash der Institute
    - Passwortschutz für abgestimmte Dateien
    - Verschlüsselte Weitergabe im Netzwerk

Eingabekontrolle

Das Ziel einer Eingabekontrolle ist es, dass nachträglich festgestellt werden kann, ob und von wem personenbezogene Daten in die Systeme und Anlagen zur Datenverarbeitung eingegeben, verändert oder entfernt worden sind.

- Die Eingabe und andere Verarbeitungen sind mittels Logdateien nachvollziehbar.
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Rechtekonzepts.
- Die Eingaben in Systeme und Anwendungen sowie deren Ausgaben werden generell protokolliert.
- Die Protokolle werden entsprechend den Inhalten und oder gesetzlichen Vorgaben archiviert oder nach Zweckerreichung gelöscht bzw. für die weitere Verarbeitung gesperrt.

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

Verfügbarkeitskontrolle

Das Ziel der Verfügbarkeitskontrolle ist es, zu gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust physisch sowie auch logisch geschützt sind.

- Es existiert ein Backupkonzept.
- Testen von Datenwiederherstellung.
- Virenschutz mit aktuellen Service Packs.
- Firewall.
- Serverräume befinden sich nicht unter wasserführenden Anlagen.
- Einheiten für unterbrechungsfreie Strom-versorgung.
- Sowohl die Versorgungs- als auch die Verarbeitungssysteme sind redundant ausgelegt.
- Daten werden mittels RAID-Systeme mehrfach gespeichert und gesichert.
- Eine permanente Überwachung der Auslastungen der Systeme sowie Maßnahmen zur Lastverteilung werden durchgeführt und erhöhen die Verfügbarkeit zusätzlich.
- Für den Katastrophen- oder Notfall bestehen ausgereifte Ausweich- und Wiederanlaufkonzepte. Ihre Funktionsfähigkeit wird regelmäßig getestet und die Testergebnisse dokumentiert, bewertet und Optimierungs-potenziale genutzt.

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

Datenschutz-Management

- Der Auftragnehmer hat ein Datenschutz-Managementsystem implementiert
- Es ist ein Datenschutzbeauftragter bestellt

Auftragskontrolle

Das Ziel einer Auftragskontrolle im Sinne von Art. 28 DSGVO ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend des Auftrags und der Weisungen des Auftragsgebers verarbeitet werden können.

- Sorgfältige Auswahl von Auftragnehmern bei der Verarbeitung von personenbezogenen Daten mit Auftragsverarbeitungsvertrag nach Artikel 26 DSGVO mit entsprechenden Kontrollrechten und Weisungsbefugnis.
- Prüfung des Auftragnehmers.
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis.
- Sicherstellung und Vernichtung von Daten nach Beendigung des Auftrags.
- Die Auftragskontrolle wird unterstützt durch: definierte Melde- und Ticketprozesse für die Auftragserteilung.
- Namentlich benannte Ansprechpartner auf Seiten Arbeitnehmer und Arbeitgeber.
- Verpflichtung des Auftragnehmers zum Datenschutz im Vertrag.
- Hinreichend dokumentierte TOMs der Dienstleister.