m^{IoT} Agreement

Dieses ifm *mobile*^{IoT} Agreement (das **"Agreement“**) wird zwischen ifm (im Folgenden **"ifm"**) und dem Kunden (im Folgenden **"Kunde**", beide gemeinsam als **"Partei"** bzw. **"Parteien"** bezeichnet) geschlossen.

ifm und der Kunde erklären sich mit den Bedingungen dieses Agreements, wie folgt, einverstanden:

1. Definitionen

"API“ bezeichnet eine Anwendungsprogrammierschnittstelle.

„API Anpassungen" haben die in Abschnitt 5.1 des Agreements festgelegte Bedeutung.

„CUs“ (Communication Units / Kommunikationseinheiten)" bezeichnet die von ifm an den Kunden verkauften und in die Endkundenmaschinen installierten Onboard-Hardwaregeräte, die Maschinendaten zu und von der ifm Plattform über das ifm Webportal übertragen.

"Derivate" bezeichnet unter anderem sämtliche Ableitungen, Modifikationen, Fehlerkorrekturen, Patches, Bugfixes, Konfigurations- und Kalibrierungseinstellungen, Software-Updates und Software-Upgrades, Verbesserungen, Weiterentwicklungen und nachfolgende Versionen der ifm Software, unabhängig davon, ob diese von ifm oder einem Dritten entwickelt wurden.

"Eingeschränkte IP-Rechte des Kunden" bezeichnet (a) die in Abschnitt 2.2 definierten Weiterveräußerungsrechte, (b) die in Abschnitt 2.2 definierten Zugriffs- und Servicekonfigurationsrechte für Maschinendaten (nur wenn vom Kunden gewählt) und (c) die in Abschnitt 8.1 definierten Unterlizenzierungsrechte.

"Endkunde" bezeichnet die Kunden des Kunden: (a) deren Maschinen Kommunikationseinheiten verwenden, die vom Kunden im Rahmen dieses Agreements und seiner Anlagen bezogen wurden, und/oder (b) die Abonnenten des ifm *mobile*^{IoT} Services sind, der vom Kunden im Rahmen dieses Agreements und seiner Anlagen bezogen wurde.

"Endnutzer" bezeichnet die Beschäftigten und temporären Mitarbeiter des Endkunden, die von ihm ermächtigt wurden, den ifm *mobile*^{IoT} Service in seinem Namen gemäß den Bestimmungen des ifm Endnutzungsvertrages zu nutzen.

"Enduser-Agreement (EUA)" bezeichnet den Endnutzer-Lizenzvertrag, der diesem Agreement als Anhang beigefügt ist und dem die Endkunden und ihre Endnutzer unterliegen, wenn sie auf den ifm *mobile*^{IoT} Service zugreifen und diesen nutzen.

"Geistiges Eigentum von ifm " bezeichnet die ifm Software, die ifm Plattform, das ifm Webportal, die ifm Spezifikationen, die ifm Marken, alle Patente, Urheberrechte, Urheberpersönlichkeitsrechte, Dienst-

leistungsbezeichnungen, Handelsnamen, Logos, Designs, Slogans, Internet-Domainnamen, geschützte Informationen und anderes geistiges Eigentum von ifm, unabhängig davon, ob diese eingetragen sind oder nicht, ob sie vor oder nach dem Inkrafttreten dieses Agreements geschaffen wurden.

"Höhere Gewalt" bezeichnet alle Ursachen außerhalb der zumutbaren Kontrolle einer Partei, die sich auf die Erfüllung des Agreements durch die betreffende Partei auswirken, einschließlich aller Fälle einer längeren Unterbrechung des Transports, des Website Zugangs, der Internetverbindung (ISP), des mobilen Kommunikationsdienstes (Netzbetreiber), anderer Telekommunikation oder der Stromversorgung.

"ifm Firmware" oder **"Firmware"** bezeichnet die Software und/oder Anwendungsprogrammierschnittstelle, die in die ifm Kommunikationseinheit (CU) eingebettet ist, die mit der Maschine verbunden ist, einschließlich Anpassungen oder anderer Derivate davon, die von ifm für den Kunden (oder unabhängig vom Kunden) erstellt wurde, damit die CU mit dem Kommunikationsprotokoll der Maschine kompatibel ist und kommunizieren kann.

"ifm Kommunikationseinheiten" siehe oben **"CUs".**

„ifm *mobile*^{IoT} Service" oder **"Service"** bezeichnet den Online Service, der von der ifm Software auf der ifm Plattform bereitgestellt und von Endkunden und ihren Endnutzern über das ifm Web Portal abgerufen wird, das Maschinendaten präsentiert, die zu und von den CUs, die in Maschinen installiert sind, die sich innerhalb des Vertragsgebiets befinden, übertragen werden.

"ifm Plattform" oder **"DataPlatform"** bezeichnet die Cloud-basierte Plattform, die die ifm Software als eine Service-Anwendung (SaaS) betreibt, wie DataPortal, Realtime Client, REST API oder andere IT Systeme, über den Kunden und ihre Endkunden und deren Endnutzer Online-Zugang zur Nutzung des ifm ***mobile***^{IoT} Services erhalten.

"ifm Software" oder **"Software"** bezeichnet die ifm Software im Objektcode-Format, die ifm *mobile*^{IoT} Service auf der ifm Plattform ausführt, einschließlich ifm Webportal, REST API und Realtime Client, von Software-Updates und -Upgrades, Konfigurations- und Kalibrierungseinstellungen und die dazu notwendigen Tools sowie Installations- und Bedienungsanleitungen und anderen damit in Zusammenhang stehenden Softwaredokumentationen.

"ifm Web Portal" oder **"DataPortal"** bezeichnet die Website, die auf Wunsch des Kunden auf seine eigene Marke konfiguriert werden kann, über die Endkunden und ihre Endnutzer online auf ihre Maschinendaten zugreifen können.

"Kunde" bezeichnet das in der Präambel zu diesem Agreement benannte Unternehmen.

"Kundenmarke" bezeichnet den Namen, die Marke, das Logo, die Adresse und andere Aspekte der Marke des Kunden.

"Maschine" bezeichnet ein Fahrzeug, eine Maschine oder einen anderen Vermögenswert, den der Endkunde vom Kunden oder einem Zwischenhändler gekauft oder geleast hat, um ihn zu Geschäftszwecken einzusetzen, für den Maschinendaten über den ifm *mobile*^{IoT} Service übertragen werden.

"Maschinendaten" bezeichnet: (a) die von den ifm Kommunikationseinheiten gesammelten und an die ifm Plattform übermittelten maschinenlesbaren Rohdaten, und (b) die daraus durch den ifm *mobile*^{IoT} Service in Form von Einzel- oder Gesamtdaten gewonnenen Nutzdaten über die Maschinen eines Endkunden, wie Status geografischen Standort, Betriebsstunden und andere zwischen der ifm Plattform und den Kommunikationseinheiten übertragenen Fahrzeug- und Maschinendaten.

"Mobiler Kommunikationsdienst" bezeichnet alle von den CUs verwendeten Kommunikationsstandards, z.B. LTE, 5G, oder einen anderen Kommunikationsdienst, der für die Übertragung von Maschinendaten zu und von den CUs und der ifm Plattform verwendet wird.

"Partei", "Parteien" hat die in der Präambel zu diesem Agreement festgelegte Bedeutung.

"Software Updates" bezeichnet eine spätere Veröffentlichung der ifm Software, die ifm Nutzung des ifm *mobile*^{IoT} Services nach eigenem Ermessen einsetzt.

„**Verbundene Unternehmen**" bezeichnet jedes Unternehmen, jede Gesellschaft oder sonstige Rechtspersönlichkeit, welche: (1) von einer Partei dieses Agreements kontrolliert wird, oder (2) eine Partei kontrolliert oder (3) mit einer Partei dieses Agreements unter gemeinsamer Kontrolle steht, solange eine solche Kontrolle fortbesteht. In diesem Sinne bedeutet "Kontrolle", dass sich mehr als fünfzig Prozent (50 %) der Beteiligungen oder Geschäftsanteile der kontrollierten Rechtspersönlichkeit, die dazu berechtigen, Entscheidungen für eine solche Rechtspersönlichkeit zu treffen, im Besitz oder unter Kontrolle, direkt oder indirekt, der kontrollierenden Rechtspersönlichkeit befinden.

"**Verletzung geistigen Eigentums**" hat die in Abschnitt 8.1 des Agreements festgelegte Bedeutung.

2. Angebot zum Vertragsschluss

2.1 ifm Kommunikationseinheiten (CUs)

ifm wird seine Kommunikationseinheiten in Übereinstimmung mit diesem Agreement und den Einzelverträgen nach Bestellung an den Kunden verkaufen.

2.2 ifm *mobile*^{IoT} Service Abonnements

Mit dem Kauf einer Kommunikationseinheit erwirbt der Kunde ein dazugehöriges Service Abonnement, das er direkt (oder über Drittanbieter) an seine Endkunden oder deren Endnutzer in Übereinstimmung mit den Bestimmungen dieses Agreements weiterveräußern darf **("Abonnement-Weiterveräußerungsrechte")**. Darüber hinaus hat der Kunde folgende angegebenen Zusatzoptionen: (a) Er kann einen lizenzierten Zugriff auf Maschinendaten für den eigenen internen Zugriff, die eigene Speicherung und Auswertung erwerben und (b) der Kunde kann Dienstleistungen erwerben, um das Web Portal so zu konfigurieren, dass der Endkunde auf den ifm *mobile*^{IoT} Service über ein auf die Kundenmarke konfiguriertes Portal (Customized Front End) zugreifen kann (**"Maschinendaten Zugriffs- und Servicekonfigurationsrechte"**).

2.3 Keine anderen Produkte, Dienstleistungen oder Lizenzen

ifm ist nicht verpflichtet, andere Produkte, Dienstleistungen oder Lizenzen im Rahmen dieses Agreements zu verkaufen oder anderweitig zur Verfügung zu stellen. Dazu bedarf es einer gesonderten schriftlichen Vereinbarung.

3. Eigentumsvorbehalt

Die Gegenstände der Lieferungen (Vorbehaltsware) bleiben Eigentum von ifm bis zur Erfüllung sämtlicher ihm gegen den Kunden aus der Geschäftsverbindung zustehenden Ansprüche. Soweit der Wert aller Sicherungsrechte, die ifm zustehen, die Höhe aller gesicherten Ansprüche um mehr als 20 % übersteigt, wird ifm auf Wunsch des Kunden einen entsprechenden Teil der Sicherungsrechte freigeben; ifm steht die Wahl bei der Freigabe zwischen verschiedenen Sicherungsrechten zu.

Während des Bestehens des Eigentumsvorbehalts ist dem Kunden eine Verpfändung oder Sicherungsübereignung untersagt und die Weiterveräußerung nur Wiederverkäufern im gewöhnlichen Geschäftsgang und nur unter der Bedingung gestattet, dass der Wiederverkäufer von seinem Kunden Bezahlung erhält oder den Vorbehalt macht, dass das Eigentum auf den Kunden erst übergeht, wenn dieser seine Zahlungsverpflichtung erfüllt hat.

Veräußert der Kunde Vorbehaltsware weiter, so tritt er bereits jetzt seine künftigen Forderungen aus der Weiterveräußerung gegen seine Kunden mit allen Nebenrechten – einschließlich etwaiger Saldoforderungen – sicherungshalber an ifm ab, ohne dass es weiterer besonderer Erklärungen bedarf. Wird die Vorbehaltsware zusammen mit anderen Gegenständen weiter veräußert, ohne dass für die Vorbehaltsware ein Einzelpreis vereinbart wurde, so tritt der Kunde denjenigen Teil der Gesamtpreisforderung an ifm ab, der dem von ifm in Rechnung gestellten Preis der Vorbehaltsware entspricht.

4. Haftung / Gewährleistung

4.1 Gefahrübergang

Die Gefahr geht auch bei frachtfreier Lieferung wie folgt auf den Kunden über:

a) bei Lieferung ohne Aufstellung oder Montage, wenn sie zum Versand gebracht oder abgeholt worden ist. Auf Wunsch und Kosten des Kunden wird die Lieferung vom Lieferer gegen die üblichen Transportrisiken versichert;

b) bei Lieferung mit Aufstellung oder Montage am Tage der Übernahme in eigenen Betrieb oder, soweit vereinbart, nach erfolgreichem Probebetrieb.

Wenn der Versand, die Zustellung, der Beginn, die Durchführung der Aufstellung oder Montage, die Übernahme in eigenen Betrieb oder der Probebetrieb aus vom Kunden zu vertretenden Gründen verzögert wird oder der Kunde aus sonstigen Gründen in Annahmeverzug kommt, so geht die Gefahr auf den Kunden über.

4.2 Haftung / Gewährleistung

Das Produkt wird in der Produktbeschreibung (Anlage 2) abschließend beschrieben. ifm gewährleistet die Funktionalität ihrer Katalogprodukte für die Dauer von 60 Monaten ab Lieferung des Produktes, sofern dieses innerhalb der Spezifikation betrieben wird. Der Kunde hat das Produkt unverzüglich, spätestens innerhalb von einem Monat ab Lieferung, auf eventuelle Mängel zu untersuchen und gegebenenfalls schriftlich zu rügen. Im Falle einer Reklamation muss der Kunde das Produkt zusammen mit

einer Fehlerbeschreibung unter Angabe der ifm Artikelnummer an die zuständige Niederlassung der ifm zurücksenden. ifm wird das Produkt untersuchen und auf Wunsch des Kunden einen Untersuchungsbericht an diesen verschicken. ifm ist Gelegenheit zur Nacherfüllung innerhalb einer angemessenen Frist zu gewähren. Im Falle einer berechtigten Reklamation sind all diejenigen Teile oder Leistungen nach Wahl von ifm unentgeltlich nachzubessern, neu zu liefern oder neu zu erbringen, sofern dessen Ursache bereits im Zeitpunkt des Gefahrübergangs vorlag. Werden vom Kunden oder von Dritten unsachgemäß Änderungen oder Instandsetzungsarbeiten vorgenommen, so bestehen für diese und den daraus entstehenden Folgen keine Mängelansprüche.

Bei Mängelrügen dürfen Zahlungen des Kunden in einem Umfang zurückbehalten werden, die in einem angemessenen Verhältnis zu den aufgetretenen Sachmängeln stehen. Der Kunde kann Zahlungen nur zurückbehalten, wenn eine Mängelrüge geltend gemacht wird, über deren Berechtigung keine Zweifel bestehen kann. Ein Zurückbehaltungsrecht des Kunden besteht nicht, wenn seine Mängelansprüche verjährt sind. Erfolgte die Mängelrüge zu Unrecht, ist der Lieferer berechtigt, die ihm entstandenen Aufwendungen vom Kunden ersetzt zu verlangen.

Schadensersatzansprüche des Kunden wegen eines Sachmangels sind ausgeschlossen. Dies gilt nicht bei arglistigem Verschweigen des Mangels, bei Nichteinhaltung einer Beschaffenheitsgarantie, bei Verletzung des Lebens, des Körpers oder der Gesundheit und bei einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung des Lieferers. Eine Änderung der Beweislast zum Nachteil des Kunden ist mit den vorstehenden Regelungen nicht verbunden. Weitergehende oder andere als in diesem Abschnitt geregelten Ansprüche des Kunden wegen eines Sachmangels sind ausgeschlossen.

4.3 Haftungsbeschränkung

Mit Ausnahme von Vorsatz und grober Fahrlässigkeit haften beide Parteien nur, sofern wesentliche Vertragspflichten (Kardinalpflichten) verletzt wurden und begrenzt auf den vertragstypischen und vorhersehbaren Schaden.

Die Parteien sind sich einig, dass der vertragstypische und vorhersehbare Schaden im Regelfall auf den Betrag begrenzt ist, welcher den vom Kunden an ifm gezahlten Abonnement-Gebühren für zwei Monate ab dem Tag der Entstehung des Anspruchs entspricht. Den Parteien bleibt es unbenommen, einen höheren Schaden nachzuweisen.

Die Parteien haften wechselseitig aus diesem Agreement nicht für Beträge, bei denen es sich um entgangenen Gewinn, entgangene Geschäfte, zufällige oder mittelbare Schäden, Folgeschäden, Strafschadensersatz der anderen Partei handelt, einschließlich für Kosten oder Entschädigungen im Zusammenhang mit Ausfallzeiten des ifm *mobile*$^{\text{IoT}}$ Services, Serviceausfallzeiten des mobilen Kommunikationsdienstes, Verlusten oder Verfälschungen von Maschinendaten oder anderen Daten, Ausfällen oder Fehlern der CU oder der Services, Arbeitsunterbrechungen oder Arbeitsverzögerungen. Die oben aufgeführten Punkte beschränken nicht die beiderseitigen Verpflichtungen im Rahmen der Leistung von Entschädigungen, Ergreifung von Verteidigungsmaßnahmen und Schadloshaltungen, die in den Abschnitten 8.1 und 8.2 des Agreements aufgeführt werden. Die Haftungsbeschränkungen bzw. -ausschlüsse gelten auch nicht im Falle der schuldhaften Verletzung des Lebens, des Körpers oder der Gesundheit sowie für die Haftung nach dem Produkthaftungsgesetz.

4.4 Schadloshaltung

Der Kunde muss ifm freistellen, schützen und schadlos halten vor Klagen, die von einem Dritten gegen ifm oder den Lizenzgeber der ifm erhoben werden, soweit sie unmittelbar auf einem Vorwurf beruhen, dass durch (a) den Zugriff auf oder die Nutzung von Kundendaten mit den Services; oder (b) die Veränderung oder Nutzung der Services mit den Anwendungen des Kunden geistige Eigentumsrechte oder

Geschäftsgeheimnisse Dritter verletzt wurden, und die Entschädigungssummen oder Kosten begleichen, die mit der Beilegung der Klage verbunden sind oder ifm im Rahmen einer solchen Klage letztendlich auferlegt werden und die unter anderem angemessene Anwaltshonorare umfassen, vorausgesetzt ifm (i) unterrichtet den Kunden umgehend von einer solchen Klage; und (ii) lässt dem Kunden umfassende Befugnisse, Informationen und Unterstützung zukommen, um einen solchen Anspruch abzuwehren; und (iii) überlässt dem Kunden die alleinige Kontrolle über die Abwehr eines solchen Anspruchs und alle Verhandlungen über einen Vergleich bezüglich eines solchen Anspruchs. Der Kunde ist berechtigt, ohne vorherige schriftliche Zustimmung von ifm einen solchen Anspruch zu erfüllen oder einen Vergleich einzugehen, sofern ifm durch die Erfüllung oder den Vergleich keine Kosten oder erheblichen Nachteile entstehen.

4.5 Keine Rechte Dritter

Die hier geregelte Gewährleistung ist nicht übertragbar. Weder die Endkunden noch ihre Endnutzer können hieraus Rechte oder Ansprüche gegen ifm herleiten.

4.6 Beschränkung der Gewährleistung

Die in diesem Agreement geregelte Gewährleistung ist exklusiv. Darüber hinaus werden keine Zusicherungen oder Garantien weder in schriftlicher noch in mündlicher Form ausdrücklich oder stillschweigend abgegeben. ifm schließt insbesondere stillschweigende Zusagen in Bezug auf die Wirtschaftlichkeit und Eignung für einen bestimmten Zweck aus. ifm haftet weder aus Vertrag noch aus Gesetz, wenn die CU von Personen verändert werden, bei denen es sich nicht um Mitarbeiter von ifm oder dessen verbundenen Unternehmen handelt.

4.7 Sonstige Schadensersatzansprüche

Soweit nicht anderweitig in diesem Agreement geregelt, sind Schadensersatzansprüche des Kunden, gleich aus welchen Rechtsgrund, insbesondere wegen Verletzung von Pflichten aus dem Schuldverhältnis und aus unerlaubter Handlung, ausgeschlossen. Dies gilt nicht, soweit wie folgt gehaftet wird:

a) Nach dem Produkthaftungsgesetz
b) Bei Vorsatz
c) Bei grober Fahrlässigkeit von Inhabern, gesetzlichen Vertretern oder leitenden Angestellten
d) Bei Arglist
e) Bei Nichteinhaltung einer übernommenen Garantie
f) Wegen der schuldhaften Verletzung des Lebens, des Körpers oder der Gesundheit, oder
g) Wegen der schuldhaften Verletzung wesentlicher Vertragspflichten.

5. Bereitstellung des ifm *mobile*^{IoT} Services

5.1 Erreichen der Interoperabilität

ifm wird mit bestem Wissen und Gewissen und mit wirtschaftlich zumutbaren Anstrengungen daran arbeiten, die Interoperabilität des *mobile*^{IoT} Services mit den Maschinen so bald wie möglich herzustellen, einschließlich der Entwicklung von Anpassungen an die vom Kunden zur Verfügung gestellten API (**"API Anpassungen")** und der Herstellung anderer von ifm für notwendig erachteter Service Konfigurationen zur Erreichung der Interoperabilität. Der Kunde sichert zu und garantiert, dass er über die volle Lizenz, das Recht und die Befugnis verfügt, die Maschinen API an ifm weiterzugeben (ohne Verpflichtung zur Vertraulichkeit), um die Interoperabilität des *mobile*^{IoT} Services mit der Maschine zu erreichen.

5.2 Konfiguration, Aktivierungshilfe, technischer Support

Der Kunde erkennt an und stimmt zu, dass es in seiner Verantwortung und Verpflichtung liegt, anfänglich und fortlaufend, (a) die Darstellung der Maschinendaten und anderer Aspekte des *mobile*^{IoT} Services in der Weise zu konfigurieren, wie sie nach der Servicedokumentation zulässig und ansonsten den Wünschen von ihm und seinen Endkunden entspricht, und (b) den Endkunden und ihren Endnutzern Aktivierungsunterstützung und technischen Support zu leisten.

5.3 Keine Erbringung von sonstigen Dienstleistungen für Endkunden

Mit Ausnahme der Erbringung des *mobile*^{IoT} Services gemäß ist ifm in keiner Weise verpflichtet, Aktivierungshilfe, technischen Support, Schulungen oder andere Dienstleistungen für Endkunden oder deren Endnutzer zu erbringen. Der Kunde ist für die Erbringung solcher Dienstleistungen für Endkunden und deren Endverbraucher allein verantwortlich.

6. Verpflichtungen des Kunden

6.1 Kontrolle über die Nutzung der *mobile*^{IoT} Dienste und Maschinendaten von ifm

Neben den in den Abschnitten 4.5, 5.1, 5.2, 5.3 und 9.3 ist der Kunde stets verantwortlich und haftbar für:

a) die rechtmäßige oder unrechtmäßige Nutzung des ifm *mobile*^{IoT} Services durch Endkunden, deren Endnutzer und andere, denen der Kunde unter Zuwiderhandlung gegen die Bestimmungen dieses Agreements Zugang gewährt haben könnte;

b) die Rechtmäßigkeit aller Maschinendaten, einschließlich, aber nicht beschränkt auf ihre rechtmäßige Beschaffung und Nutzung sowie jegliche Verpflichtung, das Eigentum an Daten zu bestimmen bzw. die darin enthaltenen Rechte auf geistiges Eigentum zu beachten;

c) jede Nachricht, Eingabe oder sonstige Auswirkung, die von den CUs durch die Nutzung *mobile*^{IoT} Services durch den Kunden in die Maschinen-Steuerung, Software oder Systemarchitektur eingebracht wird, und zwar unabhängig davon, ob ifm den Kunden auf die Eintrittswahrscheinlichkeit und die möglichen Folgen hingewiesen hat; sowie

d) die Aktualität der Firmware: Um die Funktionsfähigkeit der CUs zu gewährleisten, muss der Kunde sicherstellen, dass von ifm bereitgestellte Firmware-Updates und Sicherheits-Patches ausgeführt werden.

6.2 Zusammenarbeit und Zugangsgewährung

Wenn ifm die Notwendigkeit sieht, Aktivierungshilfe und technischen Support zu leisten, um die Interoperabilität gemäß Abschnitt 6.1 zu erreichen bzw. das DataPortal für die Kundenmarke zu konfigurieren, verpflichtet sich der Kunde, alles in seiner Macht Stehende zu unternehmen, um ifm dabei zu unterstützen, einschließlich, aber nicht beschränkt auf, (a) den uneingeschränkten Zugriff von ifm auf die Maschinen und CUs und (b) die Bereitstellung eines Ausgabeprotokolls, der Maschinendaten und aller anderen Daten, die ifm vernünftigerweise zur Reproduktion des Problems benötigt.

6.3 Untersuchung von Rechtsverletzungen Dritter

Der Kunde arbeitet mit bestem Wissen und Gewissen mit ifm zusammen und bietet ifm angemessene Unterstützung an, wenn ifm Untersuchungen aufnimmt oder eine Klage einreicht gegen eine dritte Partei, die im Verdacht steht, den *mobile*^{IoT} Service von ifm im direkten oder indirekten Zusammenhang mit

der Nutzung des Services durch den Kunden, seine Endkunden oder deren Endnutzer im Rahmen dieses Agreements zu nutzen oder genutzt zu haben, sofern ifm feststellt, dass die dritte Partei Rechte von ifm an seinem geistigen Eigentum verletzen könnte.

7. Geistiges Eigentum

7.1 Rechte am geistigen Eigentum

In Übereinstimmung mit dem Recht des Kunden, Abonnements gemäß Abschnitt 2.2 dieses Agreements weiter zu veräußern, räumt ifm dem Kunden (und seinen Drittanbietern) hiermit eine korrespondierende beschränkte, kündbare, persönliche, nicht ausschließliche und nicht übertragbare Lizenz ein, Service-Unterlizenzen an die Endkunden des Kunden und deren Endnutzer, die Abonnenten sind, zu vergeben, die in Übereinstimmung mit den Bedingungen dieses Agreements zu nutzen sind (**"Unterlizenzierungsrechte"**). Keines der beschränkten IP-Rechte des Kunden überträgt Ansprüche oder Eigentumsrechte an der CU-Firmware, den API-Anpassungen, der ifm Software, anderem geistigen Eigentum von ifm oder einem anderen Aspekt des ifm *mobile*^{IoT} Services und darf nicht als Verkauf von Rechten angesehen werden. Vorbehaltlich der beschränkten IP-Rechte des Kunden bleibt ifm Inhaber sämtlicher Rechte, Ansprüche und Inhalte aus allem geistigen Eigentum, einschließlich der CU-Firmware, der API-Anpassungen, der ifm-Software, aller Inhalte der DataPlatform und des DataPortals, die nicht die Kundenmarke sind, und aller Derivate, Verbesserungen, kundenspezifischer Anpassungen an den vorgenannten Inhalten, unabhängig davon, ob sie von ifm allein oder zusammen dem Kunden erstellt oder entwickelt wurden, und unabhängig davon, ob sie als Teil der Arbeit gemäß Abschnitt 5.1 oder im Rahmen der Bereitstellung von Aktivierungsunterstützung oder technischem Support erstellt oder entwickelt wurden.

Der Kunde verfügt über keinerlei Rechte zum Besitz von Kopien der ifm Software, es sei denn, es bestehen rechtliche Gründe, die zur Speicherung einer Sicherungskopie zum Zwecke der Archivierung berechtigt. Darüber hinaus gewähren die Bestimmungen in diesem Agreement dem Kunden kein Recht an dem Quellcode der ifm Software. Der Kunde darf weder selbst noch einem lizenzierten Benutzer oder anderen Parteien Folgendes gestatten:

a) eine Rückwärtsentwicklung des Quellcodes vornehmen, diesen dekompilieren, übersetzen, auseinandernehmen oder den Versuch unternehmen, den Quellcode bzw. die dem geistigen Eigentum von ifm zugrundeliegenden Ideen oder Algorithmen ausfindig zu machen oder in sonstiger Form das geistige Eigentum von ifm oder andere Aspekte des ifm *mobile*^{IoT} Services mit Ausnahme in der im vorliegenden Agreement gestatteten Form nutzen,

b) das geistige Eigentum von ifm oder andere Aspekte des ifm *mobile*^{IoT} Services übertragen, verkaufen, vermieten, verleihen, offenlegen, für Timesharing- oder Dienstleistungszwecke nutzen,

c) das geistige Eigentum von ifm oder andere Aspekte des ifm *mobile*^{IoT} Services zu Gunsten einer dritten Partei nutzen, dieser zur Verfügung stellen oder die Nutzung durch andere gestatten,

d) den Versuch unternehmen, das geistige Eigentum von ifm oder andere Aspekte des *mobile*^{IoT} Services von ifm zurückzusetzen oder zu deaktivieren, mit Ausnahme der in diesem Agreement gestatteten Form, oder

e) versuchen, Urheberrechte, Marken und andere Angaben, die auf geistigem Eigentum von ifm oder anderen Aspekten des *mobile*^{IoT} Services erscheinen, unkenntlich zu machen oder zu entfernen.

7.2 Lizenzverifizierung

Auf Wunsch von ifm, übermittelt durch Mitteilung an den Kunden, jedoch nicht häufiger als einmal innerhalb von zwölf (12) Monaten ist ifm berechtigt, die Nutzung der CU-Firmware, der API-Anpassung und des ifm Services durch den Kunden, seine Tochtergesellschaften, seine Endkunden und deren Endnutzer sowie durch Dritte, denen der Kunde möglicherweise Zugang zu den Diensten gewährt hat, in einem Audit (vor Ort oder per Fernzugriff) zu überprüfen.

Ein solches Audit ist während der normalen Geschäftszeiten in Absprache mit dem Kunden durchzuführen und darf die Geschäftstätigkeit nicht unangemessen stören.

7.3 Nutzung der Maschinendaten

Vorbehaltlich eingeschränkten Lizenzen und Rechte, die dem Kunden gemäß Abschnitt 7.1 gewährt werden, ist ifm berechtigt, die erfassten Maschinendaten in anonymisierter Form zu nutzen, um seine Produkte und Dienstleistungen zu verbessern sowie zu Marketingzwecken. Dieser Abschnitt 7.3 gilt auch nach der Beendigung dieses Agreements fort.

8. Entschädigung

8.1 Freistellung des Kunden

ifm hat den Kunden und seine verbundenen Unternehmen zu entschädigen, zu verteidigen und schadlos zu halten in Bezug auf sämtliche Kosten und Schäden, die dem Kunden endgültig auferlegt werden wegen eines direkten Verstoßes gegen das Recht auf geistiges Eigentum eines Dritten speziell bei Nutzung des ifm Services **(„Verletzung des geistigen Eigentums“),** unter der Bedingung, dass (a) der Kunde ifm unverzüglich schriftlich über die geltend gemachte Verletzung des geistigen Eigentums informiert, (b) der Kunde es ifm überlässt, nach eigenem Ermessen eine angemessene Verteidigungsstrategie zu verfolgen und alle damit verbundenen Verhandlungen zur Beilegung der Angelegenheit zu führen, und (c) der Kunde mit ifm bei der Ergreifung der erforderlichen Verteidigungsmaßnahmen zusammenarbeitet (einschließlich, jedoch nicht beschränkt auf, die Bereitstellung sämtlicher Dokumente und Informationen für ifm, die sich im Besitz oder unter der Kontrolle des Kunden befinden und für die Verteidigung gegen die geltend gemachte Verletzung des geistigen Eigentums relevant sind, und indem der Kunde dafür sorgt, dass sein Personal als Zeuge auftritt oder der Kunde sich mit ifm bzw. dessen Rechtsanwälten im Zusammenhang mit einer solchen Verteidigung entsprechend berät).

ifm ist jedoch nicht verantwortlich für Verletzungen des geistigen Eigentums, die beruhen auf (a) Veränderungen an den CUs, die von Personen vorgenommen werden, bei denen es sich nicht um ifm oder dessen verbundene Unternehmen handelt, (b) einer Nutzung des ifm *mobile*^{IoT} Services, die außerhalb des Umfangs der eingeschränkten Lizenzen und Rechte liegt (c) einer Nutzung der Anwendungen, Technologien oder Vermögenswerten des ifm *mobile*^{IoT} Services durch den Kunden in einer Weise, die nichtautorisierte Rechte auf geistiges Eigentum eines Dritten nutzt, und (d) Ansprüchen, die auf einer Verletzung der im Abschnitt 5.1 dargelegten Zusicherungen und Gewährleistungen des Kunden oder anderer Bereiche in der Verantwortung des Kunden gemäß den Abschnitten 4.5, 5.2, 5.3, 6.1 und/oder 9.3 beruhen („**Kundenverantwortlichkeiten**“).

Darüber hinaus kann ifm nach alleinigem Ermessen und auf seine Kosten eine der folgenden Maßnahmen ergreifen, um Forderungen bezüglich der Verletzung des geistigem Eigentums zu mildern und/oder beizulegen: (a) Austausch oder Änderung von Aspekten des ifm *mobile*^{IoT} Services, um dafür zu sorgen, dass dadurch kein Verstoß mehr begangen wird, (b) Beschaffung einer Lizenz für den Kunden zur Nut-

zung der Rechte, die vermeintlich verletzt werden, oder (c) Einstellung des *mobile*^{IoT} Services bei gleichzeitiger Erstattung bereits bezahlter Gebühren. Die oben aufgeführten Maßnahmen sind die einzigen Rechtsmittel, auf die der Kunde einen Anspruch hat, und die einzigen Verpflichtungen und Haftungspflichten, die ifm bei einem Verstoß gegen geistiges Eigentum zu übernehmen hat.

8.2 Entschädigung von ifm

Der Kunde hat ifm und seine verbundenen Unternehmen von allen Schäden, Kosten, verlorenen, offengelegten oder beschädigten Maschinendaten oder anderen Daten, entgangenen Gewinnen, angemessenen Anwaltskosten und Haftung freizustellen, einschließlich aller Ansprüche, die ifm -Mitarbeiter oder andere Dritte wegen Tod, Körperverletzung oder Schäden an materiellem oder immateriellem Vermögenswerten haben, die sich aus der Nutzung oder dem Betrieb des ifm *mobile*^{IoT} Services ergeben, wenn Schäden resultieren oder zurückzuführen sind auf:

a) Kundenverursachte Verletzungen des geistigen Eigentums;

b) Verstöße des Kunden, seiner Endkunden und/oder deren Endnutzer gegen die Bestimmungen der Abschnitte 7.1 oder 9 dieses Agreements oder der Endnutzungsvereinbarung;

c) Bereiche, die in die Verantwortung des Kunden, gemäß Abschnitt 5.1 fallen;

d) die Nutzung des ifm *mobile*^{IoT} Services durch nicht lizenzierte Benutzer, die Zugang zu dem ifm *mobile*^{IoT} Services über die von ifm dem Kunden bereitgestellten Zugangsschlüssel erlangt haben, mit Ausnahme in der in Abschnitt 2.2 aufgeführten Form; oder

e) alle Ansprüche, die Endkunden oder ihre Endnutzer gegen ifm geltend machen, einschließlich Forderungen wegen etwaiger Ausfälle oder Fehler der Services, der CU oder der Maschine.

9. Vertraulichkeit/Datenschutz

9.1 Vertraulichkeit

Beide Parteien unternehmen größtmögliche Anstrengungen, damit keine Geschäftsgeheimnisse und vertraulichen Informationen der anderen Partei während der Laufzeit dieses Agreements und während eines Zeitraums von fünf (5) Jahren im Anschluss daran an andere weitergegeben werden. Das gesamte geistige Eigentum von ifm, mit Ausnahme der Marke ifm, das dem Kunden seitens ifm zur Verfügung gestellt wird, gilt als vertrauliche Informationen und darf weder ganz noch teilweise Dritten mitgeteilt werden, sofern dies nicht ausdrücklich im Rahmen dieses Agreements erlaubt ist.

Keine der Parteien ist verpflichtet, Informationen vertraulich zu behandeln, die öffentlich bekannt sind oder werden, ohne dass diesbezüglich seitens der betreffenden Partei ein Fehler oder ein Versäumnis begangen wurde, bzw. die dieser Partei bereits bekannt waren, die seitens einer dritten Partei unabhängig entwickelt oder die im Rahmen eines rechtmäßigen Gerichts- oder Behördenverfahrens offengelegt wurden.

9.2 Datenschutzerklärung

Die Nutzung und der Schutz der personenbezogenen Daten des Kunden und seiner Endkunden sowie deren Endnutzer durch ifm unterliegt dem als Anlage 5 beigefügten Auftragsverarbeitungsvertrag (AVV).

9.3 Einhaltung der Datenschutzbestimmungen

Der Kunde versteht und stimmt zu, dass es die Verpflichtung des Kunden ist, alle Datenschutzgesetze und -vorschriften einzuhalten, die für Transaktionen des Kunden und andere im Rahmen dieses Agreements durchgeführte Handlungen gelten, einschließlich derjenigen, die sich auf die Endkunden und ihre Endnutzer beziehen.

10. Geltende ifm Richtlinien

Verhaltenskodex von ifm

Der Kunde ist verpflichtet, den als Anlage 3 beigefügten ifm Verhaltenskodex einzuhalten und auf die Einhaltung der Bestimmungen, die den des Verhaltenskodexes entsprechen, bei seinen Tochtergesellschaften, autorisierten Vertriebspartnern, Endkunden und deren Endnutzern hinzuwirken.

11. Kündigung

11.1 Laufzeit

Sofern dieses Agreement nicht, wie hierin vorgesehen, vorzeitig gekündigt wird, beginnt es am Tag des Inkrafttretens und dauert zunächst zwei (2) Jahre ("**Erstlaufzeit**") und verlängert sich danach automatisch jeweils um ein weiteres Jahr ("**Verlängerungszeitraum**", beide Laufzeiten werden zusammen als "Laufzeit" bezeichnet), es sei denn, eine Partei teilt der anderen ihre Absicht, das Agreement nicht zu verlängern, mindestens drei (3) Monate vor dem Ende der Laufzeit mit.

11.2 Kündigung im Falle wesentlicher Verstöße

Jede Partei kann dieses Agreement und die Anlagen bei einem wesentlichen Verstoß der anderen Partei gegen die Bestimmungen und Beschränkungen dieses Agreements oder seiner Anlagen dreißig (30) Tage nach Zustellung einer schriftlichen Mitteilung über einen wesentlichen Verstoß und einer bevorstehenden Kündigung an die andere Partei, die die Art der Verletzung des Agreements angibt, kündigen. Wird dieser wesentliche Verstoß innerhalb von dreißig (30) Tagen nach Erhalt der Mitteilung über den Verstoß und die bevorstehende Kündigung behoben, so werden dieses Agreement und alle Anlagen nicht beendet und bleiben umfassend in Kraft und wirksam.

Eine "wesentlicher Verstoß", auf den hierin Bezug genommen wird, umfasst ohne Einschränkung Folgendes:

a) das Versäumnis des Kunden, eine Rechnung von ifm gemäß den Zahlungsbedingungen zu bezahlen;

b) jede Verletzung von Abschnitt 8.1 dieses Agreements durch den Kunden, seine Endkunden oder deren Endnutzer;

c) jeder Verstoß seitens einer Partei gegen ihre Vertraulichkeitsverpflichtung, wie in Abschnitt 10 dieses Agreements festgelegten ist;

d) jedes Versäumnis des Kunden, ifm auf Verlangen gemäß Abschnitt 9.2 der Vereinbarung rechtmäßig freizustellen.

11.3 Kündigung durch ifm

ifm ist darüber hinaus berechtigt, dieses Agreement und die Anlagen jederzeit durch schriftliche Mitteilung über die sofortige Kündigung an den Kunden zu beenden:

a) wenn der Kunde einen Antrag auf Eröffnung eines Insolvenzverfahrens oder vergleichbaren Verfahrens wegen Zahlungsunfähigkeit oder Überschuldung eingereicht hat;

b) im Falle des Vorliegens einer Entscheidung, wonach der Kunde überschuldet, zahlungsunfähig oder insolvent ist;

c) wenn der Kunde rechtliche Schritte eingeleitet hat oder Dokumente eingereicht hat, die eine Umstrukturierung, Reorganisation oder sonstige Geschäfte des Kunden betreffende Vereinbarung bezüglich Zahlungsunfähigkeit oder Überschulung beinhalten;

d) der Bestellung eines Zwangsverwalters oder eines nach geltendem Recht vergleichbaren Verwalters für alle oder wesentliche Vermögenswerte des Kunden;

e) der Abtretung des Kunden zugunsten von Gläubigern;

f) der Einleitung eines Verfahrens zur Liquidation oder Auflösung des Kunden oder zur Beendigung seiner Gesellschafts- oder Unternehmensverträge;

g) wenn alle Vermögenswerte oder ein wesentlicher Teil der Vermögenswerte des Kunden an einen Dritten übertragen werden.

11.4 Rechtsfolgen der Kündigung

Bei Beendigung dieses Agreements aus beliebigem Grund gilt Folgendes:

a) Außer in dem in Abschnitt 11.4(f) unten geregelten Fall werden alle Anlagen des Agreements, alle ausstehenden Abonnements und alle Lizenzen oder Rechte, die auf der Grundlage dieses Agreements gewährt wurden, automatisch und gleichzeitig ohne weitere Mitteilung beendet;

b) Außer in dem in Abschnitt 11.4(f) unten geregelten Fall sind der Kunde, seine Endkunden und deren Endnutzer verpflichtet, die Nutzung des geistigen Eigentums von ifm, aller anderen Aspekte des ifm *mobile*^{IoT} Services und aller anderen vertraulichen Informationen von ifm unverzüglich einzustellen und alle Kopien derselben an ifm zurückzugeben, die sich in seinem Besitz befinden, oder ifm anderweitig einen zufriedenstellenden Nachweis ihrer Zerstörung in Form einer eidesstattlichen Versicherung zu erbringen

c) Außer in dem in Abschnitt 11.4(f) unten geregelten Fall sind der Kunde, seine Endkunden und deren Endnutzer verpflichtet, die Nutzung der CU-Firmware und API-Anpassungen sowie der von ifm bereitgestellten SIM-Karten unverzüglich einzustellen;

d) Der Kunde hat für jede Kündigung dieses Agreements gemäß den Abschnitten 11.2 oder 11.3, sofern die Beendigung nicht durch eine „wesentliche Verletzung des Agreements“ durch ifm veranlasst wurde, an ifm eine Stornierungsgebühr zu zahlen, die der Höhe von Abonnementgebühren für (i) zwölf (12) Monate oder (ii) den Rest der Laufzeit entspricht, je nachdem, welcher Zeitraum kürzer ist; und

e) werden alle noch nicht bezahlten Kosten, zusätzlichen Kosten und Kosten für eine vorzeitige Stornierung, die sich aus der Kündigung des mobilen Kommunikationsdienstes ergeben, unverzüglich fällig und sind seitens des Kunden an ifm zu zahlen.

f) Wenn dieses Agreement aus einem anderen Grund als durch ifm gemäß Abschnitt 11.2 oder 11.3 gekündigt wird und der Kunde alle Gebühren gemäß Abschnitt 11.4(d) und (e) bezahlt hat (einschließlich der Gebühren für ausstehende Abonnements) werden alle ausstehenden Endkunden Abonnements nach Beendigung des Agreements bis zum Ende der jeweils aktuellen Laufzeit fortgesetzt, wobei am Ende der Laufzeit (i) jedes Endkunden Abonnement automatisch und unwiderruflich ohne Verlängerungsmöglichkeit abläuft, (ii) die entsprechende SIM-Karte automatisch und unwiderruflich deaktiviert wird und (iii) alle entsprechenden Maschinendaten für diesen Endkunden nach dreißig (30) Tage ohne vorherige Ankündigung gelöscht werden.

11.5 Fortbestehende Klauseln

Die Abschnitte 4.5, 4.6, 5.3, 6-10, 11.4, 11.5 und 12.3 des Agreements gelten auch nach der Beendigung dieses Agreements und der Beendigung einer im Rahmen dieses Agreements gewährten Lizenz oder eines eingeräumten Rechts fort.

12. Streitschlichtung

12.1 Support

Der Supportdienst von ifm und dem Kunden sollen sich bemühen, Meinungsverschiedenheiten beizulegen. Wenn eine Meinungsverschiedenheit durch den Support nicht beigelegt werden kann, soll die Streitigkeit eskaliert und intern gemäß Abschnitt 12.2 beigelegt werden.

12.2 Interne Streitbeilegung

Keine der Parteien kann gegen die andere Partei in Bezug auf Fragen im Zusammenhang mit dieser Vereinbarung oder ihren Anlagen Klage erheben, bis die Parteien die folgenden Verfahren ausgeschöpft haben:

a) Ist eine Partei der Ansicht, dass eine Streitigkeit im Rahmen dieses Agreements oder seiner Anlagen vorliegt, kann sie die andere Partei über die Streitigkeit informieren. In der Mitteilung muss die Art der Streitigkeit angegeben werden;

b) Innerhalb von zehn (10) Tagen nach Erhalt einer Mitteilung über eine Streitigkeit müssen ein General Manager / Hauptabteilungsleiter jeder Partei zusammentreffen und in gutem Glauben versuchen, den Streit beizulegen.

c) Wenn die Streitigkeit nicht durch die in Abschnitt 12.2(b) vorgeschriebene Sitzung beigelegt wird und zehn (10) Tage nach der Mitteilung über die Streitigkeit vergangen sind, haben die jeweiligen Geschäftsführer jeder Partei innerhalb von dreißig (30) Tagen zusammenzutreffen und in gutem Glauben zu versuchen, den Streit beizulegen.

d) Alle Verhandlungen gemäß dieser Klausel sind vertraulich und werden als Kompromiss- und Vergleichsverhandlungen behandelt.

Die interne Streitbeilegung soll nur dann genutzt werden, wenn sie für beide Parteien notwendig und angemessen erscheint. Dies ist im jeweiligen Einzelfall zu bewerten.

12.3 Externe Streitbeilegung

Wenn die Streitigkeit nicht innerhalb von vierzig (40) Tagen nach Mitteilung über die Streitigkeit gemäß Abschnitt 12.2 intern beigelegt wurde, kann jede Partei eine gerichtliche Entscheidung beantragen. Alle Rechtsstreitigkeiten, die sich aus oder im Zusammenhang mit diesem Agreement oder seinen Anlagen ergeben, werden ausschließlich vor dem Landgericht geführt, an dem die ifm ihren Sitz hat.

12.4 Anwendbares Recht

Auf dieses Agreement ist das Recht des Landes anzuwenden, in dem die ifm ihren Sitz hat. Die Anwendung des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf vom 11.04.1980 (UN-Kaufrecht) wird ausgeschlossen.

13. Allgemeines

13.1 Subunternehmer

ifm kann zur Erfüllung aller oder eines Teils seiner Pflichten aus dem vorliegenden Agreement einen oder mehrere Subunternehmer einsetzen.

13.2 Kein Joint Venture

Die Bestimmungen in diesem Agreement oder seinen Anlagen dürfen weder so ausgelegt werden, dass zwischen den Parteien ein Joint-Venture, eine Partnerschaft oder ein Arbeitsverhältnis begründet wird, noch hat eine Partei das Recht, die Vollmacht oder die Befugnis, ausdrücklich oder stillschweigend im Namen der jeweils anderen Partei Verpflichtungen einzugehen.

13.3 Keine Abtretung

Die Parteien sind nicht befugt, Rechte aus diesem Agreement und seinen Anlagen zu übertragen oder Pflichten, die im Rahmen dieses Agreements bestehen, zu delegieren, ohne diesbezüglich die vorherige schriftliche Zustimmung der anderen Partei einzuholen; unter der Voraussetzung jedoch, dass ifm dieses Agreement und seine Anlagen ohne eine solche Einwilligung an eine dritte Partei übertragen darf, die das geistige Eigentum von ifm oder im Wesentlichen das gesamte Vermögen von ifm erwirbt. Eine Übertragung oder Delegierung von Pflichten unter Verstoß gegen Abschnitt 13.3 dieses Agreements ist nichtig.

13.4 Höhere Gewalt

Keine der Parteien haftet für die Nichterfüllung ihrer Verpflichtungen aufgrund eines Ereignisses höherer Gewalt.

13.5 Mitteilungen

Alle Benachrichtigungen, Anfragen, Forderungen, Ansprüche oder sonstigen Mitteilungen, die im Rahmen dieses Agreements erforderlich sind, bedürfen der Schriftform und werden entweder zugesandt per Post oder Einschreiben an die Geschäftsadresse der betroffenen Partei bzw. per E-Mail an info.mobileiot@ifm.com.

13.6 Verzicht

Das Versäumnis einer Partei, Rechte aus diesem Agreement oder seinen Anlagen geltend zu machen, gilt nicht als Verzichtserklärung oder Verzicht auf diese Rechte.

13.7 Salvatorische Klausel

Wenn Bedingungen oder Bestimmungen dieses Agreements sich als unrechtmäßig oder nicht durchsetzbar erweisen, wird dadurch die Gültigkeit oder Durchsetzbarkeit des übrigen Agreements nicht beeinträchtigt.

13.8 Schlussbestimmungen

Dieses Agreement und seine Anlagen bilden die Gesamtheit der Vereinbarungen zwischen ifm und dem Kunden und ersetzen (mit Ausnahme eines bereits wirksam abgeschlossenen NDA) alle früheren oder aktuellen Mitteilungen, Erklärungen oder Vereinbarungen zwischen den Parteien, unabhängig davon, ob diese mündlich oder schriftlich vorgenommen wurden/werden, einschließlich, jedoch nicht beschränkt auf alle Angebote, Vorschläge, E-Mails, Broschüren oder Informationen auf Internetseiten bezüglich des Gegenstandes dieses Agreements oder seiner Anlagen. Die Geschäftsbedingungen des

Kunden (einschließlich solcher, die auf der Rückseite einer Bestellung oder einem Anhang zu einer Bestellung erscheinen, ob in Bezug auf eine Zahlung oder anderweitig) finden keine Anwendung. Im Falle eines Konflikts zwischen den Bedingungen dieses Agreements und seiner Anlagen haben die Bestimmungen der folgenden Dokumente Vorrang in der Reihenfolge ihrer Auflistung:

(a) dieses Agreement, (b) die in Abschnitt 10 genannten ifm Richtlinien und (c) spezielle Angebote, die über dieses Agreement hinausgehen. Dieses Agreement und alle Anlagen dürfen nur durch eine schriftliche Änderung geändert werden, die von einem bevollmächtigten Vertreter jeder Partei unterzeichnet wurde.

ANLAGEN

Anlage 1 – **Zusätzliche SIM-Geschäftsbedingungen**

Anlage 2 – **Produktbeschreibung**

Anlage 3 – **ifm Verhaltenskodex**

Anlage 4 – **Enduser-Agreement (EUA)**

Anlage 5 – **Auftragsverarbeitungsvertrag (AVV)**

Anlage 1

“Zusätzliche SIM-Geschäftsbedingungen”

Diese zusätzlichen SIM-Geschäftsbedingungen (ZSB) ergänzen das mIoT Agreement. Sie gelten für die Mobilfunkdienste für Machine-to Machine (M2M) – und mobile Internet of Things (*mobile*^{IoT}) – Anwendungen und die zugehörigen weiteren Dienste (nachfolgend zusammen auch die „Leistungen“ genannt), die der Kunde von der ifm electronic gmbh§ 15 FAO (nachfolgend ifm) bestellt hat.

1. Definitionen

"Konzerngesellschaft" bezeichnet sämtliche Konzerngesellschaften des Kunden.

„Angeschlossene Netzwerke" bezeichnen fremde Mobilfunknetze, in denen die M2M-Dienste genutzt werden.

"Anschlussdienste" bezeichnen die M2M-Dienstleistungen von ifm.

"Endnutzer" bezeichnet die Nutzer einer SIM zu eigenen Zwecken, ohne Wiederverkäufer zu sein.

"Geräte" bezeichnen alle Geräte, in denen von ifm gem. diesen Bedingungen bereitgestellte SIM`s genutzt werden.

"Ereignis höherer Gewalt" bezeichnet ein Ereignis, das außerhalb des Einflussbereichs einer Vertragspartei (oder einer in deren Namen handelnden Personen liegt, von seiner Natur her für eine solche Vertragspartei (oder eine solche Person) nicht voraussehbar oder verhinderbar war, wobei dieser Begriff ohne Anspruch auf Vollständigkeit folgendes beinhaltet: Naturereignisse, Stürme, Flutkatastrophen, Aufstände, Brände, Sabotageakte, zivile Aufstände oder Unruhen, Eingreifen ziviler oder militärischer Behörden, Kriegshandlungen (ob erklärt oder nicht) oder bewaffnete Konflikte terroristischer Handlungen oder Versagen der Energiequellen.

"BNetzA" = Bundesagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen.

"Plattform " bezeichnet die globale M2M-Datendienstplattform.

"SIM" = eine dem Kunden im Rahmen dieser Anlage zur Verfügung gestellte Global M2M SIM.

"Vertragsgebiet" bezeichnet das Vertragsgebiet in Deutschland; andere Länder mit Roamingpartnern, sofern vereinbart.

"ifm Konzern-(gesellschaft)“ bezeichnet sämtliche Konzerngesellschaften der ifm Stiftung & Co. KG.

2. Leistungen

ifm erbringt folgende Leistungen:

- die Überlassung eines an die korrespondierende Hardware gebundenen Mobilfunkanschluss für M2M/mIoT-Anwendungen, mit dem der Kunde Daten-Mobilfunkverbindungen und weitere Netz- und Netzserviceleistungen nutzen kann – dies erfolgt durch die Bereitstellung der in der Hardware codierten SIM. Die SIM ist mit der Hardware verbaut; den Mobilfunkanschluss sowie die Netz- und Netzserviceleistung darf der Kunde ausschließlich mit der Hardware nutzen.
- Sämtliche Leistungen im Sinne dieser ZSB gelten unter dem Vorbehalt deren ausschließlicher Nutzung des Kunden in Kombination mit der Hardware.
- ifm stellt die Leistungen im Sinne dieser ZSB im Rahmen ihrer technischen und betrieblichen Möglichkeiten zur Verfügung. Die vorgenannten Mobilfunkverbindung erfolgt jeweils auf der Grundlage von Vorleistungen lizenzierter Mobilfunknetzbetreiber.

ifm steht es insoweit frei, sich jederzeit ohne die vorherige Zustimmung des Kunden für die Vertragserfüllung Dritter zu bedienen.

3. Nutzung der Dienste durch den Kunden

3.1 Der Kunde wird die Dienste nur für den Vertragszweck innerhalb des Vertragsgebietes in Übereinstimmung mit diesen Bedingungen nutzen. Er sorgt zugleich für die Einhaltung der vertraglichen Vorgaben bei seinen Endkunden, sofern der Vertragszweck auch die Weitergabe der Dienste an seine Endkunden umfasst.

3.2 Der Kunde wird die Dienste nur für den Vertragszweck innerhalb des Vertragsgebietes in Übereinstimmung mit diesen Bedingungen nutzen. Er sorgt zugleich für die Einhaltung der vertraglichen Vorgaben bei seinen Endkunden, sofern der Vertragszweck auch die Weitergabe der Dienste an seine Endkunden umfasst.

3.3 Der Kunde wird dafür sorgen, dass die im Rahmen dieser Bedingungen bereitgestellten Dienste von ihm selbst und seinen Endnutzern nur für den Vertragszweck und nicht auf irgendeine Art und Weise genutzt wird, die:

a) die Bereitstellung von Diensten über die Anschlussdienste beinhaltet, die einem Endnutzer – einschließlich über einen Proxy Server, einen Gateway oder einen Router- den Zugriff auf ein öffentlich aufrufbares Ziel (d.h. auf eine öffentliche IP-Adresse) ermöglicht, es sei denn, die Nutzung der öffentlichen IP-Adresse geschieht zu Zwecken der Konfiguration und effizienten Nutzung der M2M-Dienste gemäß dieser Bedingungen;

b) zu einer Verletzung von Urheberrechten, Warenzeichen, Geschäftsgeheimnissen oder anderen geistigen Eigentumsrechten eines Dritten führen würde;

c) die Nutzung eines Netzwerkes durch andere Nutzer stören oder zu einer Überwindung von Sicherheitsmaßnahmen führen würde, unabhängig davon, ob dieser unerlaubte Zugriff zur Verfälschung oder zum Verlust von Daten führt;

d) eine Gefahr für Leib, Leben und Gesundheit Dritter bedeuten können sowie zu Umweltschäden führen können.

e) Ungeachtet Ziffer 3.4 (e) ist der Kunde berechtigt, seine eigenen, die SIMs beinhaltenden Produkte, an Endnutzer zu verkaufen, sofern diese im Vertragszweck zwischen den Parteien vereinbart wurde.

3.4 Der Kunde wird es unterlassen und seine Endnutzer dazu verpflichten, es ebenfalls zu unterlassen:

a) die Dienste oder die SIM´s zu modifizieren, anzupassen, zu verändern, zu übersetzen, oder abgeleitete Werken daraus zu erstellen;
b) die SIM´s zusammen mit anderer Hardware, Software, Produkten oder Diensten zusammenzufügen oder gemeinsam zu verwenden, die nicht mit dem Zweck der Bedingungen in Einklang stehen oder nicht ausdrücklich von ifm genehmigt wurden;
c) über die SIM´s Unterlizenzen zu vergeben, diese zu verleasen, zu vermieten, zu verleihen oder sonst wie an Dritte zu übertragen, es sei denn, es handelt sich bei diesen Dritten um Endnutzer;
d) die SIM´s oder auf den SIM´s laufende Software zurückzuentwickeln, zu dekompilieren, zu disassemblieren oder sonst wie zu versuchen, deren Quellcode oder Objektcode zu ermitteln;
e) die Dienste weiterzuverkaufen oder zu nutzen, um Dienste für Dritte bereitzustellen oder Dritten zu gestatten, per Fernzugriff auf die Dienste zuzugreifen oder die SIM´s zur Entwicklung von den SIM´s ähnlichen Produktlinien zu verwenden (oder eine solche Verwendung zuzulassen), es sei denn, dies entspricht dem Vertragszweck und ist zwischen den Parteien vereinbart;
f) die SIM´s für andere Zwecke als für die Dienste im Zusammenhang mit dem Zweck der Bedingungen und die ausdrücklich schriftlich mit ifm vereinbarten Anwendungen zu nutzen.

3.5 Der Kunde wird alle für die Nutzung der Dienste auf seiner Seite erforderlichen Genehmigungen (inkl. einer etwaigen Registrierung bei der BNetzA) einholen.

4. Dynamische Updates der SIM`s

ifm behält sich das Recht vor, auf beliebigen Wegen Updates oder Upgrades durchzuführen. Diese Updates oder Upgrades dürfen die Funktionalität der SIMs nicht wesentlich nachteilig beeinflussen.

5. Verbindungsdienste

5.1 ifm stellt sicher, dass dem Kunden in jedem der Vertragsgebiete M2M-Dienstleistungen zur Nutzung in den angeschlossenen Netzwerken zur Verfügung stehen.

5.2 ifm behält sich das Recht vor, die Liste der angeschlossenen Netzwerke entsprechend der Änderungen der wirtschaftlichen und rechtlichen Rahmenbedingungen zu modifizieren. Dabei wird ifm die Interessen des Kunden dahingehend berücksichtigen, dass eine Änderung des Leistungsspektrums bei National Roaming während der Laufzeit der vertraglichen Vereinbarungen möglichst un-

terbleibt. Zugleich erkennt der Kunde an, dass a) die Bereitstellung bestimmter Netzwerk-Technologien zur Erbringung der Anschlussdienste auch vor Beendigung der Bedingungen enden kann oder b) bestehende Netzwerk-Technologien im Rahmen der Netzmodernisierung durch andere Netzwerk-Technologien ersetzt werden können. Dementsprechend wird der Kunde dafür sorgen, dass die von ihm eingesetzte Hardware jeweils mit den eingesetzten Netzwerk-Technologien kompatibel ist.

5.3 Der Kunde wird auf Anweisung von ifm die Freischaltung einer SIM aussetzen, wenn diese so manipuliert wurde, dass die Abrechnungsinformationen dadurch ungenau werden.

5.4 Zur Vermeidung von Unterbrechungen von M2M Anwendungen im Ausland werden für die vertragsgegenständlichen M2M-Karten standardmäßig keine Höchstbeträge für Datenroaming entsprechend der EG-Verordnung 544/2009 eingerichtet. Der Kunde wünscht keine automatischen Tarifinformationen oder Meldungen über das verbrauchte Nutzungsvolumen.

6. Geistiges Eigentum

„Geistige Eigentumsrechte“ bezeichnen Patente, eingetragene und nicht eingetragene Handels- und Dienstleistungsmarken, eingetragene Muster und Musterrechte, Urheberrechte (einschließlich solcher Rechte an Computersoftware und Datenbanken) und Datenbankrechte.

6.1 Der Kunde erkennt an, dass alle Eigentumsrechte an den Diensten sowie an allen Dokumenten, Daten und darin enthaltenen Spezifikationen ausschließliches Eigentum von ifm (und/oder von deren Lizenznehmern) bleiben und dass dem Kunden außer den in diesen Bedingungen festgelegten Rechten keinerlei diesbezügliche Rechte zukommen. Soweit der Kunde (jetzt oder in der Zukunft) geistige Eigentumsrechte an den Diensten oder bezüglich derselben erwirbt, tritt der Kunde alle solchen geistigen Eigentumsrechte an ifm ab.

6.2 Der Kunde erkennt an, dass keine Nutzung der SIM in Kombination mit einem anderen, nicht von ifm zur Verfügung gestellten Produkt erfolgt, bei der die Kombination von SIM und Produkt eine Verletzung der geistigen Eigentumsrechte Dritter darstellt.

6.3 ifm gewährt dem Kunden für die Laufzeit des mIoT Agreements bzw. bis zum Ende des längstlaufenden Einzelvertrages ein unentgeltliches, nicht ausschließliches Recht, die geistigen Eigentumsrechte für den Vertragszweck zu nutzen.

6.4 Der Kunde erkennt an, dass er zur Anmeldung gewerblicher Schutzrechte an geistigen Eigentumsrechten gemäß 6.1 nicht berechtigt ist.

7. Datenschutz

7.1 Die Parteien erkennen an, dass der Kunde, hinsichtlich des Inhalts jeglicher über die Anschlussdienste erfolgender Kommunikation sowie hinsichtlich von allen gespeicherten personenbezogenen Daten des Kunden oder des Endnutzers (der „personenbezogenen Daten des Kunden“) der für die Verarbeitung Verantwortliche ist. ifm wird hinsichtlich aller für Kunden verarbeiteten personenbezo-

genen Daten angemessene und ausreichende Sicherheitsmaßnahmen organisatorischer und technischer Art ergreifen, um diese personenbezogenen Daten des Kunden vor zufälliger oder widerrechtlicher Vernichtung oder zufälligem Verlust, Beschädigung, Änderung sowie unerlaubter Offenlegung oder Zugriff zu schützen.

7.2 Der Kunde erkennt an, dass ifm rechtlich verbindliche Aufforderungen von Behörden zur Offenlegung personenbezogener Daten des Kunden erhalten kann oder aufgrund eines Gesetzes oder einer gerichtlichen Anordnung verpflichtet sein kann, personenbezogene Daten des Kunden gegenüber anderen Personen als dem Kunden offenzulegen. ifm wird den Kunden rechtzeitig über solche Forderungen unterrichten, es sei denn, es bestehen anderweitige entsprechende Verbote wie etwa strafrechtlich begründete Verbote zur Wahrung der Vertraulichkeit im Rahmen eines Ermittlungsverfahrens

7.3 Der Kunde gewährleistet, dass er:

a) als für die Verarbeitung Verantwortlicher hinsichtlich der personenbezogenen Daten des Kunden alle anwendbaren Datenschutzgesetze einhalten wird; und
b) bei einer entsprechenden Verpflichtung im Rahmen des anwendbaren Datenschutzrechtes alle Endnutzer darüber informieren oder erforderlichenfalls das informierte Einverständnis der Endnutzer dafür einholen wird, dass ifm (oder ein Anspruch genommener Auftragsverarbeiter) die personenbezogenen Daten des Kunden für den Zweck der Bereitstellung der Dienste verarbeiten wird.

7.4 Falls nach dem anwendbaren Datenschutzrecht das Einverständnis des Endnutzers oder Kunden erforderlich ist und ein solches Einverständnis verweigert und/oder zurückgezogen wird und der Kunde in Bezug auf einen oder mehrere Endnutzer nicht anderweitig belegen kann, dass die Offenlegung und Verarbeitung von personenbezogenen Daten hinsichtlich eines oder mehrerer Endnutzer gemäß 7.4 gefordert mit dem geltenden Datenschutzrecht in Einklang steht, wird der Kunde ifm umgehend darüber in Kenntnis setzen. Der Kunde erkennt an, dass ifm ungeachtet sonstiger Bestimmungen dieses Vertrages in diesem Fall nicht zu einer weiteren Bereitstellung der Dienste hinsichtlich der betreffenden Endnutzer verpflichtet ist.

8. Vertraulichkeit

8.1 Diese Bedingungen sind vertraulich und dürfen nur mit vorheriger schriftlicher Genehmigung der anderen Partei Dritten gegenüber offengelegt werden. Jeder der Parteien ist sich bewusst, dass ihr aufgrund des Vertrages öffentlich nicht frei verfügbare Informationen über die andere Partei, ihre Mitarbeiter, Lieferanten oder dritte Subunternehmer mitgeteilt werden können, einschließlich von, aber nicht beschränkt auf Informationen bezüglich Preisen, Prozessen, finanziellen Daten, Statistiken, zukünftigen und aktuellen Produkten und aktuellen Diensten oder damit zusammenhängende Informationen (vertrauliche Informationen). Die in Empfang nehmende Partei darf vertrauliche Informationen (außer in dem für den Vertragszweck erforderlichen Umfang) nur mit vorheriger schrift-

licher Zustimmung der offenlegenden Partei anderen Personen, Firmen oder Unternehmen gegenüber offenlegen, für eigene Zwecke verwenden oder kopieren, anpassen oder sonst wie wiedergeben.

8.2 Ziffer 8.1 findet nicht auf vertrauliche Informationen Anwendung, die:

a) auf einem anderen Wege als durch eine Verletzung von Ziff. 10.1 öffentlich frei verfügbar werden;
b) von einem Dritten zur Verfügung gestellt werden, der diese regelmäßig erworben hat und nicht zur Vertraulichkeit verpflichtet ist;
c) eine unabhängige Entwicklung der die Informationen in Empfang nehmenden Partei oder einer ihrer Konzerngesellschaften darstellen;
d) aufgrund eines Gesetzes, gegenüber einer staatlichen Regulierungsbehörde oder aufgrund von anwendbaren Börsenbestimmungen offengelegt werden müssen.

9. Exportkontrolle

Jeder Partei verpflichtet sich im Zusammenhang mit der Vertragsdurchführung

a) zur Einhaltung aller einschlägigen Gesetze in Bezug auf Ausfuhrkontrollen sowie der finanziellen und wirtschaftlichen Sanktionen der Europäischen Union, der Vereinigten Staaten von Amerika und anderen Ländern, die von Bedeutung für die vertraglichen Beziehungen der Parteien sind;
b) nicht wissentlich Handlungen vorzunehmen, die die andere Partei oder ein Mitglied der Partei zur Verletzung der einschlägigen Vorschriften veranlasst.

10. Verschiedenes

10.1 Änderungen der Bedingungen bedürfen der Textform. Dies gilt auch für die Aufhebung des Textformerfordernisses.

10.2 Keine der Vertragsparteien darf ihre Rechte und Pflichten im Rahmen dieser Bedingungen ohne die vorherige schriftliche Zustimmung der anderen (wobei diese nicht in unzumutbarer Weise verweigert oder hinausgezögert werden darf) abtreten, ausgenommen dass ifm ihre Rechte abtreten und Pflichten im Rahmen dieser Bedingungen an ein anderes Mitglied des ifm-Konzern abtreten, übertragen oder untervergeben darf und ifm die Bereitstellung der Dienste im Rahmen des normalen Geschäftsganges untervergeben darf, mit der Maßgabe, dass die Bestellung eines Subunternehmers ihn nicht von irgendwelcher Haftung im Rahmen dieser Bedingungen entbindet.

10.3 Sollte eine der vorstehenden Regelungen ganz oder teilweise unwirksam sein, bleibt die Wirksamkeit der übrigen Regelungen davon unberührt. Die Parteien werden kurzfristig eine Regelung treffen, die der unwirksamen Regelung möglichst nahe kommt.

Anlage 2

Produktbeschreibung ifm *mobile*^{IoT} Plattform

Die ifm *mobile*^{IoT} Plattform besteht aus mehreren Diensten, über die Maschinen mit der Plattform verbunden werden können, sowie aus der Umgebung und dem Frontend zu ihrer Verwaltung. Die verschiedenen zur Plattform gehörigen Dienste werden in diesem Dokument beschrieben.

ifm mobile^{IoT} M2M-Dienste - Konnektivität und Mobilfunk

Der Konnektivitätsdienst umfasst die Remote- und/oder Mobilfunkverbindung von der Maschine zur ifm *mobile*^{IoT} Plattform. Bei Einsatz der ifm *mobile*^{IoT} Hardware mit integrierter SIM-Karte kann der Kunde die von ifm bereitgestellte Telekommunikations- und Netzwerkinfrastruktur nutzen. Diese Infrastruktur ist so ausgelegt, dass der Telekommunikationskanal zwischen der ifm *mobile*^{IoT} Hardware und der ifm *mobile*^{IoT} Plattform nach dem neuesten Stand der Technik gesichert ist. Wenn Hardware ohne die integrierte SIM-Karte von ifm *mobile*^{IoT} eingesetzt wird, kann diese Sicherheit nicht gewährleistet werden.

Nach Aktivierung des Konnektivitätsdienstes über einen Vertrag kann die Hardware mit den Hosting-Diensten der ifm *mobile*^{IoT} Plattform verbunden werden. Die Aktivierung des Vertrages erfolgt im Frontend der ifm *mobile*^{IoT} Suite. Die Verbindung über Mobilfunkdienste ist gemäß der beigefügten **Liste der Länder und Mobilfunkpartner** zulässig und möglich.

ifm mobile^{IoT} Echtzeitdienste – Remote-Verbindung, Diagnose und Störungsbehebung

Anhand der Echtzeitdienste kann der Kunde unabhängig davon, ob die Mobilfunkdienste genutzt werden oder nicht, einen Point-to-Point Echtzeitkanal zwischen einem Arbeitsplatz (z. B. Laptop oder PC) und der Maschine einrichten. Je nach gewähltem Kanaltyp besteht über diesen Kanal ein direkter Zugang zu CAN-Bus(sen) und Ethernet-Netzwerk(en) der Maschinen und damit zu allen an eine dieser Schnittstellen angebundenen Komponenten. Durch Einrichtung eines solchen Kanals und Herstellung einer Verbindung zu den Komponenten der Maschine werden Diagnose und Störungsbehebung in Echtzeit aus der Ferne möglich. Der beim Einsatz der Echtzeitdienste anfallende Datenverkehr wird nicht gespeichert oder aufgezeichnet. Bei Nutzung der Mobilfunkdienste wird die Verbindungsdauer der Echtzeitdienste erfasst, die entweder Teil der Vertragsvereinbarung ist oder von ifm gesondert in Rechnung gestellt werden kann.

ifm mobile^{IoT} DataHosting-Dienste – Daten- und Cloud-Hosting

Im Rahmen der DataHosting-Dienste der ifm *mobile*^{IoT} Plattform können Maschinendaten verarbeitet, gespeichert oder in Bezug gesetzt werden. Das können entweder Daten sein, die während des Maschinenbetriebs erfasst und somit von der Maschine an die Plattform gesendet werden, oder Konfigurationsdateien, Software, Firmware oder Dateien sonstiger Art. Die gespeicherten Daten sind entweder über das ifm *mobile*^{IoT} DataPortal oder die bereitgestellten APIs für alle Anwender oder Accounts mit den entsprechenden Berechtigungen für die betreffenden Daten zugänglich. Alle übrigen Arten von Daten werden so lange gespeichert, bis entweder der Maschinenvertrag ausläuft oder die Kooperation zwischen dem Kunden und ifm endet. Daten dieser Art werden in der ifm *mobile*^{IoT} Suite gespeichert und stehen dadurch allen Anwendern mit den entsprechenden Berechtigungen zur Verfügung.

Die Dateien und Daten jeglicher Art werden in der Domain des Kunden gespeichert, so dass nur mit den entsprechenden Berechtigungen darauf zugegriffen werden kann.

ifm mobile^{IoT} Suite – Managementportal

Die ifm *mobile*^{IoT} Suite ist das cloudbasierte Managementportal, das dem Kunden die Verwaltung der ifm *mobile*^{IoT} Plattform mit Schwerpunkt auf der Maschinenflotte des Kunden ermöglicht. Die ifm *mobile*^{IoT} Suite besteht aus den zwei Hauptfunktionen Asset-Management und Tooling.

Im Bereich Asset-Management kann Folgendes verwaltet werden:

- Accounts und Anwender, die in - verschiedenen Teilen - der ifm *mobile*^{IoT} Plattform zugelassen sind
- Organisationshierarchie
- Maschinen, ihre zugehörigen Komponenten und deren Konfigurationen
- Maschinen- oder Plattformverträge können voraktiviert, aktiviert und gekündigt werden

Im Bereich Tooling stehen dem Anwender oder Entwickler der Maschinen Tools zur Verfügung, mit denen sich Maschinenkonfigurationen einfach erstellen lassen oder die Maschine über die ifm *mobile*^{IoT} M2M-Dienste sogar "Over-The-Air" (über den Äther) konfiguriert werden kann.

Die ifm *mobile*^{IoT} Suite ist auf die Verwaltung und Konfiguration der ifm *mobile*^{IoT} Plattform und ihrer Komponenten ausgelegt. Frontend und Erscheinungsbild entsprechen deshalb dem ifm-Design und können nicht angepasst werden.

ifm mobile^{IoT} DataPortal – Datenvisualisierungsportal

Das ifm *mobile*^{IoT} DataPortal ist der Plattformbereich zur Datenvisualisierung, der im Rahmen der Möglichkeiten der Benutzeroberfläche des DataPortals konfiguriert, angepasst und nach den Wünschen des Kunden individuell gestaltet werden kann.

Das Frontend kann anhand des vorgegebenen Layouts und durch Einfügen verfügbarer Widgets individuell gestaltet und entsprechend den von den Maschinen erfassten und zu visualisierenden Informationen konfiguriert werden. Darüber hinaus kann das Theming des DataPortals angepasst und passend zur Corporate Identity des Kunden durch Farbgebung und Branding mit Logos gestaltet werden.

Der Kunde kann das DataPortal auch für seine(n) Kunden markenspezifisch und individuell gestalten, indem er die hierarchische Struktur verwendet und das individuelle Layout und Theming einer bestimmten Organisation in der Hierarchie zuordnet.

Neben der Frontend-Anpassung ist im DataPortal auch die Erstellung von Berichten, Diagrammen, Karten etc. möglich.

Urls:

Maschinenmanagement-Suite: https://suite.miot.ifm

DataPortal: https://portal.miot.ifm

LISTE DER LÄNDER UND MOBILFUNKPARTNER

Argentinien	Claro
Argentinien	Telecom Personal
Australien	Optus
Australien	Vodafone
Österreich	Orange
Österreich	T-Mobile
Österreich	Mobilkom
Belgien	Base
Belgien	Proximus
Bulgarien	M-Tel
Bulgarien	Globul
Bulgarien	Vivacom
Kambodscha	Cellcard
Kambodscha	Hallo
Kanada	Bell Mobility
Kanada	Telus
Kanada	Videotron
Chile	Entel
Chile	Claro
Kolumbien	Claro
Kolumbien	Tigo
Kroatien	Croatian Telecom
Kroatien	Tele2
Kroatien	VIPnet
Zypern	Cytamobile-Vodafone
Zypern	MTN
Tschechien	Vodafone
Tschechien	T-Mobile
Dänemark	Telenor
Dänemark	TDC
Ägypten	MobiNil
Ägypten	Etisalat
Ägypten	Vodafone
Estland	EMT
Estland	Tele2
Estland	Elisa
Finnland	DNA
Finnland	Alands Mobiltelefon
Finnland	Elisa
Frankreich	Orange
Frankreich	SFR
Frankreich	Bouygues
Deutschland	T-Mobile
Deutschland	Vodafone
Deutschland	E-plus
Deutschland	O2
Griechenland	Cosmote
Griechenland	Vodafone
Guatemala	Tigo
Guatemala	Claro
Hongkong	3
Hongkong	Hutchison
Hongkong	SmarTone
Ungarn	Telenor
Ungarn	T-Mobile
Ungarn	Vodafone
Indien	Idea
Indien	AirTel
Indien	Vodafone
Indonesien	3
Indonesien	Indosat
Irland	Vodafone
Italien	Vodafone
Italien	TIM
Italien	Wind
Jordanien	Zain
Jordanien	Umniah
Kasachstan	Tele2
Kasachstan	KCell
Kenia	Airtel
Kenia	Safaricom
Korea	KT
Korea	SK Telecom
Kuwait	Zain
Kuwait	Oreedo
Lettland	Tele2
Lettland	Bite Latvija
Lettland	LMT
Litauen	Tele2

Litauen	Bite GSM
Luxemburg	LUXGSM
Luxemburg	Tango
Luxemburg	Orange
Malta	Vodafone
Mexiko	IUSACell
Mexiko	Telcel
Niederlande	Vodafone
Niederlande	T-Mobile
Niederlande	KPN
Norwegen	Telia
Norwegen	Telenor
Panama	Claro
Panama	Cable & Wireless
Panama	Digicel
Paraguay	Claro
Paraguay	Airtel
Peru	Nextel
Peru	Claro
Philippinen	Globe
Philippinen	SMART Gold
Polen	Era
Polen	Plus
Polen	Play
Portugal	Optimus
Portugal	Vodafone
Portugal	TMN
Katar	Vodafone
Katar	Q-Tel
Rumänien	Vodafone
Rumänien	Orange
Russische Föderation	MTS
Russische Föderation	NCC
Russische Föderation	Rostelecom
Russische Föderation	Rostelecom
Saudi-Arabien	STC Al Jawal
Saudi-Arabien	Zain
Serbien	VIP
Serbien	Telenor
Serbien	mt:s
Singapur	M1
Singapur	StarHub
Singapur	SingTel
Slowakei	T-Mobile
Slowakei	Orange
Slowenien	Mobitel
Slowenien	SI Mobil
Südafrika	Vodacom
Spanien	Vodafone
Spanien	Orange
Schweden	Telenor
Schweden	Tele 2
Schweiz	Swisscom
Schweiz	Sunrise
Taiwan	Far EasTone
Taiwan	Taiwan Mobile
Thailand	Real Future
Thailand	True Move
Türkei	AVEA
Türkei	Vodafone
Vereinigtes Königreich	Vodafone
Vereinigte Staaten	AT&T
Vereinigte Staaten	Viaero
Vereinigte Staaten	Commnet Wireless
Vereinigte Staaten	Immix
Vereinigte Staaten	AWN
Vereinigte Staaten	Union Telephone Company
Vereinigte Staaten	T-Mobile
Vietnam	Vinaphone
Vietnam	VietnaMobile
Vietnam	Viettel

Anlage 3
Verhaltenskodex für ifm Geschäftspartner

Entsprechend des ifm Verhaltenskodex dulden wir weder Korruption, Bestechung noch Kinderarbeit. Von unseren Partnern erwarten wir die gleichen Wertvorstellungen. Dieser Verhaltenskodex legt die Grundsätze und Anforderungen an unsere Geschäftspartner bezüglich deren Verantwortung für Mensch und Umwelt dar.

1. Einhaltung der Gesetze und Normen

Der Geschäftspartner hält die geltenden einschlägigen Gesetze, Richtlinien und Normen ein.

2. Verbot von Korruption und Bestechung

Der Geschäftspartner lehnt jegliche Form von Korruption und Bestechung ab. Dazu zählt auch, dass er keine Zahlungen oder sonstige Vorteile (z.B. Kick-Back-Zahlungen, Geschenke, Entertainment) einer Einzelperson, einem Unternehmen oder einem Amtsträger gewährt, mit dem Ziel, Einfluss auf die Entscheidungsprozesse zu nehmen.

3. Vertrauliche Informationen und Datenschutz

Der Geschäftspartner hält sich an alle anwendbaren Datenschutzgesetze. Er stellt sicher, dass über vertrauliche Informationen oder Geschäftsgeheimnisse, die er im Rahmen der Geschäftsbeziehung mit ifm erlangt, strengstes Stillschweigen bewahrt wird und dass diese nicht in unzulässigerweise Weise verwendet oder gegenüber Dritten offengelegt werden.

4. Diskriminierung

Der Geschäftspartner diskriminiert niemanden aufgrund von Alter, Geschlecht, Religion, Herkunft oder aus anderen Gründen.

5. Verbot von Kinder- und Zwangsarbeit

Der Geschäftspartner stellt keine Arbeiter ein, die nicht ein Mindestalter von 15 Jahren vorweisen können. In Ländern, die bei der ILO Konvention 138 unter die Ausnahme für Entwicklungsländer fallen, darf das Mindestalter auf 14 Jahre reduziert werden.

Der Geschäftspartner beschäftigt niemanden gegen seinen Willen oder zwingt jemanden zur Arbeit.

6. Kartellrecht

Der Geschäftspartner verpflichtet sich zu fairem Wettbewerb und beachtet die geltenden Kartellgesetze und beteiligt sich nicht an Preisabsprachen, Aufteilungen von Märkten oder Kunden, Marktabsprachen oder Angebotsabsprachen.

7. Vereinigungsfreiheit und Tarifverhandlungen

Arbeitnehmer haben ohne Unterscheidung das Recht, Gewerkschaften zu ihrer Wahl beizutreten oder zu gründen und Tarifverhandlungen zu führen. Der Geschäftspartner nimmt eine offene Haltung gegenüber den Aktivitäten der Gewerkschaften und ihren organisatorischen Aktivitäten ein. Arbeitnehmervertreter werden nicht diskriminiert und haben Zugriff zur Ausübung ihrer repräsentativen Funktionen am Arbeitsplatz. Die Arbeitnehmer haben das Recht auf Vereinigungsfreiheit und Tarifverhandlungen sind gesetzlich eingeschränkt, der Arbeitgeber erleichtert und behindert nicht die Entwicklung paralleler Mittel für unabhängige und freie Vereinigungs- und Verhandlungsfreiheit.

8. Umweltschutz und Arbeitssicherheit

Der Geschäftspartner verpflichtet sich die jeweils geltenden umweltrelevanten Rechtsvorschriften sowie Auflagen von Behörden einzuhalten und darüber hinaus den Umweltschutz in einem wirtschaftlich vertretbaren Rahmen kontinuierlich zu verbessern.

Der Geschäftspartner hält die gesetzlichen Vorschriften für die Sicherstellung von Gesundheit und Sicherheit am Arbeitsplatz ein.

9. ifm Produkte nicht für militärische Applikationen

Laut der ifm Firmenphilosophie wird ifm grundsätzlich keine Produkte entwickeln, herstellen oder verkaufen, die direkt militärischen oder waffentechnischen Zwecken dienen. Der Geschäftspartner wird daher ifm Produkte nicht an Kunden liefern, die ifm Produkte für militärische Applikationen nutzen wollen oder in militärische Applikationen einbauen.

Anlage 4
Vorlage eines Enduser-Agreements für das Kunden Web Portal
(Customized oder White Label Front End)

WICHTIG: Lesen Sie das Folgende sorgfältig durch, bevor Sie die *mobile*^{IoT} Services nutzen: Dieser Enduser-Agreement ("EUA") ist eine rechtsgültige Vereinbarung zwischen Ihnen als Endkunde oder Endnutzer (beide unten definiert) und _____ ("OEM") für Ihre lizenzierte Nutzung des *mobile*^{IoT} Services, wobei der Lizenzgeber des OEM (unten definiert) ein Drittbegünstigter im Rahmen dieses EUA ist. Mit der Annahme dieses EUA oder der Aktivierung, dem Zugriff oder der anderweitigen Nutzung des *mobile*^{IoT} Services erklären Sie sich damit einverstanden, an die Bedingungen dieses EUA als Voraussetzung für Ihre Lizenz und die Nutzung des *mobile*^{IoT} Services gebunden zu sein und zu werden. Sie werden gebeten, die Bedingungen dieses EUA zu überprüfen und entweder zu akzeptieren oder nicht zu akzeptieren. Wenn Sie mit den Bedingungen dieses EUA nicht einverstanden sind, ist Ihnen die Nutzung verboten und Sie dürfen den *mobile*^{IoT} Service nicht aktivieren, darauf zugreifen oder anderweitig nutzen.

1. Definitionen

"Abonnement“ bezeichnet das Endkundenabonnement für den *mobile*^{IoT} Service, das vom OEM bereitgestellt wird.

„**Abonnementdauer**“ bezeichnet die Dauer der Abonnements für Endkunden.

„Aktivierungsdatum" bezeichnet das Datum, an dem der Endkunde oder einer seiner Endnutzer den *mobile*^{IoT} Service erstmals aktiviert oder den sonstigen Beginn des *mobile*^{IoT} Services, wie zwischen dem Endkunden und dem OEM festgelegt.

"Bösartiger Code" bezeichnet einen Code, Dateien, Skripte oder Programme, die dazu bestimmt sind, Schaden anzurichten, einschließlich z.B. Viren, Würmer, Malware und Trojaner.

“Daten Plattform” bezeichnet die Cloud-basierte Daten Plattform zusammen mit Web Portal, Realtime Client, REST API und anderen IT-Systemen, auf und über die die Software den *mobile*^{IoT} Service betreibt, die Maschinendaten speichert und Endkunden und deren Endnutzern im Rahmen des Abonnements einen lizenzierten Zugriff ermöglicht.

"Derivate" bezeichnet alle Ableitungen, Modifikationen, Fehlerkorrekturen, Patches, Bugfixes, Metadaten, Konfigurations- und Kalibrierungseinstellungen, Software-Updates und Software-Upgrades, Verbesserungen, Weiterentwicklungen und Erweiterungen und nachfolgende Releases der Software, unabhängig vom Ersteller.

"Endkunde" bezeichnet die Wirtschaftseinheit, die durch Abonnement berechtigt ist, den *mobile*^{IoT} Service zu nutzen, der vom OEM von seinem Lizenzgeber bezogen wird.

"Endnutzer" bezeichnet die Beschäftigten und temporären Mitarbeiter des Endkunden, die von ihm ermächtigt wurden, den *mobile*^{IoT} Service in seinem Namen gemäß den Bestimmungen dieses EUA zu nutzen.

“Firmware” bezeichnet die Software und/oder Anwendungsprogrammierschnittstelle, die in die Kommunikationseinheit (CU) eingebettet sind, die mit der Maschine verbunden ist, einschließlich Anpassungen oder anderer Derivate davon (wer auch immer der Ersteller ist), damit die CU mit dem Kommunikationsprotokoll der Maschine kompatibel ist und kommunizieren kann.

"Geistiges Eigentum des Lizenzgebers" bezeichnet die Firmware, die Software, die Daten Plattform, das Web Portal, die Handbücher und den *mobile*^{IoT} Service.

"Kommunikationseinheiten" oder **"CUs"** (Abkürzung für: Communication Units) bezeichnet die vom OEM an den Endkunden verkauften und auf Endkundenmaschinen installierten Onboard-Hardware-geräte, die Maschinendaten des Endkunden zu und von der Daten Plattform übertragen und dem Endkunden und seinen Endnutzern über das Web Portal einen abonnierten und lizenzierten Zugriff ermöglichen.

“Lizenzgeber” bezeichnet die ifm electronic gmbh oder eines ihrer verbundenen Unternehmen.

"Maschine" bezeichnet ein Fahrzeug, eine Maschine oder einen anderen Vermögenswert, den der Endkunde vom Kunden oder einem Zwischenhändler gekauft oder geleast hat, um ihn zu Geschäftszwecken einzusetzen, für den Maschinendaten über den *mobile*^{IoT} Service übertragen werden.

"Maschinendaten" bezeichnet: (a) die von den Kommunikationseinheiten gesammelten und an die Plattform übermittelten maschinenlesbaren Rohdaten, und (b) die daraus durch den *mobile*^{IoT} Service in Form von Einzel- oder Gesamtdaten gewonnenen Nutzdaten über die Maschinen eines Endkunden, wie Status geografischen Standort, Betriebsstunden und andere zwischen der Plattform und den Kommunikationseinheiten übertragenen Fahrzeug- und Maschinendaten.

"Mobiler Kommunikationsdienst" bezeichnet alle von den CUs verwendeten Kommunikations-standards, z.B. LTE, 5G, oder einen anderen Kommunikationsdienst, der für die Übertragung von Maschinendaten zu und von den CUs und der Plattform verwendet wird.

„mobileIoT Service" oder "Service" bezeichnet den Online Service, der von der Software auf der Plattform bereitgestellt und von Endkunden und ihren Endnutzern über das Web Portal abgerufen wird, das Maschinendaten präsentiert, die zu und von den CUs, die in Maschinen installiert sind, die sich innerhalb des Vertragsgebiets befinden, übertragen werden.

"Software" bezeichnet die Software im Objektcode-Format, die den *mobile*^{IoT} Service auf der Daten Plattform ausführt, einschließlich von Web Portal, Realtime Client und REST API, von Software-Updates und -Upgrades, Metadaten, Konfigurations- und Kalibrierungseinstellungen und die dazu notwendigen Tools sowie Installations- und Bedienungsanleitungen und anderen damit in Zusammenhang stehenden Softwaredokumentationen.

“Web Portal” bezeichnet die Website, die auf den Namen und die Marke des OEM konfiguriert ist, über die Endkunden und deren Endnutzer Online-Zugang zur Nutzung des *mobile*^{IoT} Services erhalten.

2. Gewährung einer begrenzten Lizenz für den *mobile*^{IoT} Service

Zum Aktivierungsdatum und während der Abonnementdauer gewährt der OEM dem Endkunden und seinen Endnutzern hiermit (im Namen des Lizenzgebers) eine begrenzte(s), kündbare(s), persönliche(s), nicht ausschließliche(s) und nicht übertragbare(s):

a) Lizenz zur Nutzung der Firmware,

b) Lizenz zur Nutzung der Software,

c) Recht zum Zugang und zur Nutzung des ***mobile***$^{\textbf{IoT}}$ Services über das Web Portal (im Umfang des Service Levels) für den internen Geschäftszweck des Kunden, seinen Endnutzern die Überwachung und Kontrolle von Maschinen zu ermöglichen, und

d) Lizenz zur Nutzung der daraus resultierenden Maschinendaten, die von dem ***mobile***$^{\textbf{IoT}}$ Service erzeugt und auf der Daten Plattform sortiert wurden, wobei ausdrücklich ausgeschlossen wird:

   i. jede Nutzung durch andere Benutzer als den abonnierten Endkunden und seine Endnutzer;

   ii. jede Nutzung mit CUs oder anderen Geräten, die nicht vom Lizenzgeber lizenziert sind; und

   iii. jede Nutzung für Maschinen, die keine Maschine eines Endkunden darstellen.

3. Lizenzbeschränkungen

Weder der Endkunde noch seine lizenzierten Endnutzer dürfen:

a) Aspekte des *mobile*$^{\textbf{IoT}}$ Services oder des sonstigen geistigen Eigentums des Lizenzgebers zu Gunsten einer dritten Partei nutzen, dieser zur Verfügung stellen oder die Nutzung durch andere gestatten,

b) das geistige Eigentum des Lizenzgebers oder andere Aspekte des *mobile*$^{\textbf{IoT}}$ Services übertragen, verkaufen, vermieten, verleihen, offenlegen, für Timesharing- oder Outsourcing-Zwecke nutzen,

c) den *mobile*$^{\textbf{IoT}}$ Service oder das sonstige geistige Eigentum des Lizenzgebers nutzen, um verletzendes, verleumderisches oder anderweitig rechtswidriges oder unerlaubtes Material zu speichern oder zu übertragen oder um Material zu speichern oder zu übertragen, das Datenschutzrechte Dritter verletzt,

d) den *mobile*$^{\textbf{IoT}}$ Service oder das sonstige geistige Eigentum des Lizenzgebers zum Speichern oder Übertragen von Malware verwenden,

e) versuchen, sich unbefugten Zugriff auf einen Aspekt des *mobile*$^{\textbf{IoT}}$ Services oder anderes geistiges Eigentum des Lizenzgebers zu verschaffen,

f) den *mobile*$^{\textbf{IoT}}$ Service, das sonstige geistige Eigentum des Lizenzgebers oder Teile, Merkmale, Funktionen oder Benutzeroberflächen davon kopieren,

g) den Quellcode oder zugrundeliegende Ideen oder Algorithmen des geistigen Eigentums des Lizenzgebers rückentwickeln, dekompilieren, übersetzen, disassemblieren oder zu entdecken versuchen oder anderweitig das geistige Eigentum des Lizenzgebers anders als hierin erlaubt nutzen oder versuchen, Urheberrechts-, Marken- und andere Hinweise, die auf einem geistigen Eigentum des Lizenzgebers erscheinen, unkenntlich machen oder zu entfernen.

Dieser Abschnitt 3 gilt auch nach der Beendigung dieses EUA fort.

4. Geistiges Eigentum des Lizenzgebers

Die begrenzte Lizenz und die Ihnen gemäß Abschnitt 2 gewährten Rechte verleihen keine Rechte oder Eigentum am geistigen Eigentum des Lizenzgebers und sind nicht als Verkauf von Rechten an den vorstehenden Inhalten zu verstehen. Vorbehaltlich der beschränkten Lizenz und der Ihnen gemäß

Abschnitt 2 gewährten Rechte bleibt der Lizenzgeber Inhaber sämtlicher Rechte, Ansprühe und Inhalte aus allem geistigen Eigentum, einschließlich: (a) aller Derivate, Verbesserungen, Erweiterungen, Korrekturen oder kundenspezifischen Anpassungen an den vorgenannten Inhalten, unabhängig davon, ob sie von Ihnen und/oder dem Lizenzgeber erstellt oder entwickelt wurden, und (b) aller Vorschläge, Empfehlungen und sonstigen Rückmeldungen, die von Ihrer Seite stammen. Nichts in dieser EUA gewährt Ihnen ein Recht auf den Quellcode der Software. Dieser Abschnitt 4 gilt auch nach der Beendigung dieses EUA fort.

5. Maschinendaten

Vorbehaltlich der eingeschränkten Lizenz und Rechte, die Ihnen gemäß Abschnitt 2 gewährt werden, ist der Lizenzgeber berechtigt, die erfassten Maschinendaten in anonymisierter Form zu nutzen, um seine Produkte und Dienstleistungen zu verbessern sowie zu Marketingzwecken. Dieser Abschnitt 5 gilt auch nach der Beendigung dieses EUA fort.

6. Nutzung der Nutzungshistorie und Profilinformationen

Mit der Annahme dieses EUA, ausdrücklich oder konkludent durch Aktivierung, Zugriff oder anderweitige Nutzung des *mobile*^{IoT} Services, gewähren Sie dem Lizenzgeber das Recht auf uneingeschränkten Zugriff und Nutzung Ihrer: (a) Servicekontoprofildaten und (b) Nutzungshistorie im Zusammenhang mit Ihrer Nutzung des *mobile*^{IoT} Services und der Maschinendaten ("**Nutzungs-historie**"), soweit dies für die Konfiguration und/oder Neukonfiguration der Endkunden-Servicekonten durch den Lizenzgeber zur Erbringung des *mobile*^{IoT} Services erforderlich ist. Darüber hinaus kann der Lizenzgeber von Zeit zu Zeit Ihre Nutzungshistorie mit der Nutzungshistorie anderer Endnutzer aggregieren und diese in einer nicht persönlich identifizierbaren Form zusammenstellen und diese aggregierte Nutzungshistorie an vom Lizenzgeber bestimmte Dritte weitergeben.

7. Technischer Support

Der Lizenzgeber bietet dem Endkunden oder seinen Endnutzern keinen direkten technischen Support für den *mobile*^{IoT} Service, die Software, das Web Portal, die CUs oder den Mobilfunkdienst ("**Supportgegenstände**"). Der OEM ist allein verantwortlich für die Bereitstellung von technischem Support für Endkunden und/oder Endnutzer zu den Bedingungen, die zwischen dem OEM und dem Endkunden vereinbart wurden.

8. Beschränkung der Gewährleistung

DER LIZENZGEBER MACHT KEINE ZUSICHERUNGEN UND ÜBERNIMMT DEM ENDKUNDEN ODER SEINEN ENDNUTZERN GEGENÜBER KEINE GEWÄHRLEISTUNG ODER GARANTIEN IN BEZUG AUF DEN MIOT SERVICE ODER ANDERE SUPPORTGEGENSTÄNDE. ALLE ZUSICHERUNGEN UND GARANTIEN IN BEZUG AUF DIE SUPPORTGEGENSTÄNDE, OB SCHRIFTLICH ODER MÜNDLICH, WERDEN HIERMIT AUSDRÜCKLICH AUSGESCHLOSSEN, EBENSO WIE STILLSCHWEIGENDE ZUSICHERUNGEN UND GARANTIEN IN BEZUG AUF DIE WIRTSCHAFTLICHKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. Der OEM ist allein verantwortlich für die Übernahme (falls vorhanden) von Garantien und Gewährleistung gegenüber Endkunden und/oder Endnutzern für die Supportgegenstände (falls vorhanden) zu den zwischen dem OEM und dem Endkunden vereinbarten Bedingungen. Dieser Abschnitt 8 gilt auch nach der Beendigung dieses EUA fort.

9. Haftungsbeschränkung

SOWEIT NACH GELTENDEM RECHT ZULÄSSIG, SIND DER LIZENZGEBER ODER SEINE VERBUNDENEN UNTERNEHMEN IN KEINEM FALL HAFTBAR FÜR ZUFÄLLIGE, DIREKTE, INDIREKTE SCHÄDEN, FOLGESCHÄDEN, STRAFSCHADENSERSATZ ODER SONSTIGE SCHÄDEN, DIE AUS DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DES MIOT SERVICES ODER IM ZUSAMMENHANG MIT DER ERHEBUNG DER MASCHINENDATEN ENTSTEHEN, SEI ES DASS SIE AUF VERTRAG, UNERLAUBTER HANDLUNG, NACHLÄSSIGKEIT, GEFÄHRDUNGSHAFTUNG ODER EINEM ANDEREN RECHTSGRUND BERUHEN. DIESE HAFTUNGSBESCHRÄNKUNG GILT AUCH DANN, WENN DER LIZENZGEBER ODER SEINE VERBUNDENEN UNTERNEHMEN ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDEN ODER WENN EIN RECHTSMITTEL SEINEN WESENTLICHEN ZWECK VERFEHLT. Dieser Abschnitt 9 gilt auch nach der Beendigung dieses EUA.

10. Kündigung

Dieses EUA kann jederzeit beendet werden durch: (a) Kündigung des Abonnements, (b) Kündigung des mIoT Agreements zwischen OEM und Lizenzgeber, (c) Mitteilung des Lizenzgebers an den Endkunden für den Fall, dass der Endkunde oder seine Endnutzer gegen eine Bedingung dieses EUA verstoßen. Bei Beendigung dieses EUA aus irgendeinem Grund: (a) werden die in Abschnitt 2 gewährte Lizenz und alle anderen Lizenzen oder Rechte, die an anderer Stelle in diesem EUA gewährt werden, automatisch und gleichzeitig beendet und (b) Sie müssen die Nutzung des mobileIoT Services und des anderen geistigen Eigentums des Lizenzgebers unverzüglich einstellen.

11. Anwendbares Recht, Gerichtsstand

Dieses EUA unterliegt dem Recht der Bundesrepublik Deutschland, ohne Rücksicht auf seine Kollisionsnormen und unter Ausschluss des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf (CISG). Ausschließlicher Gerichtsstand ist das Landgericht Essen.

Anlage 5

Vereinbarung zur Datenverarbeitung im Auftrag

zwischen

(Auftraggeber - nachfolgend Verantwortlicher genannt)

und

(Auftragnehmer nachfolgend – Auftragsverarbeiter genannt)

Präambel

Mit dem 25.05.2018 gilt innerhalb der EU, also auch in Deutschland, die Datenschutzgrundverordnung (DSGVO) und löst die jetzige Fassung des Bundesdatenschutzgesetzes ab. Die Verordnung enthält in Art. 28 DSGVO verbindliche Vorgaben, wenn personenbezogene Daten im Auftrag durch andere Stellen verarbeitet werden. Die Auftragsverarbeitung soll nach Art 28 Abs. 3 DSGVO auf Grundlage eines Vertrages erfolgen und die dort festgelegten Inhalte berücksichtigen.

Neben der „klassischen Verarbeitung“ von personenbezogenen Daten im Auftrag, bei der personenbezogene Daten an den Auftragsverarbeiter übermittelt werden, kann Gegenstand des Vertrages zwischen dem Verantwortlichen und dem Auftragsverarbeiter die IT-Wartung oder Fernwartung (z. B. Fehleranalysen, Support-Arbeiten in Systemen des Verantwortlichen) sein. Besteht dabei für den Auftragsverarbeiter die Notwendigkeit oder zumindest die Möglichkeit des Zugriffs auf personenbezogene Daten, so handelt es sich ebenfalls um eine Form oder Teiltätigkeit einer Auftragsverarbeitung und die Anforderungen des Art. 28 DSGVO – wie etwa der Abschluss eines Vertrages zur Auftragsverarbeitung – sind umzusetzen.

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem mIoT Agreement ergeben. Die Parteien erklären sich bezüglich der Datenverarbeitung gemäß den Bedinungen dieses AVV, wie folgt, einverstanden:

Begrifflichkeiten

Personenbezogene Daten
Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Verarbeitung von personenbezogenen Daten
Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Art. 4 Nr. 2 DSGVO).

Verantwortlicher
Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

Auftragsverarbeiter
Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

1. Gegenstand und Dauer des Auftrages

(1) Gegenstand

Der Auftrag des Verantwortlichen an den Auftragsverarbeiter umfasst folgende Arbeiten und/oder Leistungen:

Bereitstellung des internetgeschützten Portals und Übertragung der Maschinendaten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Verantwortlichen sind konkret beschrieben im mIoT Agreement.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des mIoT Agreements.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

2. Art(en) der personenbezogenen Daten:

Wenn Sie bzw. Ihre Endkunden einen Zugang zu unserer Plattform / unserem Internetportal einrichten, erheben wir folgende Informationen:

- Mitarbeiter des Auftraggebers
  - Vor- und Zuname
  - Telefonnummer (Festnetz und/oder Mobilfunk)
  - E-Mail-Adresse
- Login-Zeiten
- User-Aktionen
- Maschinendaten
- GPS-Daten (pseudonymisiert)*

*“Pseudonymisierung“ bedeutet: Die Verarbeitung personenbezogener Daten in einer Weise, dass diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Rechtsgrundlage für die Verarbeitung ist die Erfüllung eines Vertrages. Eine Speicherung der Daten zur Einrichtung Ihres Zugangs kann jederzeit widerrufen werden.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragsverarbeiter hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung,

insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Verantwortlichen zur Prüfung zu übergeben. Bei Akzeptanz durch den Verantwortlichen werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Die konkrete Beschreibung der technischen und organisatorischen Maßnahmen erfolgt in einer separaten **Anlage** zu dieser Vereinbarung.

4. Berichtigung, Einschränkung und Löschung von Daten

Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, soweit gesetzlich vorgeschrieben.

Für den Auftragsverarbeiter ist als Beauftragte(r) bestellt:

Gindat GmbH – Gesellschaft für IT-Normierung und Datenschutz
Wetterauer Str. 6
42897 Remscheid

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragsverarbeiter setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.
   Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c) Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
d) Die unverzügliche Information des Verantwortlichen über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt.
e) Soweit der Verantwortliche seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung

beim Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

f) Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

6. Unterauftragsverhältnisse

(1) Der Verantwortlich und die verantwortlichen Stellen gestatten dem Auftragsverarbeiter, Unterauftragsverarbeiter mit der Verarbeitung personenbezogener Daten zu beauftragen. Der Auftragsverarbeiter trägt die Verantwortung für Vertragsverletzungen, die durch seine Unterauftragsverarbeiter zu vertreten sind.

(2) Unterauftragsverarbeiter unterliegen in Bezug auf die Verarbeitung personenbezogener Daten entsprechenden Verpflichtungen, die für den Auftragsverarbeiter als Datenverarbeiter (oder Unterauftragsverarbeiter) gelten.

(3) Vor der Auswahl eines Unterauftragsverarbeiters prüft der Auftragsverarbeiter dessen Maßnahmen zur Wahrung der Sicherheit, des Datenschutzes und der Vertraulichkeit. Unterauftragsverarbeiter können die Anwendung angemessener Sicherheitsmaßnahmen durch Sicherheitszertifikate nachweisen. Andernfalls prüft der Auftragsverarbeiter in regelmäßigen Abständen bei jedem Unterauftragsverarbeiter dessen Sicherheitsmaßnahmen beim Umgang mit Daten.

(4) Der Einsatz von Unterauftragsverarbeitern erfolgt nach Ermessen des Auftragsverarbeiters unter der Voraussetzung, dass folgende Bedingungen eingehalten werden:

(a) Der Auftragsverarbeiter informiert den Verantwortlichen im Voraus (per E-Mail oder das Support Portal) über jegliche Änderungen der Unterauftragsverarbeiter, die nach dem Wirksamkeitsdatum der Vereinbarung eintreten (mit Ausnahme eines Notfallaustausches oder der ersatzlosen Streichung eines Unterauftragsverarbeiters).

(b) Der Verantwortliche kann der Beauftragung eines Unterauftragsverarbeiters durch den Auftragsverarbeiter widersprechen, wenn er in Bezug auf die Verarbeitung von personenbezogenen Daten durch den Unterauftragsverarbeiter einen berechtigten Grund für den Widerspruch hat, indem er dies dem Auftragsverarbeiter innerhalb von dreißig (30) Tagen nach Benachrichtigung der Änderung schriftlich mitteilt. Wenn der Verantwortliche der Beauftragung des Unterauftragsverarbeiters widerspricht, werden die Parteien nach Treu und Glauben zusammenkommen, um eine Lösung zu vereinbaren. Der Auftragsverarbeiter kann entscheiden, (i) den Unterauftragsverarbeiter nicht einzusetzen oder (ii) die vom Verantwortlichen in dessen Einspruch geforderten Korrekturmaßnahmen zu ergreifen und den Unterauftragsverarbeiter weiterhin einzusetzen. Wenn keine dieser Optionen auf zumutbare Weise umsetzbar ist und der Verantwortliche seinen Einspruch aus einem berechtigten Grund aufrechterhält, kann jede Partei die Vereinbarung mit einer Frist von dreißig (30) Tagen nach Erhalt der Mitteilung schriftlich kündigen. Wenn der Verantwortliche nicht innerhalb von dreißig (30) Tagen nach Erhalt der Mitteilung der Änderung Einspruch erhebt, gilt der neue Unterauftragsverarbeiter als vom Verantwortlichen akzeptiert.

(c) Wenn der Einspruch des Verantwortlichen sechzig (60) Tage, nachdem er erhoben wurde, nicht ausgeräumt wurde und der Auftragsverarbeiter keine Kündigungsmitteilung erhalten hat, gilt der Unterauftragsverarbeiter als vom Verantwortlichen akzeptiert.

(5) Der Auftragsverarbeiter kann einen Unterauftragsverarbeiter austauschen, wenn sich der Grund für den Austausch der Kontrolle des Auftragsverarbeiters entzieht. In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen so schnell wie möglich über den neuen Unterauftragsverarbeiter. Der Verantwortliche ist gemäß Abschnitt 6 (5) (b) berechtigt, gegen einen neuen Unterauftragsverarbeiter Einspruch zu erheben.

7. Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche hat das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen. Die Gestellung von Mitarbeitern des Auftragsverarbeiters im Rahmen einer solchen Kontrolle ist bis zu einem Umfang von vier Stunden/Jahr kostenlos, ab der fünften Stunde ist der Auftragsverarbeiter berechtigt eine angemessene Vergütung zu verlangen.

(2) Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Auftragsverarbeiter kann seinen Pflichten nach den Absätzen 1) und 2) auch erfüllen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, DIN-ISO 27001).

8. Mitteilung bei Verstößen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Verantwortlichen zu melden
c) die Verpflichtung, dem Verantwortlichen im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen. Der Auftragsverarbeitung ist berechtigt für diese Leistung eine angemessene Vergütung zu verlangen.
d) die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen.

9. Weisungsbefugnis des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten des Verantwortlichen ausschließlich entsprechend der Weisung des Verantwortlichen. Mündliche Weisungen bestätigt der Verantwortliche unverzüglich (mind. Textform).

(2) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Die Löschung bzw. Vernichtung ist dem Verantwortlichen auf Anforderung zu bestätigen. Entstehen dem Auftragsverarbeiter zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt diese der Verantwortliche.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

11. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

12. Schlussbestimmungen

(1) Für Nebenabreden ist die Schriftform erforderlich.

(2) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Anlage zur AVV

IT-Sicherheitskonzept – Technische und organisatorische Maßnahmen

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Der Auftragsverarbeiter erfüllt diesen Anspruch durch folgende(s) Maßnahmen / IT-Sicherheitskonzept:

1. Rechtliche Rahmenbedingungen

Die Einhaltung der jeweils gültigen gesetzlichen Vorschriften oder verbindlichen Vorgaben anderer Institutionen müssen eingehalten werden. Sämtliche dazu erforderlichen Maßnahmen werden an geeigneter Stelle dokumentiert und veröffentlicht. Die im Unternehmen genutzte Software ist nach den rechtlichen Vorgaben zu lizenzieren, die damit verbundene Dokumentation ist aktuell zu halten.

2. Arbeitsplätze

2.1 Verpflichtung / Sensibilisierung

Jeder IT-Benutzer ist der Einhaltung der gesetzlichen Vorgaben und internen Richtlinien verpflichtet. Neben der Kenntnisnahme und Umsetzung entsprechender Informationen gehört dazu auch die Sensibilisierung zur Vermeidung und Erkennung von Störungen, die aus Verletzungen der Vorgaben zur IT-Sicherheit entstehen oder entstehen können.

2.2 Allgemeine Nutzungsregelungen

- die jeweils erlaubte Nutzung ist ausschließlich zu dienstlichen Zwecken gestattet
- nur freigegebene Software darf verwendet werden
- die Nutzung privater Hard- und Software ist nur mit ausdrücklicher Genehmigung zulässig
- Änderungen an Systemeinstellungen, insbesondere Installationen, Deinstallationen oder Konfigurationsänderungen des Basissystems, sind ausschließlich Administratoren erlaubt

2.3 Identity Management

Zur Steuerung und Kontrolle der unterschiedlichsten Berechtigungen und zur Sicherstellung des korrekten Umgangs mit diesen ist eine umfassende Anwenderverwaltung (Identity Management) einzurichten. Darin ist eine vollständige Dokumentation zu mindestens der folgenden Bereiche pro Anwender vorzusehen und aktuell zu halten:

- Assets (Bereitstellung der Hardware, Software-Lizenzen)
- Kritikalität des Arbeitsplatzes (Bezug zu Geschäftsprozess)
- Berechtigungen (Zutritts- und Zugangsberechtigungen)

Des Weiteren sind Prozesse zu definieren, die die Einrichtung und das Ausscheiden von IT-Anwendern regeln.

2.4 Zutritts- und Zugangsregelungen

Der Arbeitsplatz ist aufgeräumt zu halten, so dass Unbefugte keinen Zugriff auf Informationen oder Anwendungen ermöglicht wird. Hierzu finden gesonderte Regelungen Anwendung. Als grundsätzliche Sicherheitsmaßnahme ist zu beachten, dass die Weitergabe von Benutzerkennungen und Passwörtern oder sonstigen Authentifizierungshilfsmitteln untersagt ist. Bei Verdacht, dass die eigene Zugangs- bzw. Zutrittsberechtigung unerlaubt durch Dritte genutzt wurde, sind entsprechende Maßnahmen zu treffen, um die Vertraulichkeit dieser Berechtigungen wiederherzustellen. Es ist eine Übersicht zu erstellen und aktuell zu halten aus der hervorgeht, welche Berechtigungen jeder Anwender hat, insbesondere Zugang zu Daten bzw. Informationen der Klasse „vertraulich“.

2.5 Passwort-Regeln

Es gibt eine interne Passwortrichtlinie. Die Administration ist angehalten, geeignete technische Maßnahmen so einzurichten, dass die Einhaltung für Anwender verständlich und einfach ist und Fehlbedienungen ausgeschlossen sind.

2.6 Sicherheitsupdates
Die Sicherheitseinstellungen sämtlicher IT-Systeme, die der Behebung von Schwachstellen dienen, sind auf aktuellem Stand zu halten („Sicherheitsupdates“).

2.7 Virenschutz
Auf sämtlichen IT-Systemen ist durch die IT ein aktiver und aktueller Virenschutz sicherzustellen. Die eingestellten Konfigurationen dürfen vom Anwender nicht deaktiviert oder verändert werden. Jeder elektronische Datenträger ist vor Verwendung auf Viren oder sonstige Schadprogramme zu untersuchen.

2.8 Verschlüsselung
Der Verschlüsselung kommt eine besondere Bedeutung zu, für die es eine interne Klassifizierungsrichtlinie gibt.

2.9 Notfallvorsorge
Jeder Anwender hat regelmäßige Sicherungen durchzuführen von Dateien, die nicht über zentrale Mechanismen gesichert werden (können). Dabei ist darauf zu achten, dass die Datensicherung verschlüsselt erfolgt, die Datenträger sicher aufbewahrt und in ausreichenden Zeitabständen auf Lesbarkeit überprüft werden.

3. Zentrale Systeme und Netzwerke
3.1 Verfügbarkeit
Abhängig von ihrer Funktion innerhalb von Geschäftsprozessen und den Vereinbarungen mit Nutzern bzw. Nutzergruppen der Systeme ist für diese die geforderte Verfügbarkeit sicherzustellen.

3.2 Monitoring
Es ist ein Monitoring zu etablieren, welches die Kenntnis von Unregelmäßigkeiten des Betriebs in einer angemessenen Zeit ermöglicht. Die Schwerpunkte liegen in der Überwachung der Verfügbarkeit, der sicheren Kommunikation und der Unversehrtheit der Daten. Im Rahmen gesetzlicher Vorschriften ist die sachgerechte Protokollierung und Auswertung relevanter Vorgänge, auch die von Anwenderaktivitäten, einzurichten. Darüber hinaus ist über das Monitoring der Nachweis über die Einhaltung von SLA´s und eine Übersicht über sicherheitsrelevante Vorkommnisse zu erbringen (Reportwesen).

3.3 Zugriffsregelungen
Den Zugriffsregelungen auf das Netz des Auftragsverarbeiters aus öffentlichen Netzen heraus kommt besondere Bedeutung zu. Sie sind entsprechend differenziert erstellt und besonders zu kontrollieren.

3.3.1 Physikalischer Zugang
Der Zugang zu lokalen Netzen, kabelgebunden oder drahtlos, darf nur berechtigten Personen oder Systemen mit eindeutiger Autorisierung möglich sein. Die Bereitstellung von offenen Zugangspunkten ist nur dann erlaubt, wenn gleichzeitig sichergestellt ist, dass keine sicherheitsrelevanten Komponenten berührt werden. Dazu zählen neben physikalischen Systemen und Applikationen insbesondere interne Daten und Informationen.

3.3.2 Authentifizierung
Jeder Nutzer der Infrastruktur des Auftragsverarbeiters hat sich eindeutig zu authentifizieren (personalisierte Anmeldung). Da über die Authentifizierung auch Berechtigungen gesteuert werden sind sog. Gruppen-logins, bei denen sich mehrere Anwender mit derselben Kennung anmelden, nur in besonderen Ausnahmefällen erlaubt. Die damit verbundenen Regelungen (u. a. die interne Passwortrichtlinie) sind zu beachten.

3.3.3 Autorisierung
Ein unbeaufsichtigter bzw. unprotokollierter Zugang zu Daten und Informationen der Klasse „vertraulich“ bzw. „streng vertraulich“ ist zu verhindern. Anfragen zu Zugängen zu Informationen der genannten Klassen sind nur nach Rücksprache mit dem Eigentümer der Information zu bearbeiten.

3.4 Datensicherungskonzept
Sämtliche Daten sind in geeigneter Weise zu sichern. Abhängig ihrer Kritikalität bei Verlust sind der Umfang, die Regelmäßigkeit, die Aufbewahrung, Anforderungen an Wiederherstellbarkeit und mögliche Besonderheiten zu berücksichtigen.

3.5 Change Management

Jede Änderung an der IT-Infrastruktur kann Auswirkungen auf die gesetzten Schutzziele haben und ist nur nach entsprechender Planung und Vorbereitung durchzuführen.

3.6 Desaster Recovery

Die im Rahmen eines „Desaster Recovery“ aufgeführten Maßnahmen betreffen Störfälle, die deutlich über den Umfang zu erwartender Störungen hinausgehen (Katastrophen). Die damit verbundenen besonderen und umfangreichen Maßnahmen können erheblichen Einfluss auf sonstige Organisationen, Prozesse und Richtlinien haben. Das grundlegende Konzept für diese Fälle ist separat erstellt.

4. Externe Sicherheit

Der Bereich der externen Sicherheit umfasst sämtliche Verbindungen von IT-Komponenten zu öffentlichen Umgebungen. Die Schwerpunkte liegen dabei auf den zentralen Übergängen eines internen Netzes in ein öffentliches Netz und den Zugängen einzelner Arbeitsstationen in das interne Netz.

4.1 Zutrittsregelungen

Die im Bereich der Arbeitsplatzsicherheit aufgeführten Anforderungen finden gleichermaßen für den Gebäudeschutz Anwendung. Firmenfremde Personen sind, besonders in sicherheitskritischen Bereichen, ständig zu beaufsichtigen. Je nach Schutzbedarf sind weitere einschränkende Maßnahmen durchzuführen.

4.2 Zugangssteuerung / -Überwachung

Es sind nur Netzübergänge erlaubt, die einen unberechtigten Zugang verhindern und über Protokollierungsmaßnahmen verfügen, die einen derartigen Versuch erkennen lassen. Durch die IT-Administration muss sichergestellt werden, dass nur bekannte und berechtigte Personen Zugang zum Netzwerk haben. Entsprechende Dokumentationen und Kontrollverfahren sind zu etablieren. Externe Dritte dürfen nur unter Einrichtung solcher Maßnahmen Zugang erhalten, die eine Kontrolle des Zugangs und des Zugriffs erlauben und eine möglicherweise erforderliche sofortige Unterbindung ermöglichen.

4.3 Internet

Dem Übergang ins Internet kommt im Rahmen der Sicherheitsbetrachtungen erhebliche Bedeutung zu. Es muss gewährleistet sein, dass aus dem Internet kein unerkannter unberechtigter Zugriff auf interne IT-Komponenten, besonders der Daten, möglich ist. Bei Erkennen eines unberechtigten Zugriffs sind sofortige Maßnahmen zu dessen Unterbindung zu treffen.