Everllence

Allgemeine Bedingungen zur Cybersicherheit für Lieferanten und Auftragnehmer

1. Begriffsbestimmungen

In diesen Allgemeinen Bedingungen haben die folgenden Begriffe die nachstehenden Bedeutungen:

1.1. **AG** bezeichnet den Auftraggeber. Das ist diejenige Gesellschaft innerhalb des Everllence Konzerns, welche die Leistungen nach dem jeweiligen Vertrag bestellt (je nachdem Everllence SE oder deren Betriebsstätten oder Tochtergesellschaften).

1.2. **AN** bezeichnet den Lieferanten/Auftragnehmer des AG.

1.3. **Aktiv ausgenutzte Schwachstelle** bezeichnet eine Schwachstelle, zu der verlässliche Nachweise dafür vorliegen, dass ein böswilliger Akteur sie in einem System ohne Zustimmung des Systemeigners ausgenutzt hat.

1.4. **Ausnutzbare Schwachstelle** bezeichnet eine Schwachstelle, die von einem unbefugten Dritten unter praktischen Betriebsbedingungen wirksam genutzt werden kann.

1.5. **CE-Kennzeichnung** bezeichnet eine Kennzeichnung, durch die ein Hersteller erklärt, dass ein Produkt mit digitalen Elementen und die vom Hersteller festgelegten Verfahren den grundlegenden Cybersicherheitsanforderungen in Anhang I des Cyber Resilience Act und anderen geltenden Harmonisierungsrechtsvorschriften der Union über ihre Anbringung genügen.

1.6. **Cyber Resilience Act (CRA)** bezeichnet die EU-Verordnung 2024/2847 sowie alle delegierten Rechtsakte und nationalen Umsetzungsvorschriften.

1.7. **Everllence** bezeichnet die Everllence SE sowie alle von Everllence mittelbar und unmittelbar nach §§ 15 ff. des Aktiengesetzes verbundenen Unternehmen.

1.8. **Dienste** sind Informations- und Kommunikationsdienste sowie Telekommunikations- und telekommunikationsgestützte Dienste.

1.9. **Hersteller eines Produktes mit digitalen Elementen** bezeichnet eine natürliche oder juristische Person, die Produkte mit digitalen Elementen entwickelt oder herstellt oder die Produkte mit digitalen Elementen konzipieren, entwickeln oder herstellen lässt und sie unter ihrem Namen oder ihrer Marke vermarktet, sei es gegen Bezahlung, zur Monetarisierung oder unentgeltlich.

1.10. **Händler** bezeichnet einen AN, der ein Produkt mit digitalen Elementen an AG verkauft, vermietet und/oder vertreibt, ohne der Hersteller des jeweiligen Produktes zu sein.

1.11. **Bedingungen** bezeichnet diese „Allgemeine Bedingungen zur Cybersicherheit für Lieferanten und Auftragnehmer“.

1.12. **Netz- und Informationssysteme** bezeichnet alle digitalen Systeme und Netzwerke, die zur Bereitstellung und Nutzung von Informationsdiensten dienen. Darunter fallen zum Beispiel IT-Infrastrukturen, Server, Kommunikationsnetze und alle damit verbundenen Hardware- und Software-Komponenten.

1.13. **Produkt mit digitalen Elementen** bezeichnet ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden. Datenfernverarbeitung im vorgenannten Sinne bezeichnet entfernt stattfindende Datenverarbeitung, für die eine Software vom Hersteller

selbst oder unter dessen Verantwortung konzipiert und entwickelt wird und ohne die das Produkt mit digitalen Elementen eine seiner Funktionen nicht erfüllen könnte.

1.14. **Schwachstelle** bezeichnet eine Schwäche, Anfälligkeit oder Fehlfunktion eines Produkts mit digitalen Elementen oder eines IKT-Produktes oder eines IKT-Dienstes, die bei einer Cyberbedrohung ausgenutzt werden kann.

1.15. **Sicherheitsvorfall** bezeichnet ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt.

1.16. **Software-Stückliste** bezeichnet eine Aufzeichnung der Einzelheiten und Lieferkettenbeziehungen der Komponenten, die in den Softwareelementen eines Produkts mit digitalen Elementen enthalten sind.

1.17. **Systeme** sind IT-Systeme, IT-Netze und IT-Einrichtungen und/oder Daten- und Telekommunikationsanlagen, -einrichtungen, -netze, -linien, -übertragungswege einschließlich der Hard- und Software.

1.18. **Unterstützungszeitraum** bezeichnet den genauen Zeitraum, inklusive eines konkreten Enddatums, in dem der Hersteller eines Produktes mit digitalen Elementen sicherstellen muss, dass die Schwachstellen des Produkts mit digitalen Elementen wirksam und im Einklang mit den Bedingungen behandelt werden.

1.19. **Leistungen** sind sämtliche im Rahmen des Vertrages vereinbarten, vom AN zu erbringenden und zu liefernden Leistungen.

2. Geltungsbereich

2.1. Diese Bedingungen gelten für alle Leistungen des AN und sind integraler Bestandteil aller Aufträge des AG an den AN und verbindlicher Vertragsteil der den jeweiligen Aufträgen zugrunde liegenden Vertragsbedingungen.

2.2. Vertragliche Bedingungen des AN oder Dritter zur Cybersicherheit finden keine Anwendung, es sei denn, die Parteien haben deren Anwendung ausdrücklich schriftlich vereinbart.

2.3. Soweit der AN aufgrund des CRA und / oder anderen Rechtsakten aus dem Bereich der Informationssicherheit zusätzlichen gesetzlichen Pflichten unterliegt, die über die Anforderungen in diesen Bedingungen hinausgehen, gelten diese zusätzlich zu den in den Bedingungen genannten Anforderungen.

3. Informationssicherheit von Produkten mit digitalen Elementen

3.1. Soweit die vom AN bereitgestellten Leistungen Produkte mit digitalen Elementen beinhalten und der AN Hersteller dieser Produkte mit digitalen Elementen ist, gilt Folgendes:

i) Der AN gewährleistet, dass die Produkte mit digitalen Elementen ein angemessenes Cybersicherheitsniveau nach dem neuesten Stand der Technik gewährleisten, einschließlich der Minimierung negativer Auswirkungen auf die Verfügbarkeit anderer Produkte, verbundener Geräte oder Dienste. Insbesondere müssen die Produkte mit digitalen Elementen a) ohne bekannte ausnutzbare Schwachstellen bereitgestellt werden, b) mit einer sicheren Standardkonfiguration bereitgestellt werden und die Möglichkeit bieten, die Produkte in ihren ursprünglichen Zustand zurückzusetzen, c) sicherstellen, dass Schwachstellen behoben werden können, ggf. auch durch automatische Sicherheitsupdates, d) die Verfügbarkeit wesentlicher und grundlegender Funktionen, auch nach einem Sicherheitsvorfall sicherstellen, e) sicherheitsbezogene Informationen

durch Aufzeichnung und/oder Überwachung einschlägiger interner Vorgänge wie Zugang zu Daten, Diensten oder Funktionen und Änderungen daran bereitstellen, mit der Option, diese Funktion zu deaktivieren.

ii) Für die Zwecke der Erfüllung von Ziffer 3.1 i) führt der AN eine Bewertung der Cybersicherheitsrisiken durch, die die Produkte mit digitalen Elementen bergen, und berücksichtigt das Ergebnis dieser Bewertung in der Planungs-, Konzeptions-, Entwicklungs-, Herstellungs-, Liefer- und Wartungsphase der Produkte mit digitalen Elementen, um die Cybersicherheitsrisiken zu minimieren, Sicherheitsvorfälle zu verhindern und die Auswirkungen solcher Sicherheitsvorfälle so gering wie möglich zu halten. Der AN stellt dem AG das Ergebnis dieser Bewertung auf Verlangen in dokumentierter Form zur Verfügung.

iii) Der AN wird während des Unterstützungszeitraumes (vgl. insoweit Ziffer 3.1 iv)) (einschließlich, aber nicht beschränkt auf die Entwicklung, Herstellung, Lieferung und Wartung) unentgeltlich angemessene Standards, Prozesse und Methoden implementieren und aufrechterhalten, um jegliche ausnutzbare Schwachstellen in den Produkten mit digitalen Elementen zu verhindern, zu identifizieren, zu bewerten und zu beheben. Der AN meldet dem AG unverzüglich ausnutzbare Schwachstellen, die vor Auslieferung der Produkte mit digitalen Elementen dem AN bekannt sind oder bekannt sein müssten, oder die dem AN während des Unterstützungszeitraumes bekannt werden, inklusive praktikabler Mitigationsmöglichkeiten / Risikominderungsmöglichkeiten (z.B. Möglichkeiten zur Konfiguration, Patches). Dies gilt insbesondere auch für Produkte mit digitalen Elementen oder Komponenten hiervon, die für den Einbau in die Produkte des AG vorgesehen sind.

iv) Der AN benennt vor Vertragsabschluss den Unterstützungszeitraum, in dem er seinen Verpflichtungen zur Behandlung von Schwachstellen gemäß Ziffer 3.1 iii) nachkommt. Die Dauer des Unterstützungszeitraumes entspricht mindestens der üblichen Lebensdauer vergleichbarer Produkte, sofern nicht ausdrücklich schriftlich etwas anderes vereinbart wird.

v) Der AN stellt dem AG unentgeltlich eine vollständige Software-Stückliste in einem gängigen, maschinenlesbaren Format zur Verfügung. Die Software-Stückliste hat alle in den bereitgestellten Produkten mit digitalen Elementen enthaltenen Software-Komponenten, einschließlich solcher von Dritten, eindeutig zu identifizieren und die jeweilige Versionsbezeichnung anzugeben. Die Bereitstellung erfolgt spätestens mit der Übergabe der Produkte mit digitalen Elementen sowie jeweils nachträglich bei wesentlichen Änderungen oder Aktualisierungen, die Auswirkungen auf die Software-Stückliste haben.

vi) Der AN wird dem AG auf Verlangen unverzüglich sämtliche Dokumente und Informationen zur Verfügung stellen, die erforderlich sind, damit der AG die Konformität der Produkte mit digitalen Elementen als Bestandteil der eigenen Produkte des AG mit gesetzlichen Anforderungen nachweisen kann. Darüber hinaus gilt Ziffer 4.5 entsprechend. Soweit der AN als Hersteller dem CRA unterliegt, stellt der AN auf Verlangen des AG diesem die technische Dokumentation im Sinne des Art. 31 CRA unentgeltlich zur Verfügung.

3.2. Soweit die vom AN bereitgestellten Leistungen Produkte mit digitalen Elementen beinhalten und der AN Händler dieser Produkte mit digitalen Elementen ist, gilt Folgendes:

i) Die nachfolgenden Regelungen gemäß Ziffer 3.2 ersetzen die vorstehenden Regelungen gemäß Ziffer 3.1.

ii) Der AN gewährleistet, dass seine Verträge mit seinen Unterlieferanten sicherstellen, dass die in den Ziffern 3.1 enthaltenen Anforderungen an Hersteller von Produkten mit digitalen Elementen in seiner Lieferkette eingehalten werden.

iii) Der AN prüft, ausgehend von den ihm vorliegenden Informationen, dass

(a) die Produkte mit digitalen Elementen, die er dem AG bereitstellt, den Anforderungen von Ziffer 3.1 i) und

(b) die vom Hersteller der Produkte mit digitalen Elementen festgelegten Verfahren den Anforderungen von Ziffer 3.1 iii) jeweils genügen.

iv) Der AN gewährleistet, dass die dem AG bereitgestellten Produkte mit digitalen Elementen mit der CE-Kennzeichnung versehen ist und sie keiner Änderung unterzogen wurden, die ihre Konformität mit dem CRA beinträchtigen.

v) Ist der AN der Auffassung oder hat er Grund zu der Annahme, dass ein Produkt mit digitalen Elementen oder die vom Hersteller festgelegten Verfahren nicht den Anforderungen von Ziffer 3.1 i) und / oder Ziffer 3.1 iii) genügen, stellt er das Produkt dem AG erst dann bereit, wenn die Konformität dieses Produkts und der vom Hersteller festgelegten Verfahren mit den vorgenannten Anforderungen hergestellt ist. Wenn das Produkt mit digitalen Elementen ein erhebliches Cybersicherheitsrisiko birgt, unterrichtet der AN hierüber unverzüglich den AG und den Hersteller. Ferner sorgt der AN dafür, dass unverzüglich die erforderlichen Korrekturmaßnahmen ergriffen werden, um die Konformität des Produktes mit den vorgenannten Anforderungen herzustellen oder um gegebenenfalls das Produkt vom Markt zu nehmen oder zurückzurufen. Der AN wird im Fall von Korrekturmaßnahmen oder eines Rückrufes vollumfänglich und unentgeltlich mit dem AG und den zuständigen Behörden zusammenarbeiten, einschließlich des Austausches nicht-konformer Produkte mit digitalen Elementen.

3.3. Hinsichtlich Forderungen und Ansprüchen, die Dritte wegen der Verletzung der in diesem Abschnitt der Bedingungen (Ziffer 3) niedergelegten Pflichten des AN geltend machen, gilt Ziffer 4.6 entsprechend.

3.4. Hinsichtlich der Mitteilungen des AN, die Pflichten oder Angelegenheiten betreffen, welche in diesem Abschnitt der Bedingungen geregelt sind, gilt Ziffer 4.8 entsprechend.

3.5. Hinsichtlich der Kontrolle der Einhaltung der vertraglichen und / oder gesetzlichen Informationssicherheitsverpflichtungen des AN durch den AG gilt Ziffer 4.9 entsprechend. Darüber hinaus ist der AG berechtigt, die Produkte mit digitalen Elementen jederzeit selbst oder durch Dritte, beispielsweise auch durch Penetrationstests, auf ausnutzbare Schwachstellen zu testen, wobei der AN den AG in angemessener Weise unterstützen wird

3.6. Verletzt der AN eine wesentliche Verpflichtung aus diesen Bedingungen oder erfüllt der AN, soweit auf ihn oder die von ihm bereitgestellten Produkte mit digitalen Elementen anwendbar, die Anforderungen des CRA nicht, ist der AG berechtigt, den jeweiligen Vertrag unmittelbar und ohne Fristsetzung außerordentlich zu kündigen bzw. von dem Vertrag zurückzutreten. Weitergehende gesetzliche und vertragliche Rechte des AG bleiben unberührt.

4. Informationssicherheit von Daten und Netz- und Informationssystemen

4.1. Der AN ergreift geeignete und verhältnismäßige technische und organisatorische Maßnahmen nach dem neuesten Stand der Technik, um die im Zusammenhang mit den bereitgestellten Leistungen verarbeiteten Daten des AG und dessen Netz- und Informationssysteme gegen unbefugten Zugriff zu schützen und die Auswirkungen von Sicherheitsvorfällen auf den AG zu verhindern oder möglichst gering zu halten.

4.2. Der AN stellt dem AG auf Verlangen sämtliche Informationen in Textform zur Verfügung, die dieser zur Durchführung und Dokumentation einer Bewertung der Risiken für die Informationssicherheit im Zusammenhang mit den bereitgestellten Leistungen benötigt. Hierzu zählen

insbesondere Informationen zu den implementierten technischen und organisatorischen Sicherheitsmaßnahmen, ein Verzeichnis der dem AG bereitgestellte IKT-Produkte, -Dienste und -Prozesse, Zertifizierungen, Risikobewertungen, Angaben zu relevanten Subunternehmern, Zugriffsmöglichkeiten, bekannten Schwachstellen. Der AN informiert den AG unverzüglich in Textform über wesentliche Änderungen, die Einfluss auf die Bewertung der Risiken für die Informationssicherheit im Zusammenhang mit den bereitgestellten Leistungen haben oder haben können.

4.3. Der AN hat den AG unverzüglich, spätestens jedoch innerhalb von zwölf (12) Stunden nach Kenntniserlangung des AN, und unentgeltlich über alle eingetretenen oder vermuteten Sicherheitsvorfälle sowie über alle Schwachstellen zu benachrichtigen, die im Betrieb des AN oder bei seinen Dienstleistungen und Produkten entdeckt und/oder aktiv ausgenutzt werden, soweit der AG davon tatsächlich betroffen ist oder in Zukunft betroffen sein könnte. Diese Benachrichtigung enthält, soweit dem AN zu diesem Zeitpunkt bekannt oder mit angemessenem Aufwand feststellbar, mindestens:

i) Datum und Uhrzeit der Kenntniserlangung des Sicherheitsvorfalls bzw. der Schwachstelle;

ii) eine Kurzbeschreibung des Sicherheitsvorfalls bzw. der Schwachstelle einschließlich der betroffenen oder potenziell betroffenen Leistungen, Produkte, Systeme, Daten und Standorte;

iii) eine Einschätzung (1) der tatsächlichen oder möglichen Betroffenheit des AG sowie der Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten, Diensten oder Netz- und Informationssystemen des AG, (2) des Schweregrads und der Auswirkungen, (3) einschlägige Kompromittierungsindikatoren, (4) bislang bekannte Ursachen;

iv) Angaben dazu, ob der Sicherheitsvorfall oder die Schwachstelle auf rechtswidrige oder böswillige Handlungen zurückzuführen sein könnte;

v) die bereits ergriffenen und die geplanten Eindämmungs- und Abhilfemaßnahmen.

Der AN informiert den AG unaufgefordert und fortlaufend über die zur Aufklärung und Behebung des eingetretenen oder vermuteten Sicherheitsvorfalles bzw. der Schwachstelle getroffenen Maßnahmen. Dies beinhaltet sämtliche Informationen, die erforderlich sind, um die Auswirkungen des eingetretenen oder vermuteten Sicherheitsvorfalles bzw. der entdeckten und / oder aktiv ausgenutzten Schwachstelle zu bewerten und um dem AG die Erfüllung seiner gesetzlichen Verpflichtungen, insbesondere im Bereich des Informationssicherheitsrechts, zu ermöglichen, mindestens aber die in i) – v) genannten Informationen.

4.4. Der AN stellt im Falle von ihm mitgeteilten oder öffentlich bekannt gewordenen Sicherheitslücken und Schwachstellen unverzüglich und unentgeltlich ein Sicherheits-Update zur Verfügung oder ergreift sämtliche sonstigen Maßnahmen, die die Sicherheitslücken und Schwachstellen beseitigen.

4.5. Der AN arbeitet auf erstes Anfordern mit den für den AG zuständigen Aufsichtsbehörden zusammen, ermöglicht Kontrollen der Behörden vor Ort und unterstützt den AG angemessen bei behördlichen Kontrollmaßnahmen.

4.6. Der AN stellt den AG auf erstes Anfordern von allen Forderungen und Ansprüchen frei und verteidigt ihn gegen alle Ansprüche, die wegen der Verletzung seiner in diesem Abschnitt der Bedingungen (Ziffer 4) niedergelegten Pflichten durch Dritte geltend gemacht werden. Der AN erstattet dem Auftraggeber alle angemessenen, entstehenden Verteidigungskosten und sonstigen Schäden.

Everllence

4.7. Der AN gewährleistet, dass seine Verträge mit Unterauftragnehmern diesen im Wesentlichen dieselben Anforderungen an die Informationssicherheit auferlegen, wie sie für den AN nach diesem Abschnitt 4 gelten, und dass diese Anforderungen in der Lieferkette angemessen weitergegeben werden.

4.8. Alle Mitteilungen des AN, die Pflichten oder Angelegenheiten betreffen, welche in diesem Abschnitt der Bedingungen geregelt sind, sind an die folgende Kontaktstelle des AG wie folgt zu richten:

a) **Sicherheitsvorfälle** und/oder entdeckte und / oder aktiv ausgenutzte **Schwachstellen** müssen dem Käufer gemäß Ziffer 4.3 unter Verwendung der folgenden funktionierenden E-Mail-Adresse gemeldet werden: **cybersecurity@everllence.com**

b) Jede andere Mitteilung, bei der es sich **nicht** um die Meldung eines Sicherheitsvorfalls und/oder einer entdeckten und / oder aktiv ausgenutzten Schwachstelle gemäß Ziffer 4.3 handelt, ist an den zuständigen Mitarbeiter des Einkaufsteams des Bestellers zu richten, mit dem der Lieferant bezüglich der betreffenden Lieferung in Kontakt steht.

c) Der AN hat seinerseits dem AG eine zentrale Kontaktstelle inklusive einer E-Mail-Adresse mitzuteilen unverzüglich über Änderungen zu informieren.

4.9. Der AG ist berechtigt, die Einhaltung der vertraglichen und / oder gesetzlichen Informationssicherheitsverpflichtungen des AN durch die Einholung von Auskünften und die Abfrage von Nachweisen beim AN, beispielsweise in Form von marktüblichen Zertifizierungen und / oder Eigenerklärungen des Auftragnehmers zu kontrollieren. Der AG ist außerdem berechtigt, die Einhaltung der vertraglichen und / oder gesetzlichen Cybersicherheitsverpflichtungen des AN mittels eines Audits zu überprüfen bzw. mit Unterstützung eines qualifizierten Dritten, der gegenüber dem AG zur Geheimhaltung der Geschäfts- und Betriebsgeheimnisse des AN verpflichtet ist, durchführen zu lassen. Ergibt das Audit eine nicht unerhebliche Verletzung der Informationssicherheitsverpflichtungen des AN, trägt der AN die Kosten des Audits.

4.10. Bei Beendigung des jeweiligen Vertrags hat der AN sämtliche ihm, seinen Mitarbeitenden, Unterauftragnehmern oder sonstigen zur Leistungserbringung eingesetzten Dritten eingeräumten oder von diesen genutzten Zugangs-, Fernwartungs-, Administrations-, Support- und sonstigen Zugriffsberechtigungen auf Systeme, Netz- und Informationssysteme, Anwendungen, Schnittstellen oder Daten des AG unverzüglich zu deaktivieren, zu entfernen oder deren Deaktivierung oder Entfernung zu veranlassen. Dies umfasst insbesondere Benutzer- und privilegierte Konten, Service-Accounts, Passwörter, Zugangsdaten, Zertifikate, Tokens, sowie VPN-, Remote-Access- und Support-Zugänge und sonstige technische Verbindungsartefakte. Der AN hat die vollständige Umsetzung dieser Maßnahmen dem AG auf Verlangen unverzüglich in Textform zu bestätigen und sicherzustellen, dass die vorstehenden Pflichten auch durch seine Unterauftragnehmer und sonstigen eingesetzten Dritten erfüllt werden.