CARIAD
A VOLKSWAGEN GROUP COMPANY

Cyber Security Grundanforderungen vom 17.02.2022 der CARIAD SE (nachfolgend „CSGA“)

Die betroffenen Leistungen des Auftragnehmers zum Projekt (nachfolgend „Projekt“ oder „Projekt-Umfänge“) umfassen (auch) Cyber Security-relevante Umfänge. Der Auftraggeber ist aufgrund regulierungsrechtlicher Anforderungen verpflichtet, seine Produkte (als „Produkt“ sind hierbei alle Gegenstände zu verstehen, die der Auftraggeber in Verkehr bringt und die Projekt-Umfänge enthalten. Dies umfasst insbesondere Fahrzeuge, Ladehardware und Apps) im Hinblick auf Cyber Security umfassend und während des gesamten Produktlebenszyklus abzusichern. In Bezug auf die Projekt-Umfänge ist dies ohne Beteiligung des Auftragnehmers nicht möglich. Der Auftragnehmer erklärt sich daher bereit, gemäß den Regelungen dieses CSGAs seinen Beitrag dazu zu leisten.

Dies vorausgeschickt, vereinbaren die Parteien was folgt:

1. Begriffe

Begriffe in diesem CSGA haben die in Anlage 1 festgehaltene Bedeutung.

2. Systematisches Testing

2.1. Im Themengebiet Systematisches Testing sind durch den Auftragnehmer die folgenden Anforderungen zu erfüllen, die auch in den Konzern Grundanforderungen Software (KGAS, im Projekt gültige Version) enthalten sind. Sie sind dem Auftraggeber in der geforderten Form zu dokumentieren („Security-Nachweis“):

a) Der Auftragnehmer muss auf Anfrage die erhobenen Metriken dem Auftraggeber zur Verfügung stellen. Das Austauschformat wird durch den Auftraggeber festgelegt.

b) Der Auftragnehmer muss dem Auftraggeber Informationen über alle in der gelieferten Software verwendeten Free and Open Source Softwareelemente zur Verfügung stellen.

c) Neben der Anwendung geeigneter Codierrichtlinien oder Modellierungsrichtlinien muss der Auftragnehmer Security-Codierrichtlinien anwenden.

d) Für die Erfüllung der Anforderungen dieses Abschnitts sollten Analyse-Werkzeuge zur Metrik-bzw. Defektanalyse nach Stand der Technik in den Software-Erstellungsprozess integriert werden.

e) Die bekannten Fehler des Projekt-Umfangs sowie deren Auswirkungen müssen dokumentiert sein.

f) Für alle Softwareelemente muss die verwendete Version und ggf. Patch Level dokumentiert sein.

g) Der Projekt-Umfang darf keine bekannten Schwachstellen enthalten. Abweichungen müssen in den Risikoanalysen berücksichtigt und begründet werden.

h) Auf Anfrage des Auftraggebers muss der Auftragnehmer dem Auftraggeber die Möglichkeit einräumen, gemeinsam mit dem Auftragnehmer toolbasierte Analysen über den gesamten Quellcode in Räumen des Auftragnehmers durchzuführen.

i) Ein Security-Nachweis muss vom Auftragnehmer regelmäßig mit jeder Softwarelieferung in Abstimmung mit dem Auftraggeber erbracht werden.

2.2. Das konkrete Nachweisformat, sowie die Liefermodalitäten werden durch den Auftraggeber bereitgestellt und ggf. jährlich bestätigt:

a) Der Security-Nachweis muss eine Zusammenfassung der Ergebnisse der Security-Risikoanalysen beinhalten.

b) Der Security-Nachweis muss aufzeigen, dass die Security-Anforderungen umgesetzt und verifiziert wurden.

c) Der Security-Nachweis muss aufzeigen, dass die Security-Codierrichtlinien eingehalten wurden.

d) Der Security-Nachweis muss aufzeigen, dass der Reaktionsprozess zum Umgang mit identifizierten Schwachstellen und die aktive Überwachung des Lieferumfangs etabliert sind.

3. Penetrationstesting

3.1. Der Auftragnehmer gestattet dem Auftraggeber ausdrücklich und räumt dem Auftraggeber die entsprechenden Rechte ein, die Projekt-Umfänge jederzeit, insb. vor und nach etwaigen Inverkehrbringen der mit den bereitgestellten Projekt-Umfängen ausgestatteten Produkts seitens des Auftraggebers, umfassend auf Cyber Security-Schwachstellen hin zu untersuchen, zu modifizieren und zu testen. Der Auftraggeber darf daher insbesondere

a) selbst,

b) durch Dritte, die von ihm beauftragt sind oder mit dem Auftraggeber zusammenarbeiten oder

c) von sonstigen Dritten im Rahmen etwaig von dem Auftraggeber organisierter Wettbewerbe (einschließlich sog. Bug Bounty – Programme)

jegliche Methoden und Techniken (u.a. Security-/Penetrationstests sowie Analysen, etwa Umgehung von Schutzmaßnahmen, Reverse Engineering, Fuzzing, Sniffing, Spoofing, Eavesdroping und Manipulation, Code Injection/Execution, Disassemblierung) anwenden beziehungsweise anwenden lassen, die dem Auffinden von Schwachstellen dienen können.

3.2. Im Rahmen der Penetrationstests kann sich als mögliche Cyber Security-Schwachstelle auch ein eigentlich nicht vorgesehener Zugriff auf außerhalb der eigentlichen Projekt-Umfänge liegende Systeme und Daten des Auftragnehmers oder Dritte als möglich erweisen. Wird eine solche Zugriffsmöglichkeit festgestellt, erfolgt eine Rücksprache zwischen Auftragnehmer und Auftraggeber vor Fortsetzung der Tests. Dabei wird sich der Auftraggeber bemühen, den tatsächlichen Zugriff auf die Systeme oder Daten soweit möglich zu unterlassen. Der Auftragnehmer erlaubt dem Auftraggeber unter Berücksichtigung der oben beschriebenen Einschränkungen die Testdurchführung auch in dieser Hinsicht ausdrücklich und versichert, dass er die für diese Erlaubnis erforderlichen Verfügungsbefugnisse hat bzw. von Dritten (insbesondere von seinen Lieferanten) eingeholt hat.

3.3. Bei einer vertraglich zulässigen Verwendung der Projekt-Umfänge durch andere VW-Konzernunternehmen, dürfen auch diese die unter dieser Ziffer 3 genannten Handlungen ausüben.

3.4. Die Pflichten des Auftragnehmers bleiben hiervon unberührt. Weder das Recht des Auftraggebers, Tests durchzuführen noch die tatsächliche Durchführung von Tests schränken die Pflichten des Auftragnehmers gegenüber dem Auftraggeber oder Dritten ein oder begründen eine Mitverantwortung des Auftraggebers.

4. Incident/Vulnerability Management

4.1. Der Auftragnehmer muss eine Anlaufstelle für einen bidirektionalen Reaktionsprozess zum Umgang mit *Cyber Security Meldungen* etablieren und innerhalb einer angemessenen Zeit auf Anfragen des Auftraggebers reagieren. Der Auftraggeber und der Auftragnehmer einigen sich auf jeweils eindeutige Referenzen, die bei der Kommunikation von einzelnen Cyber Security Meldungen herangezogen werden. Sollte der Auftragnehmer Unterauftragnehmer im Rahmen des Projekts einsetzen, so verpflichtet der Auftragnehmer die Unterauftragnehmer, vergleichbare Anlaufstellen einzurichten, um je nach Relevanz-oder Dringlichkeitsebene der Cyber Security Meldung angemessen schnell und in angemessener Detailtiefe reagieren zu können.

4.2. Der Auftragnehmer ist verpflichtet einen *Verantwortlichen für die Sicherheit* seines Projekt-Umfanges (*Chief Information Security Officer, Chief Product Security Officer*, o.ä.) und eine Funktionsmail Adresse als Kontakt für Meldungen durch den Auftraggeber zu benennen, mit der Möglichkeit zur verschlüsselten Kommunikation (siehe auch Einkaufsbedingungen). Die Informationen müssen in der Lieferantendatenbank (LDB – zu erreichen über die One Konzern Business Plattform) durch den Auftragnehmer hinterlegt und bei Bedarf aktualisiert werden.

4.3. Erhält der Auftragnehmer Kenntnis über Fälle der Kategorie *Weakness* oder höher, oder hat den Grund zur Annahme, dass ein Fall der Kategorie *Vulnerability* oder höher in den Projekt-Umfängen enthalten ist, benachrichtigt er den Auftraggeber unverzüglich (nachfolgend „**Meldung**“). Bei Verdacht zu Fällen in,

a) bereits *in Verkehr* gebrachten Produkten des Auftraggebers

b) IT-Systemen die dazu dienen, um den Beauftragungsumfang zu realisieren

c) Entwicklung befindlichen Fahrzeugprojekten

d) allen sonstigen Umfängen im Zusammenhang mit dem Projekt-Umfang erfolgt die Meldung an das Incident Team des Auftraggebers unter folgender Emailadresse:

CARIAD Kontakt für Vulnerabilities: vuln@cariad.technology

CARIAD Kontakt für Incidents: sirt@cariad.technology

4.4. Für jede Meldung stellt der Auftragnehmer innerhalb eines angemessenen Zeitraums eine Erstanalyse zur Verfügung. Die konkreten Inhalte der Erstanalyse umfassen mindestens die Kategorisierung und Beschreibung des Verdachtsfalls, Beschreibung des Angriffsweges, Beschreibung der Auswirkung, Einschätzung der Eintrittswahrscheinlichkeit, die betroffenen Produkte, Umfänge, Bauteile, Komponenten, Systemen und Projekte einschließlich des konkreten Software-Stands und des voraussichtlichen Risikos sowie einen Vorschlag zu möglichen Gegenmaßnahmen inkl. Zeitplan und Verantwortlichkeiten. Im Bedarfsfall kann der Umfang der Erstanalyse in Abstimmung zwischen Auftragnehmer und Auftraggeber erweitert werden.

4.5. Innerhalb einer durch den Auftraggeber festgelegten, angemessenen Frist führt der Auftragnehmer anschließend in enger Abstimmung mit dem Auftraggeber eine detaillierte technische Analyse durch, erarbeitet konkrete Gegenmaßnahmen sowie einen Umsetzungsplan. Die Erstellung einer Behebung der Problemursachen hat je nach Dringlichkeitsebene der Meldung sofort (Kategorien *Incident* oder höher) zu erfolgen oder (Kategorie *Vulnerability* und darunter) erfolgt erst nach einem Wirksamkeitsnachweis und der schriftlichen Anweisung des Auftraggebers. Bei Meldungen von Dringlichkeitsebenen *Vulnerability* und darunter erfolgt vor Erstellung der Behebungen stets zunächst eine Klärung der Beauftragungs- oder Bearbeitungsart, i.e. ob die Leistung unter Gewährleistung, Support, Einzelbeauftragung o.ä. fällt. Der Auftragnehmer stellt zu allen Aspekten eine ausführliche Dokumentation zur Verfügung.

4.6. Sollte durch den Auftragnehmer eine Kommunikation nach außen geplant sein, die den Auftraggeber betrifft, ist dies mit dem Incident Team des Auftraggebers abzustimmen.

4.7. Der Auftragnehmer muss auf Anfrage durch den Auftraggeber auf eigene Kosten in angemessenem Umfang Hard- und/oder Software-Muster zur Verfügung stellen, die es dem Auftraggeber ermöglichen, die Schwachstelle sowie die bereitgestellte Lösung zu verifizieren.

4.8. Der Auftragnehmer muss für die Projekt-Umfänge einen Prozess zur aktiven und kontinuierlichen Überwachung des Cyber Security Status etablieren und gegenüber dem Auftraggeber nachweisen gemäß VDA „Automotive Cybersecurity-Managementsystem-Audit".

4.9. Die Angemessenheit eines Zeitraums bemisst sich insbesondere daran, dass der Auftraggeber seinen gesetzlichen und behördlichen (Melde-)pflichten fristgerecht unter Einbeziehung Auftraggeber interner Bearbeitungszeiten nachkommen kann.

4.10. Anderweitige Informationspflichten des Auftragnehmers, z.B. Lieferantenselbstanzeige bei Beschaffung und Kaufteilqualität, bleiben unberührt.

5. Support Zeitraum

5.1. Der Auftragnehmer muss in der Lage sein und damit sicherstellen, dass er Support- und Wartungsdienste zur Behebung von Cyber Security-Schwachstellen für einen Zeitraum von fünfzehn (15) Jahren nach Produktionsende ("EOP") (s. KGAS) erbringen kann, soweit nicht in der Beauftragung (z.B. im Lastenheft) für das konkrete Projekt ein anderer Zeitraum festgelegt ist. Dies umfasst die Fähigkeit alle zur Software zugehörigen Spezifikationen sowie den Quellcode anzupassen, die entsprechenden Binärdateien zu erstellen und alle Teststufen durchzuführen. EOP bedeutet in diesem Zusammenhang das Produktionsende des Produktes, in das die Projekt-Umfänge eingebaut oder genutzt werden.

5.2. Der Auftraggeber kann eine Hinterlegung des Source-Codes inklusive der vollständigen, notwendigen Entwicklungsumgebung mit SOP und allen folgenden Major Releases bei einem vom Auftraggeber bestimmten unabhängigen Dritten („Hinterlegungsstelle") verlangen. Der Auftragnehmer hat mit Hinterlegung kein Rückforderungsrecht bis zum Ablauf des Support-Zeitraums, gleich aus welchem Rechtsgrund. Die Hinterlegungsstelle wird im Augenblick der Hinterlegung Inhaber der Hinterlegungsgegenstände. Die Hinterlegungsstelle ist berechtigt einzig für den Fall der Insolvenz des Auftragnehmers oder der Geschäftsfeldaufgabe durch den Auftragnehmer, dem Auftraggeber (i) das übertragbare Eigentum an den Hinterlegungsgegenständen, soweit das Eigentum an diesen übertragbar ist, insbesondere an der verkörperten Dokumentation und den hinterlegten Datenträgern und (ii) sofern an den Hinterlegungsgegenständen kein Eigentum eingeräumt werden kann, insbesondere an der auf den hinterlegten Datenträgern abgebildeten Software,

das Recht zur unentgeltlichen, inhaltlich, räumlich und zeitlich uneingeschränkten Nutzung, Vervielfältigung und Umarbeitung, insbesondere Fehlerbeseitigung, Änderung, Erweiterung und Herstellen von Schnittstellen, sowie zur Unterlizenzierung an Konzernunternehmen zum Zwecke der Beseitigung von Mängeln und Schwachstellen einzuräumen.

6. Bereitstellung von Hardware- und Software-Informationen

6.1. Wenn die Projekt-Umfänge Bestandteil von Produkten werden, muss der Auftragnehmer dem Auftraggeber im Rahmen der Hardware-/ Software-Dokumentation (vgl. auch Bauteil- und Querschnittslastenhefte) für das Projekt mindestens folgende Informationen zur Verfügung zu stellen:

a) Hardware-Informationen sind gemäß vertraglicher Vereinbarungen (u.a. eNA) im System HAMON durch den TIER 1 bereitzustellen, aus Cyber Security Sicht insbesondere:
   - Projektdaten des Bauteils (intelligente Bauelemente, z. B. Controller, Prozessoren)
   - Bauelementehersteller
   - Herstellerteilenummern der Bauelemente

b) Folgende Software-Informationen sind bereitzustellen:
   - Name und Version Bootloader
   - Name und Version Betriebssystem
   - Auflistung aller verwendeten Treiber
   - Informationen über jede Software (auf dem Steuergerät) (unabhängig von Eigenentwicklung, Free and Open Source Software, Zukauf von Software)
     - Software-Modul/Library Hersteller
     - Software-Modul/Library Bezeichnung
     - Software-Modul/Library Versionsnummer
     - Software-Modul/Library Verweis/Link auf Bezugsquelle
     - Software-Modul/Library Hashwert inkl. Hashverfahren

Die erstmalige Eingabe von Software-Informationen erfolgt durch den Auftragnehmer im Rahmen der Produktentwicklung und -qualifizierung. Die vollständigen Daten des Serienstands müssen bis zur Entwicklungsfreigabe in den relevanten Systemen bereitgestellt werden. Sollten im Rahmen der Supportprozesse Änderungen im Lieferumfang entstehen, so sind diese in der Dokumentation durch den Auftragnehmer nachzuziehen.

6.2. Anderweitige Informationspflichten des Auftragnehmers, z.B. für im Projekt-Umfang enthaltene Free and Open Source Software oder Befüllungspflicht in HAMON, bleiben unberührt.

7. Absicherung der Zulieferkette

Der Auftragnehmer stellt sicher, dass alle Unterauftragnehmer, die im Projekt mitarbeiten oder deren Komponenten im Rahmen des Projekts verwendet werden, ebenso zur Einhaltung dieser CSGA verpflichtet sind. Er haftet für das Verschulden seiner Unterauftragnehmer wie für eigenes Verschulden.

8. Sonstiges

8.1. Die Vertragspartner sind sich darüber einig, dass diese CSGA auch auf solche Projekt-Umfänge Anwendung findet, die im Rahmen des Projekts bereits vor Unterzeichnung dieser CSGA erbracht wurden.

8.2. Änderungen und Ergänzungen dieser CSGA bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für eine Änderung dieser Schriftformklausel.

8.3. Sollte eine Bestimmung dieser CSGA unwirksam sein oder werden, so wird dadurch die Gültigkeit des der CSGA im Übrigen nicht berührt. Die Parteien sind verpflichtet, über eine die unwirksame Bestimmung ersetzende Regelung nach Treu und Glauben zu verhandeln.

8.4. Es gilt ausschließlich das Recht der Bundesrepublik Deutschland, soweit nicht etwas anderes vereinbart ist. Die Anwendung des Übereinkommens der Vereinten Nationen vom 11.4.1980 über Verträge über den internationalen Warenkauf ist ausgeschlossen.

Anlagen:

Anlage 1: Ergänzende Unterlage zu Begrifflichkeiten und Definitionen

Anlage 1: Ergänzende Unterlage zu Begrifflichkeiten und Definitionen

Bei der Auslegung und Anwendung der Cyber Security Grundanforderungen gelten insbesondere die folgenden Begriffsdefinitionen:

BTV	Bauteilverantwortlicher
Bug Bounty - Programm	Initiative zur Aufdeckung von Fehlern und Schwachstellen mit Sach- oder Geldpreisen für die Entdecker
Chief Information Security Officer	Ansprechpartner für die Sicherheit von Informationen in seinem Unternehmen
Chief Product Security Officer	Ansprechpartner für die Sicherheit seines gelieferten Produktes
Code Injection/Execution	Einbringen / Ausführen von Code durch Verarbeitung ungültiger Eingabedaten
Codierrichtlinien	Regeln & Standards zur Verbesserung der Softwarequalität
CSGA	Cyber Security Grundanforderungen
Cyber Security Meldungen	Unterscheidung von 5 Dringlichkeitsstufen
Cyber Security Information	Alle Informationen die im Rahmen des Monitoring-Prozesses erfasst werden und deren Cyber Security Relevanz (potentielle Schwachstelle) noch nicht eingestuft ist. Dringlichkeitsstufe 1
Cyber Security Event	Cyber Security Information, welche als potentielle Schwachstellen (ohne Risikobewertung) für das Unternehmen oder seine Produkte als relevant eingestuft wird und eine weitere Behandlung (CSI-Prozess, Information Assessment, etc.) bedingt. Dringlichkeitsstufe 2

Cyber Security Weakness	Fehler im Security-Konzept oder in der Implementierung (technisch, organisatorisch, prozessual) eines Assets. Dringlichkeitsstufe 3
Cyber Security Vulnerability	Weakness eines Assets, die durch eine oder mehrere Bedrohungen (Threat) ausgenutzt werden kann. Dringlichkeitsstufe 4
Cyber Security Incident	Einzelne oder eine Reihe unerwünschter oder unerwarteter Cyber Security Ereignisse, die die Ausnutzung einer Vulnerability belegen und einen signifikanten Einfluss auf die Security eines Bauteils/Funktion haben könnten (z. B. eine Schädigung des Assets hervorrufen). Dringlichkeitsstufe 5
Disassemblierung	Umwandlung von binärem Maschinencode in lesbare Assemblersprache
Eavesdropping und Manipulation	Mitlesen bzw. Modifizierung von ausgetauschten digitalen Daten
eNA	Electronic Nomination Agreement
Erhobene Metriken	Vorgegebene Metriken zur Bewertung der Softwarequalität (siehe KGAS)
EOP	End of Production
Free and Open Source Software	Free and Open Source Software (FOSS) ist jegliche Software, die unter Nutzungs- und Lizenzbestimmungen vertrieben wird, zu deren wesentlicher Verpflichtung typischerweise die Weitergabe oder Offenlegung des Quellcodes der Software bei deren Verbreitung gehört. Free and Open Source Software ist eine Variante von Software von Dritten.
Fuzzing	Fuzzing ist eine Technik zum Testen von Software durch ungültige, unerwartete oder zufällige Eingabedaten

Gelieferte Software	Gelieferte Software, ist die vom Auftragnehmer gelieferte Software (u.a. Auftragnehmer Software, Beistellsoftware, Software von Dritten).
HAMON	Plattform des VW Konzerns für Informationen zu elektrischen und elektronischen Bauelementen
Incident Team	Das Incident Team koordiniert die Bearbeitung von Cyber Security Meldungen
Informationen der Free and Open Source Software	Für jedes verwendete FOSS-Element müssen mindestens die folgenden Informationen enthalten sein: ● Name ● Eindeutige Versionskennzeichnung ● Lizenzname mit eindeutiger Lizenzversionsnummer ● Vollständiger Lizenztext ● Download-Link des Lizenztexts sowie des Quellcodes inklusive letztem Zugriffsdatum ● Quellcode und Urheberrechtsvermerke ● Information, ob Quellcode und Urheberrechtsvermerke weiterzugeben bzw. zu veröffentlichen sind ● Etwaige Subelemente, die zur Verwendung des Softwareelements erforderlich sind, inklusive der vorgenannten Angaben zur Lizenzierung
Konzern Grundanforderung Software (KGAS)	Konzern Querschnittslastenheft zur Regelung der Softwarequalität
Sniffing	Technik zur Analyse von Netzwerkverkehr
Spoofing	Technik zur Verschleierung der eigenen Identität in Netzwerken
System	Das System ist der gesamte vom Auftragnehmer zu erbringende Lieferumfang. Das System besteht aus Systemelementen.

Systemelement	Ein Systemelement ist ein logischer Bestandteil eines Systems. Systemelemente sind in der Systemarchitekturspezifikation beschrieben. Typische Systemelemente sind Software, Hardware (z. B. Sensoren, Aktoren, Leiterplatten, Bauteile und Verbindungen) und Mechanik (z. B. Gehäuse).
Verantwortlichen für die Sicherheit	Ansprechpartner für die Sicherheit seines gelieferten Produktes