Informationssicherheitsanforderungen für Lieferanten und Dienstleister (Stand: März 2023)

Inhaltsverzeichnis

Weitergabe sowie Vervielfältigung dieser vertraulichen Unterlage(n), Verwertung und Mitteilung ihres Inhaltes ist nicht ohne unsere vorherige schriftliche Genehmigung gestattet. Zuwiderhandlungen verpflichten zu Schadensersatz. Alle Rechte für den Fall der Patenterteilung oder Gebrauchsmuster-Eintragung vorbehalten.

The copying, use, distribution or disclosure of the confidential and proprietary information contained in this document(s) is strictly prohibited without prior written consent. Any breach shall subject the infringing party to remedies. The owner reserves all rights in the event of the grant of a patent or the registration of a utility model or design.

1 Zweck

Informations- und IT-Sicherheit ist für uns und unsere Kunden ein wesentlicher Bestandteil der Geschäftsprozesse und der Lieferketten. OEMs (Original Equipment Manufacturer) arbeiten in der gesamten Wertschöpfungskette mit einer Vielzahl von Unternehmen zusammen, um die Entwicklung und Herstellung der Erzeugnisse zu gewährleisten. Dabei werden u.a. vertrauliche Informationen, wie z. B. der Entwurf eines Prototyps an die Lieferanten/Dienstleister weitergegeben. Auch die Produktionsprozesse sind hochgradig IT-gestützt und der OEM verlässt sich auf den Schutz der IT-Systeme vor Ausfällen, wie z. B. den Befall durch einen Erpressungstrojaner. Folglich müssen die Informationen und IT-Systeme angemessen geschützt werden, sodass der Austausch von Daten und die Verfügbarkeit der IT-Systeme entlang der Zuliefererkette nicht gefährdet ist. Aufgrund dessen verlangen OEMs von uns und unseren Lieferanten/Dienstleistern ein funktionierendes Informationssicherheitsmanagementsystem (ISMS), um ihre Informationen angemessen zu schützen und die Produktionsprozesse nicht zu unterbrechen.

2 Schutzbedarfslevel und Nachweispflicht

Die Umsetzung von Informations- und IT-Sicherheitsanforderungen ist abhängig von den Informationen, die wir entlang der Wertschöpfungskette austauschen. Wir haben diesen Informationsaustausch in die vom Verband der deutschen Automobilindustrie (VDA) harmonisierten Informations-Klassifizierungsstufen (öffentlich, intern, vertraulich und streng vertraulich) unterteilt. In Abhängigkeit dazu bestimmt sich die Anforderung an den Schutzbedarf und daraus leiten wir wiederum die vorzulegenden Zertifikate ab. Die Information, welches Schutzniveau der Lieferant/Dienstleister zu erfüllen hat, wird diesem separat mitgeteilt.

Die Lieferanten/Dienstleister haben **12 Monate nach Erhalt dieser Information** in Form einer Aufforderung durch die Brose Unternehmensgruppe (bspw. per E-Mail) die Möglichkeit, die entsprechenden Zertifikate unter partner-informationsecurity@brose.com einzureichen. Nachweise über eine TISAX Zertifizierung sind über das ENX-Portal mit der Brose Participant-ID P1X21X zu teilen. Nach Ablauf der Frist behält sich Brose vor, das Fehlen von Zertifikaten in der Lieferantenbewertung zu berücksichtigen.

Vertraulichkeitsstufe der Information	**Schutzbedarfslevel**	**Gefordertes Zertifikat* (Mindestanforderung)**
Öffentlich	Kein Schutzbedarf	N/A
Intern	Normaler Schutzbedarf	Befüllung der VDA ISA Selbstauskunft mit Unterschrift des Managements
Vertraulich	Hoher Schutzbedarf	Auswahlmöglichkeiten: • TISAX nach VDA ISA gemäß Assessment Level 2 • TPISR • SOC 2 Typ 2 Report (in Abhängigkeit des Scopes)
Streng vertraulich	Sehr hoher Schutzbedarf	Auswahlmöglichkeiten: • TISAX nach VDA ISA gemäß Assessment Level 3 • ISO/IEC 27001 (in Abhängigkeit des Scopes)
Streng vertraulich + Prototypen	Sehr hoher Schutzbedarf	TISAX nach VDA ISA gemäß Assessment Level 3+

*Selbstverständlich können auch die Anforderungen für einen höheren Schutzbedarf nachgewiesen werden.

Weitergabe sowie Vervielfältigung dieser vertraulichen Unterlage(n), Verwertung und Mitteilung ihres Inhaltes ist nicht ohne unsere vorherige schriftliche Genehmigung gestattet. Zuwiderhandlungen verpflichten zu Schadensersatz. Alle Rechte für den Fall der Patenterteilung oder Gebrauchsmuster-Eintragung vorbehalten.

The copying, use, distribution or disclosure of the confidential and proprietary information contained in this document(s) is strictly prohibited without prior written consent. Any breach shall subject the infringing party to remedies. The owner reserves all rights in the event of the grant of a patent or the registration of a utility model or design.

3 Definitionen

TISAX nach VDA ISA
TISAX steht für Trusted Information Security Assessment Exchange und ist ein vom Verband der Automobilindustrie (VDA) definierter Standard für Informationssicherheit, dessen Anforderungen in einem Fragenkatalog (VDA ISA) verankert sind. Die Anforderungen basieren auf der internationalen Industrie-Norm ISO/IEC 27001 und wurden an die Automobil-Welt angepasst. Dieser deckt die Themenbereiche Informationssicherheit, Prototypen- und Datenschutz ab. Die ENX Association agiert in diesem System als Governance-Organisation - lässt Prüfdienstleister zu und überwacht die Qualität der Prüfungen. Voraussetzung hierfür ist die Anmeldung bei ENX. (ref.: TISAX)

TPISR
Die Automotive Industry Action Group (AIAG), der vor allem große US-Unternehmen der Automobilindustrie angehören, hat einen Cybersecurity-Standard für Zulieferer veröffentlicht. TPISR, steht für Third-Party Information Security Requirements, definiert Mindestanforderungen an die IT-Sicherheit von Firmen, die geschützte Informationen von Automobilunternehmen erhalten, diese speichern und verarbeiten. TPISR erfüllt damit eine ähnliche Rolle für US-Unternehmen wie TISAX in der deutschen Autoindustrie, obgleich die Qualität aufgrund der fehlenden unabhängigen Prüfung der Angaben deutlich geringer ausfällt. (ref.: TPISR)

SOC 2 Typ 2 Report
Die Service Organization Control (SOC) Reports sind übergreifende Rahmenwerke, die das amerikanische Institut für Wirtschaftsprüfer (AICPA) als Standard zur Verfügung stellt, um Dienstleister bzw. Serviceorganisationen nach festgesetzten Regeln zu auditieren. Bei diesen Reports geht es um interne Kontrollen in Bezug auf Sicherheit, Verfügbarkeit, Integrität bzw. Vertraulichkeit (Datenschutz). Der Report Typ II prüft darüber hinaus auch jeweils die Wirksamkeit der implementierten Kontrollen über einen definierten Zeitraum.

ISO/IEC 27001
Die internationale Norm ISO/IEC 27001 spezifiziert die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung des Kontexts einer Organisation. Darüber hinaus beinhaltet die Norm Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken entsprechend den individuellen Bedürfnissen der Organisation. Hierbei werden sämtliche Arten von Organisationen (z. B. Handelsunternehmen, staatliche Organisationen, Non-Profitorganisationen) berücksichtigt.

4 Kontakt

Bei Fragen hierzu kontaktieren Sie uns bitte per E-Mail: partner-informationsecurity@brose.com

Weitergabe sowie Vervielfältigung dieser vertraulichen Unterlage(n), Verwertung und Mitteilung ihres Inhaltes ist nicht ohne unsere vorherige schriftliche Genehmigung gestattet. Zuwiderhandlungen verpflichten zu Schadensersatz. Alle Rechte für den Fall der Patenterteilung oder Gebrauchsmuster-Eintragung vorbehalten.

The copying, use, distribution or disclosure of the confidential and proprietary information contained in this document(s) is strictly prohibited without prior written consent. Any breach shall subject the infringing party to remedies. The owner reserves all rights in the event of the grant of a patent or the registration of a utility model or design.