Anforderungen an Cybersicherheit und Datenschutz für Auftragnehmer

Stand: Juni 2025

Es gelten folgende Anforderungen an den Lieferanten/Dienstleister und deren Subunternehmer (im Folgenden „Auftragnehmer"):

I. Anforderungen an die Organisation des Auftragnehmers, sowie an Dienstleistungen die an SMA-Systemen/Eigentum durchgeführt werden:

- ISO 27001 Zertifizierung (mit Scope aller relevanten Bereiche)
- Falls keine ISO 27001 Zertifizierung erfüllt wird, müssen folgende Anforderungen erfüllt werden:

1. Datenschutz und Vertraulichkeit

1.1. Der Auftragnehmer ist verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen und aufrechtzuerhalten, um vertrauliche Informationen und Kundendaten vor unbefugter oder rechtswidriger Verarbeitung sowie vor versehentlichem Verlust, Zerstörung, Beschädigung, Veränderung oder Offenlegung zu schützen.

1.2. Der Auftragnehmer muss sicherstellen, dass alle Mitarbeiter, die Zugang zu Kundendaten haben:

- Eine angemessene Sicherheitsüberprüfung durchlaufen haben
- Schriftliche Vertraulichkeitsverpflichtungen eingegangen sind
- Mindestens einmal jährlich eine Schulung zum Thema Informationssicherheit absolviert haben

2. Sicherheitsstandards und deren Einhaltung

2.1. Der Auftragnehmer ist verpflichtet folgendes zu gewährleisten:

- ISO 27001 Zertifizierung oder ein gleichwertiges Sicherheitsmanagement
- Einhaltung relevanter Industrienormen, einschließlich IEC 62443 für industrielle Steuerungssysteme
- Regelmäßige Sicherheitsbewertungen und Penetrationstests durch Dritte
- SOC 2 Type II Berichte (falls zutreffend)

SMA Solar Technology AG • Sonnenallee 1 • 34266 Niestetal • Germany • Tel. +49 561 9522 - 0 • E-Mail: info@SMA.de • www.SMA.de

2.2. Der Auftragnehmer muss auf Anfrage Nachweise über die Einhaltung vorlegen und SMA innerhalb von 48 Stunden über den Verlust des Zertifizierungsstatus informieren.

3. Sicherheitsvorfallmanagement

3.1. Der Auftragnehmer ist verpflichtet:

- Einen dokumentierten Plan zur Reaktion auf Sicherheitsvorfälle zu führen
- SMA innerhalb von 24 Stunden nach Entdeckung eines Sicherheitsvorfalls, der Kundendaten oder -systeme betrifft oder betreffen könnte, zu benachrichtigen
- Detaillierte Vorfallberichte innerhalb von 72 Stunden nach Entdeckung bereitzustellen
- Vollständig mit jeder von SMA initiierten Untersuchung zu kooperieren

3.2. Der Auftragnehmer muss in der Lage sein:

- Sicherheitsereignisse rund um die Uhr zu erkennen und darauf zu reagieren (24/7/365)
- Forensische Beweismittel zu sichern
- Sofortige Eindämmungsmaßnahmen zu ergreifen

4. Zugangskontrolle und Identitätsmanagement

Der Auftragnehmer ist verpflichtet:

- Die Rollenbasierte Zugriffskontrolle (RBAC) zu implementieren
- Multi-Faktor-Authentifizierung für alle privilegierten Zugriffe zu verwenden
- Zugriffsrechte vierteljährlich zu überprüfen
- Protokolle über alle Zugriffe auf SMA Systeme und -daten zu führen
- Den Zugang innerhalb von 24 Stunden nach Beendigung des Arbeitsverhältnisses zu widerrufen

5. Sicherheit der Lieferkette

Der Auftragnehmer ist verpflichtet:

SMA Solar Technology AG • Sonnenallee 1 • 34266 Niestetal • Germany • Tel. +49 561 9522 - 0 • E-Mail: info@SMA.de • www.SMA.de

- Ein Inventar aller Unterlieferanten zu führen, die auf Kundendaten zugreifen oder diese verarbeiten könnten
- Sicherzustellen, dass Unterlieferanten vertraglich an gleichwertige Sicherheitsanforderungen gebunden sind
- Sicherheitsbewertungen der Unterlieferanten mindestens einmal jährlich durchzuführen

6. Sichere Entwicklung und Betrieb

Für jede Software oder Firmware:

- Implementierung von SDLC-Praktiken (Secure Development Lifecycle)
- Sicherheitstests vor jeder Veröffentlichung durchführen
- Zeitnahe Sicherheitsupdates und -patches bereitstellen
- Aufrechterhaltung sicherer Code-Signing-Prezesse
- Alle Drittanbieterkomponenten und -abhängigkeiten dokumentieren
- Der Privacy-by-Design-Ansatz und der Security-by-Default-Ansatz sind verpflichtend

7. Geschäftskontinuität und Notfallwiederherstellung

Der Auftragnehmer ist verpflichtet:

- Dokumentierte Geschäftsfortführungs- und Notfallwiederherstellungspläne aufrechtzuhalten
- Diese Pläne mindestens einmal jährlich zu testen
- Sicherzustellen, dass die „Recovery Time Objectivies" (RTO) den Anforderungen von SMA entsprechen
- Alle Kundendaten nach angemessenen Zeitplänen zu sichern

8. Prüf- und Bewertungsrechte

SMA behält sich das Recht vor:

- Sicherheitsbewertungen mit einer Vorankündigung von 5 Werktagen durchzuführen
- Nachweise über Sicherheitskontrollen und deren Wirksamkeit anzufordern

SMA Solar Technology AG • Sonnenallee 1 • 34266 Niestetal • Germany • Tel. +49 561 9522 - 0 • E-Mail: info@SMA.de • www.SMA.de

- Die Behebung identifizierter Sicherheitsprobleme innerhalb vereinbarter Fristen zu verlangen
- Den Vertrag bei schwerwiegenden Sicherheitsverletzungen zu kündigen

9. Datenrückgabe und -vernichtung

Bei Vertragsbeendigung ist der Auftragnehmer verpflichtet:

- Alle Kundendaten in einem vereinbarten Format zurückzugeben
- Alle Kopien der Kundendaten sicher zu vernichten
- Eine schriftliche Bestätigung der Vernichtung vorzulegen
- Keine Kopien, es sei denn, diese sind gesetzlich vorgeschriebenen, aufzubewahren

10. Sicherheitsverbesserung und -entwicklung

Der Auftragnehmer ist verpflichtet:

- Sicherheitsbedrohungen kontinuierlich zu überwachen und zu bewerten
- Sicherheitskontrollen zu verbessern, wenn sich Bedrohungen entwickeln
- Sicherheitsverbesserungen gemäß den Empfehlungen von SMA umzusetzen
- Vierteljährlich an Sicherheitsüberprüfungen von SMA teilzunehmen

11. Einhaltung von Sicherheitsgesetzen und -vorschriften

Der Auftragnehmer ist verpflichtet die folgende Anforderung einhalten:

- Falls zutreffend, Anforderungen zum Schutz kritischer Infrastrukturen

SMA Solar Technology AG • Sonnenallee 1 • 34266 Niestetal • Germany • Tel. +49 561 9522 - 0 • E-Mail: info@SMA.de • www.SMA.de

II. Anforderungen an die Produkte (betrifft Komponenten / Inbound-Geräte und „White Label"-Geräte):

1. Bei SMA sind Cybersicherheit und Datenschutz integraler Bestandteil unserer Lösungen und Produkte, insbesondere vor dem Hintergrund der zunehmenden Konnektivität, Systemintegration und der sich entwickelnden gesetzlichen Anforderungen und Standards.

2. Der sichere Betrieb von Energiesystemen, der Schutz vor Cyberangriffen und das Vertrauen in ein sicheres Datenmanagement sind entscheidend für eine zukünftige Energieversorgung im Zeitalter der Digitalisierung und Künstlicher Intelligenz. Die Vision unserer Organisation ist es, die Energieversorgung der Zukunft durch die Bereitstellung cybersicherer Produkte, Lösungen und Dienstleistungen unverwundbar zu machen, ohne deren Funktionalität und Nutzbarkeit einzuschränken und die Daten zu schützen.

3. Im Kontext von Inbound-Projekten und Inbound-Produkten setzt SMA auf die Zusammenarbeit des Auftragnehmers, um die Konformität mit spezifischen Anforderungen zu erfüllen, und der Auftragnehmer sichert SMA diese Erfüllung zu. Diese Anforderungen wurden im Rahmen einer umfassenden Risikobewertung für die vom Auftragnehmer bereitgestellten Inbound-Projekte und Inbound-Produkte festgelegt und sind nachstehend detailliert aufgeführt.

SMA Solar Technology AG • Sonnenallee 1 • 34266 Niestetal • Germany • Tel. +49 561 9522 - 0 • E-Mail: info@SMA.de • www.SMA.de

III. Anforderungen an die Cybersicherheit für Auftragnehmer von Inbound- Geräten und -Komponenten:

1. Der Auftragnehmer versichert, dass alle Funktionen innerhalb der bereitgestellten Inbound-Geräte und -Komponenten mit dem vereinbarten Verwendungszweck übereinstimmen. Dies bezieht sich insbesondere auf das Fehlen von Funktionen, die darauf ausgelegt sind, andere Komponenten oder Systeme durch Fehlfunktionen und fehlerhafte Bedienung absichtlich zu beschädigen.

2. Der Auftragnehmer bestätigt die Einhaltung internationaler Standards in den Bereichen Cybersicherheit und Datenschutz, insbesondere der in Deutschland, EU und USA, während der gesamten Produktentwicklung und -produktion und verpflichtet sich, die Einhaltung sofort und unaufgefordert nachzuweisen. Insbesondere bestätigt der Auftragnehmer die Einhaltung der ISO 27001:2022 (Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmanagementsysteme – Anforderungen).

3. Der Auftragnehmer verpflichtet sich, regelmäßige Schulungen zur Cybersicherheit und zum Datenschutz für Mitarbeiter in relevanten Bereichen durchzuführen, um das Bewusstsein für potenzielle Bedrohungen zu schärfen.

4. Der Zugang zu den Inbound-Produkten ist auf autorisiertes Personal beschränkt, das an der Hardware- und Softwareentwicklung sowie der Produktion beteiligt ist.

5. Alle von SMA zur Verfügung gestellten Komponenten und Daten dürfen nur für die im Vertrag ausdrücklich vereinbarten Zwecke verwendet werden. Reverse Engineering und die Weitergabe von Daten an Dritte ohne vorherige schriftliche Zustimmung von SMA sind strengstens untersagt. Im Falle eines Verstoßes gegen diese Einschränkung haftet der Auftragnehmer für alle Schäden, die SMA entstehen können, soweit dies nach geltendem Recht zulässig ist.

6. Der Auftragnehmer verpflichtet sich, auf Verlangen von SMA regelmäßig und jederzeit Risikobewertungen durchzuführen, um potenzielle Cybersicherheitslücken zu identifizieren, geeignete Risikominderungsstrategien zu implementieren und diese Informationen SMA unverzüglich und unaufgefordert zur Verfügung zu stellen.

SMA Solar Technology AG • Sonnenallee 1 • 34266 Niestetal • Germany • Tel. +49 561 9522 - 0 • E-Mail: info@SMA.de • www.SMA.de

7. Der Auftragnehmer wird alle Vorgänge im Zusammenhang mit Cybersicherheit und Datenschutz dokumentieren und diese Dokumentation, soweit gesetzlich zulässig, sofort und unaufgefordert an SMA zur Verfügung stellen.

8. Der Auftragnehmer erklärt, dass zum Zeitpunkt der Lieferung an SMA keine bekannten Schwachstellen in den zur Verfügung gestellten Inbound-Geräten und -Komponenten bekannt sind und verpflichtet sich, diese Behauptung beispielsweise durch eine „Software Bill of Materials" (SBOM) zu untermauern.

9. Der Auftragnehmer verpflichtet sich, SMA innerhalb von 36 Stunden nach Entdeckung über neu festgestellte Schwachstellen in den zur Verfügung gestellten Inbound-Geräten und -Komponenten zu informieren.

10. Der Auftragnehmer verpflichtet sich, während des vereinbarten Supportzeitraums kostenlose Software- und Firmware-Updates für die zur Verfügung gestellten Inbound-Geräten und -Komponenten bereitzustellen, die sich an der erwarteten Lebensdauer der zur Verfügung gestellten Inbound-Geräte und -Komponenten orientieren und öffentlich bekannte ausnutzbare Schwachstellen beheben.

11. Der Auftragnehmer wird SMA innerhalb des vereinbarten Supportzeitraums, spätestens 45 Tage nach Bekanntwerden einer Schwachstelle, Sicherheitsupdates für die zur Verfügung gestellten Inbound-Geräten und -Komponenten liefern.

12. Der Auftragnehmer bestätigt, dass in den zur Verfügung gestellten Inbound-Geräten und -Komponenten keine Hintertüren oder Standardpasswörter vorhanden sind.

13. Der Auftragnehmer erklärt, dass es keine unbefugte ein- oder ausgehende Datenkommunikation von den zur Verfügung gestellten Inbound-Geräten und -Komponenten zu anderen Komponenten oder Systemen gibt, abgesehen vom SMA-Kommunikationsmodul (z.B. SMA-COM). Andernfalls bedarf die Datenkommunikation an externe Systeme über Nicht-SMA-Komponenten, sofern unvermeidbar, der vorherigen schriftlichen Zustimmung von SMA.

14. Der Auftragnehmer bestätigt, dass alle Debug- und Testschnittstellen in der Produktionsversion der zur Verfügung gestellten Inbound-Geräte und -Komponenten entfernt oder dauerhaft deaktiviert wurden, einschließlich, aber nicht beschränkt auf alle JTAG-Schnittstellen am Steuerprozessor.

SMA Solar Technology AG • Sonnenallee 1 • 34266 Niestetal • Germany • Tel. +49 561 9522 - 0 • E-Mail: info@SMA.de • www.SMA.de

15. Der Auftragnehmer versichert, dass für die Integration der zur Verfügung gestellten Inbound-Geräte und -Komponenten in SMA-Komponenten keine Closed-Source-Software (Software-Binaries, kompilierte Software-Stacks) erforderlich ist. Falls Closed-Source-Software aus technischen Gründen notwendig ist, muss der Auftragnehmer den dokumentierten Quellcode einschließlich der Kompilierungsdetails, Prüfsummen zur Validierung bereitstellen und sicherstellen, dass die Closed-Source-Software in einer Sandbox-Umgebung betrieben werden kann, um unbefugte Datenkommunikation zu verhindern.
16. Der Auftragnehmer garantiert, dass zur Verfügung gestellten Inbound-Geräte und -Komponenten mit den von SMA unterstützten Update-Mechanismen aktualisiert, werden können. Aktualisierungen über nicht-SMA-Mechanismen sind nicht gestattet.
17. Der Auftragnehmer gewährt SMA das Recht, Audits des Produktionsprozesses hinsichtlich Cybersicherheit durchzuführen, insbesondere in Bereichen, in denen SMA-Firmware oder -Daten verwendet werden.
18. Zum Zweck der Einhaltung und Anpassung an Änderungen, die an nationalen und internationalen Standards und Gesetzen vorgenommen werden könnten, behält sich SMA das Recht vor, seine Cybersicherheitsanforderungen jederzeit zu ändern oder zu erweitern, und solche Änderungen sind für die Parteien verbindlich.

Stand: Juni 2025

CSA_AG_GER_202506

SMA Solar Technology AG • Sonnenallee 1 • 34266 Niestetal • Germany • Tel. +49 561 9522 - 0 • E-Mail: info@SMA.de • www.SMA.de