Wichtiger Hinweis für Kunden: Sicherstellung der Einhaltung des EU-Datenschutzrechts.

Als Anbieter digitaler sozialer Alarmsysteme, die PD CLC/TS 50134-9:2018 und SS 91100:2014 (Digitales soziales Alarmsystem – „Social Care Alarm Internet Protocol" (SCAIP) – Spezifikation) implementieren, unterstützen wir unsere Kunden bei der Einhaltung der relevanten EU-Gesetzgebung, insbesondere die sogenannte Funkgeräterichtlinie „Radio Equipment Directive" (RED).

Unsere sozialen Alarmsysteme sind darauf ausgelegt, das „Social Care Alarm Internet Protocol" (SCAIP) zu nutzen und basieren auf SS 91100:2014 und PD CLC/TS 50134-9:2018. Diese Standards legen die Verwendung eines XML-Formats für Alarm- und Informationscodes fest, die über ein IP-Kommunikationsnetzwerk wie das Internet übertragen werden. Das Protokoll nutzt das „Session Initiation Protocol" (SIP) für die Sitzungsverwaltung.

Um die Einhaltung des EU-Rechts, insbesondere in Bezug auf den Schutz personenbezogener Daten und die Privatsphäre in der elektronischen Kommunikation, zu gewährleisten, ist es entscheidend, dass alle Alarmmeldungen sowie die zugehörigen Sprach- oder Multimedia-Kommunikationen über einen sicheren Kanal übertragen werden.

Obwohl unsere Produkte so konfiguriert werden können, dass sie Alarmmeldungen im „Klartext" übertragen, um bestehende Infrastrukturen von Alarmempfangszentralen (ARC) zu unterstützen, die möglicherweise derzeit noch keine „Transport Layer Security" (TLS) implementieren. Allerdings gilt diese Kommunikationsmethode im Allgemeinen nicht als sicher für sensible Informationen.

PD CLC/TS 50134-9:2018 legt ausdrücklich fest, dass die „Local Unit and Controller" (LUC) sowie die Alarmempfangszentrale (ARC) Verschlüsselung unterstützen müssen und dass die LUC keine persönlichen oder sensiblen Informationen über eine ungesicherte Verbindung ohne Verschlüsselung übertragen darf. Darüber hinaus schreibt die Spezifikation vor, dass persönliche und sensible Daten ausschließlich über sicheres SIP (SIPS) übertragen werden dürfen. Dies umfasst die Unterstützung von sicherem SIP über unsichere Verbindungen sowie für Sprachsitzungen die Verwendung des „Secure Real-time Transport Protocol" (SRTP) mit mindestens AES-128-Verschlüsselung.

Daher müssen Kunden, um die Anforderungen des EU-Rechts in Bezug auf den Datenschutz und die Sicherheit der elektronischen Kommunikation zu erfüllen, sicherstellen, dass bei der Implementierung ihres sozialen Alarmsystems eine der folgenden Maßnahmen ergriffen wird:

Verwendung von Secure SIP (SIPS) mit TLS 1.2 oder höher: Dies ist die bevorzugte Methode zur Sicherung sowohl von Alarmmeldungen als auch von Sprach-/Multimedia-Kommunikationen über IP-Netzwerke. Unsere Produkte unterstützen diese Funktionalität. Die Alarmempfangszentrale (ARC) muss ein gültiges ITU X509-Zertifikat vorlegen, und der Alarmsender (LUC) muss die Identität des Serverzertifikats mithilfe eines lokalen Root-CA-Zertifikats überprüfen.

Übertragung von Alarmmeldungen und Sprache über einen separaten sicheren Kanal (z. B. ein Virtual Private Network (VPN)): Falls eine direkte SIP-TLS-Verschlüsselung aufgrund bestehender Einschränkungen der ARC-Infrastruktur nicht möglich ist, muss ein sicherer Tunnel, wie ein VPN,

eingerichtet werden, um alle Kommunikationen zwischen dem Alarmsender (LUC) und dem Alarmempfänger (ARC) zu verschlüsseln.

Die Nichtumsetzung angemessener Sicherheitsmaßnahmen für die Übertragung von Alarmmeldungen und Sprachkommunikation kann zu Nichteinhaltung der EU-Datenschutz- und elektronischen Kommunikationsvorschriften führen. **Es liegt in der Verantwortung des Kunden, das System so zu konfigurieren und zu betreiben, dass die Einhaltung dieser Vorschriften sichergestellt wird.** Wir empfehlen dringend, sich mit Ihren juristischen und IT-Sicherheitsteams abzustimmen, um sicherzustellen, dass Ihre Implementierung alle geltenden regulatorischen Anforderungen erfüllt.