legrand® | care

Important Guidance for Customers: Ensuring Compliance with EU Data Privacy Laws and regulations.

As a provider of digital social alarm systems that implement PD CLC/TS 50134-9:2018 and SS 91100:2014 (Digital social alarm – Social care alarm internet protocol (SCAIP) – Specification), we are committed to helping our customers achieve compliance with relevant EU legislation, particularly the Radio Equipment Directive (RED) Delegated Act.

Our social alarm systems are designed to utilize the Social Care Alarm Internet Protocol (SCAIP) and are based on SS 91100:2014 and PD CLC/TS 50134-9:2018. These standards specify the use of an XML format for alarm and information codes, transported over an IP communication network such as the internet. The protocol leverages Session Initiation Protocol (SIP) for session management.

To ensure compliance with EU law, specifically regarding the protection of personal data and privacy in electronic communications, it is crucial that all alarm messages and associated voice or multimedia communications are transmitted over a secure channel.

While our products can be configured to transmit alarm messages in "clear text" to accommodate existing Alarm Receiving Centre (ARC) infrastructures that may not currently implement Transport Layer Security (TLS), this method of communication is generally not considered secure for sensitive information.

PD CLC/TS 50134-9:2018 explicitly states that the Local Unit and Controller (LUC) and the ARC shall support encryption, and the LUC shall not transmit personal or sensitive information over an unsecure connection without encryption. It further mandates that personal and sensitive data are only allowed to be transmitted over secure SIP (SIPS). This includes supporting secure SIP over unsecure connections, and for voice sessions, using Secure Real-time Transport Protocol (SRTP) with AES-128 encryption minimum.

Therefore, to align with the requirements of EU law concerning data protection and the security of electronic communications, customers must ensure one of the following for their social alarm system deployments:

Utilize Secure SIP (SIPS) with TLS 1.2 or higher: This is the preferred method for securing both alarm messages and voice/multimedia communications over IP networks. Our products support this functionality. The ARC shall present a valid ITU X509 certificate, and the LUC shall verify the identity of the server certificate using a local Root CA Certificate.
Transmit alarm messages and voice over a separate secure channel (e.g., a Virtual Private Network (VPN)): If direct SIP TLS encryption is not feasible due to existing ARC infrastructure limitations, a secure tunnel such as a VPN must be established to encrypt all communications between the alarm sender (LUC) and the alarm receiver (ARC).

Failure to implement adequate security measures for the transmission of alarm messages and voice communications may result in non-compliance with EU data protection and electronic communication regulations. **It is the customer's responsibility to configure and operate the system in a manner that ensures such compliance.** We strongly advise consulting with your legal and IT security teams to ensure your deployment meets all applicable regulatory requirements.

Legrand Care, Innovation House, Silverton Court, Cramlington, Northumberland Business Park, NE23 7RY