Intrado Life & Safety's Privacy Program and Compliance Guide

Effective April 2023

This document outlines some of Intrado Life & Safety's ("Intrado") core privacy and compliance processes. For additional information, you may contact the Intrado privacy team at privacy.lifesafety@intrado.com.

LEGAL AND REGULATORY COMPLIANCE

Intrado's privacy and data protection team ensures compliance with applicable privacy and data protection laws (including, but not limited to, the California Consumer Privacy Act, the Data Protection Act, and the General Data Protection Regulation) and manages data protection related complaints and queries.

TRAINING AND AUDITS

Intrado provides its employees with mandatory privacy and security training and awareness. Such training and awareness outlines the processes and procedures for protecting data, information, and information systems. Intrado also conducts risk and privacy impact assessments of our privacy protection position against any legislative or contractual requirements and our policies.

THIRD PARTY MANAGEMENT

Intrado does not share information with third parties unless that transfer of information is necessary for completion of required business operations and, at all times, complies with relevant law and privacy regulations. Third parties acting on behalf of Intrado are subject to written nondisclosure and/or confidentiality agreements and privacy and information security requirements.

DATA INTEGRITY

Intrado only processes personal information in a way compatible with and relevant for the purpose for which it was collected or authorized by a customer. To the extent necessary for those purposes, Intrado takes reasonable steps to ensure personal information is accurate, complete, current and reliable for its intended use. Intrado provides customers the opportunity to correct inaccuracies in the personal information it retains and delete personal information upon a customer's request, unless the burden or expense of providing access would be disproportionate to the risks to a customer's privacy or where the rights of a customer would be violated.

PRIVACY AND SECURITY RISK MANAGEMENT

Intrado conducts privacy and security risk management at various levels to evaluate the systems and functions of its various business units.

PURPOSE OF PROCESSING DATA

The processing of personal data is made for some of the following purposes to the extent it is required for the delivery of Intrado's services:

- service usage;
- support, maintenance and resolution of customer queries;
- account set-up and account management;

- invoicing and collections purposes;
- records and internal administration;
- business reporting, administration and statistical analysis;
- complying with legal obligations of the data exporter and/or the data importer; and
- cooperating with respect to actual or prospective legal proceedings, inquiries and investigations of governmental, judicial or regulatory authorities.

GENERAL DATA PROTECTION REGULATION (“GDPR”)

Under GDPR, Intrado may act as a "data processor" in relation to the personal data from customers or on behalf of customers, and each customer remains the "data controller" with respect to such personal data.

Customer personal data may be processed by Intrado, its affiliates and contractors in the United States, the United Kingdom, the European Union and the rest of the world and may be transferred outside the country in which a customer provided such personal information. We obtain valid grounds for processing personal data from customers via customer contracts, order forms and/or website terms and conditions. We also keep an internal database of executed contracts and order forms.

Intrado conducts privacy impact assessments on its services, systems, platforms, databases, processes, and vendors. We also incorporate policies such as data minimization, privacy by design and pseudonymization into our privacy processes. Additionally, we integrate data privacy into its information security policy and implements regular security risk assessments, data quality procedures, tools for data de-identification and an encryption policy.

Intrado has data breach notification procedures to ensure it notifies customers where required and in accordance with GDPR and customer contract obligations. We also have a breach response plan to ensure compliance with Article 33 of GDPR in respect of timing requirements for notification and the content of a notification letter. The breach response plan includes a log to track data breaches and we maintain data breach metrics.

Intrado has procedures to respond to requests to be forgotten or for erasure of data. We ensure deletion of personal data on the grounds of data is no longer necessary for processing, unless we are required to retain the data for a longer period of time as required by applicable law. We have processes in place to ensure records of personal data are used in line with any pertinent restrictions, and respond to requests to opt-out, restrict or object to processing. We also maintain procedures to respond to requests to update or correct customer personal data and maintains technical solutions for processing data portability requests.

Intrado only engages sub-contractors who have sufficient guarantees to implement appropriate measures to guarantee GDPR compliance and with a contract that governs the relationship. We provide information security and privacy screening questions for potential sub- contractors and other processors, as well as maintaining lists of sub-contractors that process our personal data, which are available to customers, employees and supervisory authorities upon request. Our contracts with sub-contractors also require compliance with privacy, confidentiality and information security terms.

Customers' personal information is not kept for longer than is necessary to accomplish the purpose for which it was collected. Intrado undertakes to review the length of time it retains personal information and securely delete such data when it is no longer needed for a specific purpose. Personal data related to users may include first and last time, telephone numbers, email addresses, geolocation data, call records, service, usage and connection data, account numbers, and billing related information.

Intrado implements physical, administrative and technical security measures. If Intrado learns of a security breach involving personal data, when required by law or contract, we notify the affected customer so appropriate protective steps can be taken. Intrado is not responsible for unauthorized access to such

personal data by hackers or others that obtain access through illegal measures, in the absence of negligence on the part of Intrado. Intrado's information security policy incorporates the ISO 27002 information security framework.

Intrado has a designated data protection officer (“DPO”) in order to comply with Article 37 of GDPR. Sean Ward is Intrado’s DPO. Intrado’s privacy team is response for ensuring our compliance with applicable data privacy legislation and contractual obligations. The privacy team may be contacted via email at privacy.lifesafety@intrado.com. Intrado’s EU representative office for purposes of legal matters and GDPR is in Dublin Ireland at 2 Grand Canal Square, Dublin 2, D02 A342, Ireland.

Intrado maintain logs and records of the personal data transfers. The basis for such transfers include but are not limited to: service usage; support, maintenance and resolution of customer queries; account set-up and account management; and, invoicing and collections purpose.