Intrado Privacy Program and Compliance Guide

Effective April 2021

This document outlines some of Intrado's core privacy and compliance processes.

LEGAL AND REGULATORY COMPLIANCE

At all times, Intrado ensures compliance with privacy and data protection laws in the United States and Canada (including, but not limited to, the Gramm Leach-Bliley Financial Services Modernization Act, the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act, applicable U.S. state legislation, Canada's Personal Information Protection and Electronic Documents Act, and applicable provincial legislation); the United Kingdom (including the Data Protection Act); the European Union (including the General Data Protection Regulation and EU member state legislation); the Asia- Pacific region (including, but not limited to, Japan's Act on the Protection of Personal Information, Australia's Privacy Act along with the Australian Privacy Principles and Singapore's Personal Data Protection Act); and any other applicable laws around the world.

PRIVACY TEAM

Intrado has a dedicated privacy and data protection team. The team is comprised of lawyers and privacy practitioners, many of whom are certified privacy professionals. The team is spread across the world and assists on privacy and data protection matters with global customers. The team fosters a data protection culture among employees and communicates personal data protection policies to stakeholders. Additionally, the team helps to ensure Intrado is compliant with data protection legislation and manages data protection related complaints and queries.

TRAINING AND AUDITS

Intrado provides its employees with regular mandatory privacy and security training and awareness. Such training and awareness outlines the processes and procedures for protecting data, information, and information systems. Attendance and comprehension are tracked.

Intrado conducts regular risk assessments and privacy impact assessments. The objective of a privacy impact assessment is to assess Intrado's privacy protection position against any legislative requirements, contractual requirements, or international best practices, and to review compliance with Intrado's own privacy-related policies. The scope involves evaluating procedures undertaken by Intrado throughout the typical information life-cycle phases: how information is created or received, distributed, used, maintained and disposed of or deleted.

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 with Intrado and are required to comply with Intrado's privacy policies and processes. Such contractors of Intrado are responsible for adhering to the approved information security policies and procedures. Violations of the information security policy are subject to penalizing action up to and including termination of the relationship between Intrado and the contractor. Third parties will be asked to commit to these obligations via contract.

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.

CUSTOMER PRIVACY POLICY

Intrado has extensive customer privacy statements, which are found at www.west.com/legal-privacy/

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. At the highest level, Intrado's Enterprise Compliance, Security and Audit Committee meets to set policy and address corporate-level privacy and security issues.

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")

INTRODUCTION

The GDPR applies to any business that acts as data controller or data processor and offers goods or services to individuals in the European Union ("EU"), regardless of whether it is physically located in the EU. Intrado and its affiliate companies that process personal data of individuals in the EU ("Intrado" or "we") has implemented the measures outlined in herein. Intrado has implemented GDPR compliance standards globally regarding the handling of personal data.

Under GDPR, Intrado acts 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. There are a number of obligations on data processors under GDPR. Accordingly, Intrado has a comprehensive GDPR compliance program that outlines Intrado's processes in relation to demonstrating compliance (privacy by design, privacy impact assessments on our services, data mapping, privacy audits, updating our customer contracts and training videos), retention policies (data minimisation, data accuracy, record keeping, and access rights), security (ensuring accuracy and meeting ISO27002 standards), notification policies (breach notification procedures) and subcontracting (ensuring our subcontractors meet our privacy and security minimum standards).

PROCESSING PERSONAL DATA

Intrado conducts privacy impact assessments on its services, systems, platforms, databases, processes, and vendors. We keep records of data processing activities and a personal data inventory. We also incorporate policies such as data minimisation, privacy by design and pseudonymisation into our privacy processes.

Intrado integrates data privacy into its information security policy by including storage and limitation, encryption, integrity and confidentiality, breach notifications and transparency. Intrado implements regular security risk assessments, data quality procedures, tools for data de-identification and an encryption policy. We have policies and procedures to ensure personal data is accurate and kept up to date. For inaccurate data, the data is erased, updated or otherwise rectified.

Intrado obtains valid grounds for processing personal data from customers via customer contracts, order forms and/or website terms and conditions. We keep an internal database of executed contracts and order forms. We also maintain a data inventory that sets out what ground is relied on when processing personal data.

DATA BREACH NOTIFICATION PROCEDURES

Intrado has data breach notification procedures to ensure it notifies customers where required and in accordance with GDPR and customer contract obligations. Intrado has 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 maintains a log to track data breaches. Intrado conducts data breach response testing and we maintain data breach metrics. Documentation outlining Intrado's data breach notification procedures and incident response plan is available upon request.

RIGHT TO BE FORGOTTEN, CORRECTIONS AND PORTABILITY

Intrado has procedures to respond to requests to be forgotten or for erasure of data. Intrado ensures 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. Intrado has a data retention policy available upon request. It outlines times on the erasure or pseudonymisation of customer personal data.

Intrado maintains procedures to respond to requests to update or correct customer personal data and maintains technical solutions for processing data portability requests.

Audits and Privacy Impact Assessments

Intrado has implemented appropriate technical and organisational measures to ensure and be able to demonstrate compliance with GDPR. These measures include but are not limited to privacy impact assessments and data mapping of products, solutions, databases and projects ("PIAs"), annual internal privacy audits, data inventory lists, data breach assessments and information security testing (together, "Audit Measures").

Audit Measures are taken on certain new programs, products, systems, databases and processes. Intrado engages internal stakeholders from relevant departments when conducting Audit Measures, which take into account the following:

- A description of the processing activities being assessed;
- An assessment of the risks to data subjects; and
- A description of the measures Intrado takes to address risks, including safeguards, security measures and mechanisms that Intrado will implement to ensure GDPR compliance. Data protection issues or risks are then tracked and addressed.

The objective of a PIA is to assess Intrado's privacy protection position against any legislative, contractual requirements and international best practices and to review compliance with Intrado's own privacy policies. The scope of a PIA involves evaluating procedures undertaken by Intrado throughout the typical information life-cycle phases: how data is created or received, distributed, used, maintained and disposed of or deleted.

Audit Measures guarantee data protection risks are measured, analysed and mitigated and they enable Intrado to identify issues and risks and determine, based on the likelihood and impact, where to prioritise resources to mitigate risk. Audit Measures also ensure the ability for Intrado to demonstrate appropriate technical and organisational measures have been put in place for compliance with GDPR.

Privacy by Design

Intrado integrates privacy by design into our systems and product development. Examples of privacy by design include application development protocols, security risk assessments, software for aggregation, data masking and pseudonymisation, encryption and anonymisation. Intrado implements data protection by default into our security, product and operational processes.

Intrado anonymizes personal data in which direct and indirect personal identifiers are removed and technical safeguards are implemented such that the personal data can never be re-identified so there is zero re-identification risk.

In some cases, Intrado pseudonymizes or encrypts processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided such additional information is kept separately and is subject to technical and organisational measures to ensure the personal data is not attributed to an identified or identifiable natural person.

SUB-CONTRACTING AND THIRD PARTY VENDORS

Intrado only appoints sub-contractors who have sufficient guarantees, including Standard Contractual Clauses, 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.

Intrado appoints sub-contractors under a binding written agreement, which requires sub-contractors only act on Intrado's instructions and ensure the security of Intrado's personal data it processes. At a minimum, Intrado's binding written agreement stipulates sub-contractors must:

- Only act on Intrado's documented instructions;
- Impose confidentiality obligations on all personnel who process the relevant data;
- Ensure the security of the personal data that it processes;
- Not send personal data to third party suppliers or impose the same data protection obligations on its third-party suppliers without our approval; and
- Implement measures to assist Intrado in complying with the rights of data subjects.

Intrado conducts regular due diligence audits and assessments on its sub-contractors to ensure compliance with GDPR and general data protection and security obligations. Intrado's sub-contractors are required to keep personal data they process confidential.

DATA INVENTORY

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.

Intrado has data centers in the United States, Canada, European Union and United Kingdom. Intrado customer and administrative support centers in India and the Philippines may also process customer personal data.

DATA RETENTION

Customers' personal information is not kept for longer than is necessary to accomplish the purpose for which it was collected. Intrado undertakes to do the following:

- Review the length of time it retains personal information;
- Securely delete personal information no longer needed for a specific purpose; and
- Update, archive or securely delete personal information if it becomes out of date.

CATEGORIES OF PERSONAL DATA PROCESSED BY INTRADO

Personal Data related to users, as necessary for the delivery and invoicing of Intrado's services, may include:

- First name and last name;
- Telephone and fax numbers, job title, e-mail address and similar communication data;
- Service, usage and connection data in relation to the use of the services;
- Account numbers and pass codes in relation to the delivery of the services;

- Recordings and transcriptions, as requested by a customer;
- Information provided for administration, monitoring, training, coaching and quality purposes; and
- Other data required pursuant to statutory provisions and other information voluntarily disclosed by the users through the use of the services.

SECURITY

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.

The following security measures are implemented by Intrado:

- encryption of personal data at rest and in transit;
- technical security measures such as intrusion detection, firewalls and monitoring;
- on-going tests and reviews of security measures;
- redundancy and back-up facilities;
- processes to restore availability of and access to personal data in the event of an incident;
- password parameters, data centre security measures, identity access management and restrictions on accessing personal data;
- audits and tests on information on Intrado's internal security processes and Intrado's sub-contractors information security processes;
- information security incident/breach response plan; and
- data logging to track all data privacy incidents and breaches.

Intrado has a dedicated information security team that assists the business globally.

DATA PROTECTION OFFICERS AND REGISTRATION WITH A SUPERVISORY AUTHORITY

Intrado has a designated data protection officer ("DPO") in order to comply with Article 37 of GDPR. Steven Taylor is Intrado's DPO. Additionally, Intrado has a dedicated privacy and data protection team of legal professionals ("Privacy Office") who are responsible for Intrado's compliance with applicable data privacy legislation and contractual obligations. The Privacy Office may be contacted via email at privacy@intrado.com.

For the purposes of GDPR compliance, Intrado's lead supervisory authority in the EU is the Swedish Authority for Privacy Protection in Sweden. Intrado's EU representative office for purposes of legal matters and GDPR is in Paris, France at 4 Rue Charras, Paris 75009 France.

CROSS BORDER DATA TRANSFERS

Intrado's PIAs and data mapping 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;
- 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.

Intrado and its affiliates use standard contractual clauses as a data transfer mechanism. Personal data may be transferred around the world in the countries noted above. Intrado has reviewed the Schrems II decision and, as noted above, ensures that personal data is encrypted in transit and at rest. Intrado strives to protect all personal data from unauthorized access, including by government agencies, through robust security measures such as those outlined above.

Privacy Training

Intrado provides its employees with mandatory Privacy compliance and security training and awareness. Such training and awareness outlines the processes and procedures for protecting and managing data, information, and information systems under GDPR and all applicable global privacy regulations. Attendance and comprehension are tracked.

Conclusion

Intrado proactively monitors future developments in EU and global privacy laws, including best practices. Intrado may at any time update or modify its privacy and data security processes. The information contained herein has been prepared for general information purposes only to permit you to learn more about Intrado's privacy and data protection processes. The information presented is not legal advice, is not to be acted on as such, may not be current and is subject to change without notice.

Need More Information?

You may contact privacy team members from Intrado's Legal Department at privacy@intrado.com.