

Intrado Corporation

Global Privacy Statement for Applicant Data

Introductory Statement

In order to implement and promote compliance with the various privacy and data protections obligations of Intrado Corporation and its subsidiaries (collectively, “Intrado” or the “Company”), Intrado has adopted this Global Privacy Statement (the “Statement”). The Statement is based on the privacy and data protection principles common to the countries in which Intrado operates and is applied in light of our over-arching obligations to:

- comply with applicable laws and regulations, including laws local to each jurisdiction in which Intrado operates;
- preserve and secure the Personal Data of individuals, whether current or prospective clients, employees or others; and
- respect the privacy of persons applying for employment with Intrado (“Applicants”).

Intrado’s employees and service providers must respect the privacy of Personal Data, and use reasonable and appropriate security safeguards to protect such data against loss and misuse as well as unauthorized access, disclosure, alteration or destruction.

This Statement is binding on all Intrado personnel, including personnel from Intrado subsidiaries and contractors, and shall be implemented globally throughout Intrado. Appropriate disciplinary proceedings, including possible termination, are potential consequences of a failure to comply with this Statement.

Please refer requests to access your Personal Data, concerns about inaccurate information or disputes regarding privacy and data protection issues to Amrik Mann at amann@intrado.com for EMEA, Prathibha Pillai at prathibha.pillai@intrado.com for APAC, or Bryon Langenfeld at blangenfeld@intrado.com for all remaining Intrado locations. You may also contact privacy@intrado.com for any privacy and data protection matters.

Intrado’s Data Protection Officer (“DPO”) is Steven Taylor. He can be contacted at steven.taylor@intrado.com.

This Statement may be updated from time to time. Any changes in how Intrado handles Personal Data will be communicated to applicants through updates to this Statement. The most current version of this Statement is available on Intrado sites where employment applications may be filed.

Definitions

For the purpose of this Statement, the following defined terms shall have the following meanings:

- **“Personal Data”** means any information relating to an identified or identifiable living natural person. “Personal Data” may include, for example, names, signatures, employee identification numbers, social security numbers or other national identification numbers, telephone numbers, insurance policy numbers, job titles, financial information, account numbers, or any other information that is capable of being associated with a particular identifiable individual. “Personal Data” does not include aggregate data where a person cannot be identified.
- **“Sensitive Personal Data”** means data about children, financial information, health information (including PHI as defined by HIPAA), Social Security or other national identification number, racial or ethnic origin, political opinions, religious beliefs, trade union membership, sex life, criminal convictions, and precise geolocation data.

SECTION 1. COLLECTION AND USE OF PERSONAL DATA

1.1 *Personal Data*

Intrado limits the collection, usage, disclosure and retention of Personal Data relating to Applicants to that which is relevant and proportionate to its legitimate business purposes as set out in this Statement, or for those purposes subsequently authorized by the individual, or as required or permitted by law.

Intrado collects, maintains and uses Personal Data, including when necessary Sensitive Personal Data, about Applicants for administrative purposes, to conduct the business of Intrado and to comply with legal and regulatory obligations. Such Personal Data may include, but is not limited to, any references obtained during recruitment, details of terms of employment, payroll details, tax and national insurance information, details of job duties, details of health and sickness absence records, details of education and certification records, information about performance, details of any disciplinary investigations and proceedings, training records, contact names and addresses, and other information voluntarily given to Intrado or publicly available. Intrado may process Personal Data about Applicants for purposes connected with employment, including recruitment and termination, as well to monitor the performance of the duties and obligations, ensure appropriate internal controls on financial and accounting systems, and conduct investigations and other activities in connection with legal proceedings or in anticipation of potential proceedings.

Intrado does not transfer Personal Data about Applicants to unaffiliated third parties except as otherwise provided in this Statement. Intrado may, from time to time, disclose Personal Data about Applicants to relevant third parties for its reasonable business and legal purposes. For example, Intrado may be legally obligated by a government agency to disclose Personal Data. Recipients of such data may include affiliated corporate entities, including successor entities, agents, contractors involved with any payments or benefits, future employers who request a reference, proposed assignee or transferee of the business, as well as governmental, judicial or regulatory authorities in order to comply with legal or regulatory obligations or as authorized by the Applicant. Intrado does not sell, rent or lease Personal Data about Applicants.

1.2 Sensitive Personal Data

Sensitive Personal Data are not disclosed to unaffiliated third parties or used for purposes other than those for which the data were initially collected without consent of the data subject or the presence of other circumstances requiring or justifying such use under applicable law. Sensitive Personal Data may be processed to meet Intrado's legal responsibilities, for purposes of personnel management and administration, suitability for employment and to comply with equal opportunity legislation.

Data subjects are given this notice of the processing performed on their Sensitive Personal Data and, where feasible and appropriate, opportunities to express their choices regarding Sensitive Personal Data. In particular, a choice is regularly offered where Intrado seeks to use Sensitive Personal Data for a purpose that is incompatible with the original purposes for which the data were collected or subsequently authorized, or transferred to a third party that is not acting as an agent of Intrado. Intrado does not process Sensitive Personal Data in any manner not allowed by applicable law.

SECTION 2. DATA INTEGRITY & RETENTION

Intrado endeavors to keep all Personal Data in its possession reasonably current and accurate. Applicants are expected to keep Intrado informed of any changes to their Personal Data such as a change in address or any other information affecting services provided by Intrado. Intrado strives to maintain Personal Data, including Sensitive Personal Data, for periods no more extensive than what is necessary for the purposes for which it was collected or for which it may be appropriately used, but it retains data when required to do so by law.

SECTION 3. ACCESS TO PERSONAL DATA

3.1 Applicant access

Subject to applicable law and regulation, an Applicant may inspect Personal Data in his or her personnel file, and if necessary request corrections to such data. Requests for such access must be made in writing to Human Resources or as outlined above in the Introductory Statement. Human Resources shall keep a written record of such requests and will provide a response to such a request as soon as reasonably possible within the time frame required by law. Such response may include a determination Human Resources needs additional time to provide a response to the request. Upon receipt and verification of corrected Personal Data, Human Resources will ensure appropriate correction is made.

Access to Personal Data is not guaranteed, however, reasonable requests for access will be granted subject to Intrado's rights and responsibilities and in accordance with applicable law and regulation.

3.2 No automated decision making without appropriate safeguards

Intrado Applicants are not subject to decisions concerning them which are based solely on automated processing of Personal Data unless appropriate human mechanisms are in place to safeguard against inaccurate or improper decisions.

SECTION 4. DATA SHARING

4.1 Service Providers

Personal Data regarding Applicants may be shared with service providers who process data on behalf of Intrado in order to supply Intrado and its Applicants with the services necessary to manage the business. Intrado requires all service providers, vendors and other processors of Personal Data to process such Personal Data under the direction of Intrado and provide adequate protections for the Personal Data entrusted to them by Intrado, at least at the same level of privacy protection as required by these privacy principles. Intrado will only transfer Personal Data to a non-agent third party where such transfer is consistent with the notice provided to the data subjects at the time the Personal Data were collected.

Intrado may use or disclose Applicants' Personal Data if required to do so by law or in the good faith belief such action is necessary to adhere to any applicable law or comply with legal process served on or applicable to Intrado, protect and defend the rights or property of Intrado, or act to protect the personal safety of Intrado employees or members of the public or otherwise aid law enforcement or protect national security. Intrado may also disclose Personal Data or other data relating to Applicants to anyone the data subject authorizes.

Intrado may disclose Personal Data to third parties where necessary to comply with any legal obligation of Intrado, in connection with actual or prospective legal proceedings against Intrado and otherwise in connection with the establishment, investigation, exercise or defense of legal claims.

In the event of a sale, assignment, bankruptcy, liquidation or other transfer of all or substantially all of the stock, assets or business of Intrado, Personal Data may be transferred to a relevant successor entity, subject to the applicable privacy statement. Any corporate successors to Intrado may be provided with Applicant files during a corporate transaction including during any due diligence process for prospective transactions, provided the receiving party agrees to privacy and security conditions equivalent to those provided in this Statement.

4.2 Intra-Intrado transfers

As a global corporation operating in several countries, Intrado transfers Personal Data between offices of Intrado across national borders for the purposes of international administration and operations or for any of the other purposes referred to in this Statement. Such intra-Intrado transfers of Personal Data may result in the transfer of data between countries that have differing legal regimes for privacy protection and provide different levels of privacy protection. In particular, data are routinely transferred between countries in the European Union and other countries around the world, some of which the European Union currently does not deem to have “adequate” privacy safeguards. One purpose of this Statement is to address this concern by ensuring the data transferred will be consistently treated with best practices and a high-level standard of protection regardless of the office location.

Personal Data are processed and transferred between the Company’s offices pursuant to the data protection requirements of this Statement. Such transfers will take place on the basis of: (i) the consent of the data subject, (ii) the EU's standard contractual clauses for data transfers; (iii) being necessary for the performance of a contract between the data subject and the Company or the implementation of such pre-contractual measures taken in response to the data subjects request; (iv) being necessary for the conclusion or performance of a contract in the interest of the data subject between the Company and third parties; or (v) being necessary or legally required on important public interest grounds or for the establishment, exercise or defense of legal claims.

SECTION 5. MONITORING

Intrado may monitor Applicants consistent with applicable law for certain purposes including compliance with regulatory practices, quality control, to prevent or detect crime, to investigate unauthorized use, or to determine whether communications are business or personal communications. For instance, Intrado may use security monitoring devices, such as remote cameras in lobbies of offices and key-cards to enter offices, when allowed by law.

Intrado may also conduct background checks or other investigations of personnel in accordance with applicable law when Intrado deems such information necessary to protect the Company or its customers.

SECTION 6. INFORMATION SECURITY

Information security is an important component of Intrado's data protection obligations. Intrado takes appropriate precautions to restrict access to Personal Data to only those Intrado personnel with a need to know. Intrado implements and maintains reasonable and appropriate measures to protect the Personal Data in its possession from loss, misuse, unauthorized access or inadvertent destruction. Intrado also maintains physical, electronic and procedural safeguards in order to protect the data under its control.

Intrado personnel are responsible for maintaining information security with respect to Personal Data and must take all appropriate precautions to protect against unauthorized access to Intrado's computer networks and information systems, including protection of user-IDs and passwords. All employees and each department must ensure all devices containing Personal Data are properly disposed of when taken out of service.

Intrado evaluates and implements new information security technologies and practices on an ongoing basis and will, from time to time, communicate new or additional requirements to Intrado employees.

EFFECTIVE DATE

This Statement is effective as of November 26, 2019 for all of Intrado Corporation.