InfoGrid Systems Inc.

- Corporate Privacy Policy -

Version: 3.0
January 1, 2019

Table of Contents

Purpose

InfoGrid Systems Inc. ("IGS") is committed to managing data in compliance with all applicable privacy and data protection laws.

The purpose of this document is to outline the core privacy principles that govern IGS's standard practices with respect to the collection, use, disclosure and storage of personal information.

Scope of Policy

This policy establishes minimum standards for protecting personal information in the control or custody of IGS, its staff, contractors, agents and service providers. This policy applies regardless of the geographic location of the businesses using IGS's products and services.

Personal information is any information about an identifiable individual. Although there may be some information in IGS's databases that is business rather than personal in nature (for example, business contact information), IGS extends the same or a similar level of protection to this business information as it does to personal information, whenever appropriate.

Core Principles

IGS's data cleanup and data mining tools can be accessed by clients from virtually any country in the world.

Where such countries have established privacy laws in place, the specific responsibilities imposed on organizations doing business in different jurisdictions may vary significantly. As a result, to meet the inherent challenges of this global context, IGS has elected to adopt an internationally recognized general framework for the handling of personal information: the eight privacy principles codified in 1980 by the Organization for Economic Co-operation and Development ("OECD"), "Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data". These eight principles are summarized below, along with IGS's implementation of these principles.

Principle 1: Collection Limitation

The personal information collected is limited to those details necessary for the purposes identified by IGS. Personal information is collected by fair and lawful

means, with the knowledge or consent of the client if required by local law or regulation.
Personal information is collected indirectly by IGS from the public domain or from various sources that are required to obtain and disclose the information in accordance with applicable data protection laws. The information collected includes names, addresses and phone numbers of individuals in North America, as well as the contact information of their neighbors or employers if available.

IGS reminds its customers to consider privacy and information security when using information obtained from IGS's databases.

Principle 2: Data Quality

Personal information is maintained by IGS in as accurate, complete and up-to-date form as is necessary to fulfill the purposes for which it is to be used.

IGS has invested substantial time and resources to develop proprietary methods that allow the company to maintain accurate data. Updates or corrections to information in IGS's databases, are made using publicly available information or consent-based lists.

Principle 3: Purpose Specification

The purposes for which personal information is collected are identified by IGS before or at the time the personal information is collected, except where the collection is required or permitted by law.

Any personal information collected by IGS is for the purpose of providing debt collectors, credit grantors or debt acquirers holding delinquent accounts with contact information that is as current as possible, based on IGS's proprietary methodology. IGS only uses information entered into its databases to provide this service to its customers, and will not re-use personal information for alternate purposes at a later time without the express and informed consent of the individuals to whom the information relates.

Principle 4: Use Limitation

Personal information is not disclosed, made available or otherwise used by IGS for purposes other than those identified, except with the consent of the data subject; or by the authority of law.

Sharing of personal information only occurs with licensees of IGS's products and services (IGS's customers) who require the information in order to locate individuals.

Agents, service providers or contractors may, in the course of their work, require access to IGS systems. In such a case, detailed third party information protection agreements must be signed before such access is granted.

In accordance with local laws, IGS will provide appropriate levels of system and data access to law enforcement and other government agencies for the legitimate execution of lawful investigations.

Principle 5: Security Safeguards

Personal information is protected by appropriate security safeguards to reduce the risk of loss or unauthorized access, destruction, use, modification or disclosure of personal information.

As part of its standard business practice, IGS protects *all* information (including personal information) in its care through a complementary combination of physical, technical and administrative safeguards including, but not limited to, the following:

- Use of enterprise-class, high-end security hardware and software solutions that automatically restrict and monitor traffic traveling across the boundary between the Internet and IGS's corporate systems;
- Annual vulnerability and penetration testing on IGS systems;
- The servers that host IGS's data and software are configured and maintained in accordance with information security best practices:
    - The firewall installed is regularly tested and updated with security patches;
    - Anti-virus and intrusion detection software is installed and kept current on all IGS servers;
    - The following security measures are implemented for registered user access to IGS's software products:
        - A strong password scheme;
        - Encrypted password store; and
        - A secure, fully encrypted tunnel for data transmissions.
- Records containing personal information are disposed of in a secure manner, appropriate to the format of the record (i.e. shredding of paper records, erasure of electronic records).

Principle 6: Openness

IGS has a general rule of openness about its policies and practices that relate to the handling of personal information.

This policy is available to the public for review. Any related policies and procedures involving the safeguarding of personal information are available upon request, by contacting IGS's Privacy Officer.

Principle 7:Individual Participation

Upon request, individuals are informed of the existence, use and disclosure of their personal information, and given access to it. Individuals may verify and challenge the accuracy and completeness of their personal information, and have it amended, if appropriate.

Individuals interested in checking for the existence of personal information relating to themselves, that may be in IGS's custody or control, should submit a written request to IGS's Privacy Officer. The Privacy Officer can then make the necessary arrangements for an appropriate search to be undertaken, and for the results to be provided to the requestor in a suitable format.

Requests for corrections to, updates or deletions of information should be directed to IGS's Privacy Officer.

Principle 8: Accountability

IGS is responsible for maintaining and protecting personal information under its control. In fulfilling this mandate, an individual has been designated who is accountable for compliance with this Privacy Policy.

IGS's Privacy Officer is charged with ensuring that the organization conducts itself in accordance with the above principles. Further, the Privacy Officer will ensure that all staff are made aware of their obligations with respect to this policy.

IGS's IT Manager is responsible for all aspects of IT security and the protection of data within the company's custody and control, including the following specific duties:

- Establish and maintain security and risk management programs at IGS;
- Maintain policies and procedures that provide for security and risk management of information resources; and
- Direct initiatives such as security testing and security audits.

Additionally, all new IGS staff receive security training, and are empowered to make suggestions regarding ways in which security practices and measures can be improved.

Exceptions to this Policy

In situations where a specific country's legal requirements may conflict with the principles and practices outlined above, IGS's Privacy Officer will address such issues on a case-by-case basis, in co-operation with the appropriate authorities, to arrive at a law-abiding and optimal resolution for all concerned parties.

Contact Information

Questions about this policy, or privacy procedures and practices should be directed to IGS's Privacy Officer by e-mail at privacy@infogridsystems.com.

Review of this Policy

This policy will be reviewed for accuracy and consistency with IGS's practices on an annual basis, or more frequently, at the discretion of senior management and/or IGS's Privacy Officer.