Corporate Data Privacy Policy

Gonvarri Industries

POLT-CORP-05

Content:

1. Objetive

The main objectives of the Data Privacy Policy are:

- To ensure that all of the personal information in GI custody is adequately protected against threats to maintain its security.
- To ensure that GI employees are fully aware of the contractual, statutory or regulatory implications of any privacy breaches.
- To limit the use of personal information to identified business purposes for which it is collected.
- To create an awareness of privacy requirements to be an integral part of the day to day operation of every employee and ensure that all employees understand the importance of privacy practices and their responsibilities for maintaining privacy.
- To make all the employees aware about, the processes that need to be followed for collection, lawful usage, disclosure/ transfer, retention, archival and disposal of personal information.
- To ensure that all third parties collecting, storing and processing personal information on behalf of GI provide adequate data protection.
- To ensure that applicable regulations and contracts regarding the maintenance of privacy, protection and cross border transfer of personal information are adhered to.

This Policy defines requirements to help ensure compliance with laws and regulations applicable to GI's' collection, storage, use, transmission, disclosure to third parties and retention of Personal and sensitive personal data (also referred to as personal and sensitive personal information respectively in this policy).

2. Scope

This Policy applies to all the companies that make up the Gonvarri Industries Group, in which the parent company, Gonvarri Corporación Financiera, S.L.U., and all the personnel of the Gonvarri Industries Group hold a majority interest, directly or indirectly, in the exercise of their functions and responsibilities, and in all the professional areas in which they represent the Group, meaning the directors, executives, employees and collaborators of the GI Group, regardless of their position, responsibility or geographical location

In any case, the Group's actions comply with the legislation in force in each jurisdiction, and therefore, in some of these jurisdictions, the principles set forth in this policy may be replaced by more restrictive laws and regulations in force.

3. Terms and Definitions

Anonymize: To process a collection of personal data or information such that a natural person cannot be identified on the basis of the output collection of data or information.

Data subject: A living individual about whom personal information is processed by or on behalf of GI.

GI: GI Limited / its Subsidiaries / its Group Companies / its affiliates, its directors, employees (excluding the User/affirming employee in this context), assigns and successors.

Information security: Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Personal Data or personal information: Any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

Third party: All external parties – including without limitation contractors, interns, summer trainees, vendors, service providers and partners – who have access to GI information assets, information systems or who are pass personal information from them.

4. Introduction

GI endeavours to meet leading standards for data protection and privacy. While our reasons are founded in ethical and corporate responsibility, our privacy practices as outlined in this policy facilitate the following:

- Competitive Advantage: Our emphasis on protecting the privacy of customers, vendors, and employees distinguishes us from our competitors.
- Good Corporate Citizenship: A sound privacy policy is emblematic of reliable corporate citizens that respect data subjects' privacy.
- Business Enablement: Since GI uses significant volumes of personal information, privacy notices become a prerequisite to building enduring business relationships.
- Legal Protection: Appropriate privacy notices offer an opportunity to eliminate allegations of unlawful usage of personal information.

GI Privacy Policy aligns with Generally Accepted Privacy Principles. In view of the changing legislative and technological environment for data privacy, the Privacy Policy will undergo revisions. The guiding privacy principles articulated in this policy document are as follows:

- Management:

  Define, document, communicate, and assign accountability for GI Privacy policy and procedures

- Notice:

  Provide notice about GI Privacy policy and procedures and identify the purposes for which personal information is collected, used, retained, and disclosed

- Choice and Consent:

  Describe the choices available to the individual and obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information

- Collection of personal information:

  Collect personal information only for the purposes identified in the notice

- Limiting Use, Disclosure and Retention:

  Limit the use, storage and retention of personal information is limited to the purposes identified in the data privacy notice and for which the individual has provided implicit or explicit consent. Retain personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately dispose of such information.

- Access for review and update:

  Provide data subjects with access to their personal information for review and update

- Disclosure to third parties:

  Disclose personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual

- Security practices for privacy:

  Protect personal information against unauthorized access (both physical and logical)

- Quality of personal information:

  Maintain accurate, complete, and relevant personal information for the purposes identified in the notice

- Monitoring and enforcement:
  Monitor compliance with GI Privacy policy and procedures, and have procedures to address privacy related complaints and disputes

5. Main Aspects of the Privacy Policy

5.1 Management

- A Data Privacy Policy shall be developed and maintained to document the privacy principles and practices followed by GI. (Refer: Introduction of this document)
- A privacy organization shall be defined for governance of data privacy initiatives. (Refer: Document of GDPR Management Model)
- A Responsible of Privacy shall be appointed to process complaints and requests for information related to GI privacy practices.
- Establish procedures for the identification and classification of personal information.
- GI Privacy Policy statement shall be made available on GI's internal portal.
- The Data Privacy Policy shall be communicated to GI internal personnel.
- Procedures shall be established for disciplinary and remedial action for violations of the Data Privacy Policy.
- Changes or updates to the Data Privacy Policy shall be communicated to GI internal personnel when the changes become effective.
- Establish procedures for performing mandatory registration with regulatory bodies.
- Risk Assessment is to be carried out on a periodic basis to ensure risks to personal information are identified and mitigated.
- The potential impact on data privacy is assessed when new processes involving personal information are implemented, or when significant changes are made to such processes. (Refer: Document of PIA guidelines)

5.2 Notice

- Appropriate notice shall be provided to data subjects at the time personal information is collected. (Refer: Document of Clauses consent and information model and contract with responsible of treatment)
- The privacy notice or policies and other statements to which they are linked shall provide as full information as is reasonable in the circumstances to inform an individual how their personal

information will be used so that GI's use is fair and lawful. The following information should be considered for inclusion in a notice (as is appropriate in individual circumstances):

- Purposes for which personal information is collected, used and disclosed;
- Choices available to the individual regarding collection, use and disclosure of personal information, wherever applicable;
- Period for which personal information shall be retained as per identified business purpose or as mandated by regulations, whichever is later;
- That personal information shall only be collected for the identified purposes;
- Methods employed for collection of personal information, including 'cookies' and other tracking techniques, and third party agencies;
- That an individual's personal information shall be disclosed to Third Parties only for identified lawful business purposes and with the consent of the individual, wherever possible;
- That an individual's personal information may be transferred within GI entities, globally as per requirement, for business purposes with adequate security measures required by law or as per guidance of provided by industry leading practices;
- Consequences of withholding or withdrawing consent to the collection, use and disclosure of personal information for identified purposes;
- Data subjects are responsible for providing GI with accurate and complete personal information, and for contacting the entity if correction of such information is required;
- Process for an individual to view and update their personal information records;
- Process for an individual to register a complaint or grievance with regard to privacy practices at GI;
- Contact information of person in charge of privacy practises and responsible for privacy concerns with address at GI;
- Process for an individual to withdraw consent for the collection, use and disclosure of their personal information for identified purposes; and
- That implicit or explicit consent is required to collect, use and disclose personal information, unless a law or regulation specifically requires or allows otherwise.

- Data subjects shall be provided a Privacy Notice in case any new purpose is identified for using or disclosing personal information before such information is used for purposes not previously identified.

5.3 Choice and Consent

- Implicit or explicit consent shall be obtained from data subjects at the time of collection of personal information or as soon as practical thereafter.

- Explicit consent shall be obtained from data subjects for the collection, use and disclosure of sensitive personal information, unless a law or regulation specifically requires or allows otherwise. A record is maintained of explicit consent obtained from data subjects.

- Implicit consent shall be considered adequate for the collection, use and disclosure of personal information which does not qualify as sensitive personal information.

- Consent shall be obtained from data subjects before their personal information is used for purposes not previously identified.

- Appropriate consent shall be obtained from data subjects before their personal information is transferred to or from their information processing systems.

5.4 Collection of Personal Information

- The collection of personal information shall be limited to the minimum requirement for lawful business purposes.

- Methods of collecting personal information shall be reviewed by management to ensure that personal information is obtained:
    - Fairly, without intimidation or deception, and
    - Lawfully, adhering to laws and regulations relating to the collection of personal information.

- Management shall confirm that Third Parties from whom personal information is collected:
    - Use fair and lawful information collection methods, and
    - Comply with the GI Privacy Policy and their contractual obligations with respect to the collection, use and transfer of personal information on behalf of GI
    - Data subjects shall be notified if additional information is developed or acquired about them.

5.5 Limiting Use, Disclosure and Retention

- Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

- Personal information retention shall be only for the duration necessary to fulfil the identified lawful business purposes or as prescribed by law.

- Guidelines and procedures shall be developed for the retention and disposal of personal information. These shall address minimum and maximum retention periods, and modes of storage.

- Upon the expiration of identified lawful business purposes or withdrawal of consent, GI shall either securely erase or anonymize the data subjects' personal information. Data is anonymized to prevent unique identification of an individual.

5.6 Access for Review and Update

- Processes shall be established for data subjects to:
    - Request access to their personal data or information as prescribed by law;
    - Correct or update their personal data or information; and

- Withdraw consent for the collection, use and disclosure of their personal information.

- The identity of data subjects requesting access their personal information, or the identity of the data subjects authorized by the data subject to access the data subject's information, shall be reasonably verified before providing access to such information.

- A response shall be given data subjects requesting access to their personal information in an accessible form, within a defined period from receipt of complaint/ request as prescribed by law.

- Data subjects shall be notified, in writing, the reason for any denial of requests for access to personal information to the extent required by applicable law.

5.7 Disclosure to Third Parties and Outward Transfers

- Personal information shall be disclosed to third parties only for identified lawful business purposes and after obtaining appropriate consent from the data subjects, unless a law or regulation allows or requires otherwise.

- Where reasonably possible, management shall ensure that third parties collecting, storing or processing personal information on behalf of GI have:
  - Signed agreements to protect personal information consistent with GI Privacy Policy and information security practices or implemented measures as prescribed by law;
  - Signed non-disclosure agreements or confidentiality agreements which includes privacy clauses in the contract; and
  - Established procedures to meet the terms of their agreement with GI to protect personal information.

- Personal information may be transferred across geographies from where GI operates for storage or processing where any of the following apply:
  - The individual has given consent to the transfer of information.
  - The transfer is necessary for the performance of a contract between the individual and GI, or the implementation of pre-contractual measures taken in response to the individual's request.
  - The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between GI and a third party.
  - The transfer is necessary or legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
  - The transfer is required by law.
  - The transfer is necessary in order to protect the vital interests of the individual.
  - The transfer is made under a data transfer agreement.
  - The transfer is otherwise legitimised by applicable law.

- Remedial action shall be taken in response to misuse or unauthorized disclosure of personal information by a third party collecting, storing or processing personal information on behalf of GI

5.8 Security Practices for Privacy

- GI information security policy and procedures shall be documented and implemented to ensure reasonable security for personal information collected, stored, used, transferred and disposed by GI.

- Information asset labelling and handling guidelines shall include controls specific to the storage, retention and transfer of personal information.

- Management shall establish procedures that maintain the logical and physical security of personal information.

- Management shall establish procedures that ensure protection of personal information against accidental disclosure due to natural disasters and environmental hazards.

- Incident response protocols are established and maintained in order to deal with incidents concerning personal data or privacy practices. (Refer: Procedure of security incidents management)

5.9 Quality of Personal Information

- GI may perform additional validation procedures to ensure that personal information collected is accurate and complete for the business purposes for which it is to be used.
- GI shall ensure that personal information collected is relevant to the business purposes for which it is to be used.

5.10 Privacy Monitoring and Enforcement

- Procedures shall be established for recording and responding to complaints/ grievances registered by data subjects.

- Each complaint regarding privacy practices registered by data subjects shall be validated, responses documented and communicated to the individual.

- Annual privacy compliance review shall be performed for identified business processes and their supporting applications.

- A record shall be maintained of non-compliances identified in the annual privacy reviews. Corrective and disciplinary measures shall be initiated and tracked to closure, guided by GI management.

- Procedures shall be established to monitor the effectiveness of controls for personal information and for ensuring corrective actions, as required.

- Any conflicts or disagreements relating to the requirements under this policy or associated privacy practices shall be referred to the Privacy Officer for resolution.

5.11 Personally Identifiable Information (PII) of GI employee

- Data protection laws govern the use of personally identifiable information. This term means any data relating to a living individual who can be identified using that data. GI may hold the following types of sensitive and non-sensitive PII:
    - names, addresses, telephone numbers and other personal contact details;
    - gender, date of birth, physical or mental health or condition;
    - marital status, next of kin, racial or ethnic origin, sexual orientation, religious, philosophical, political or similar beliefs;
    - national insurance or social insurance number, immigration status, trade union membership;
    - personnel records including training, appraisal, performance and disciplinary information, and succession planning;
    - bank details, salary, bonus, benefits and pension details and other financial information; and
    - Criminal offences committed (or allegedly committed) including any proceedings and sentencing in relation to any such criminal offence.

5.12 Staff data processing activities

- Personal information about individuals may only be processed for a legitimate purpose. GI may undertake a number of activities with an individual employee's personal information including, but not limited to:
    - salary, benefits and pensions administration;
    - health and safety records and management;
    - security vetting, criminal records checks and credit checks and clearances (where applicable and allowed by law);
    - confirming information on résumés, CVs and covering letters, providing reference letters and performing reference checks;
    - training and appraisal, including performance evaluation and disciplinary records;
    - staff management and promotions;
    - succession planning;
    - equal opportunities monitoring;
    - any potential change of control of a group company, or any potential transfer of employment relating to a business transfer or change of service provider;
    - other disclosures required in the context of staff employment;
    - promoting or marketing of GI, its products or services;
    - provision of staff or business contact information to customers and agencies in the course of the provision of GI's services;
    - CCTV monitoring for security reasons;
    - compliance with applicable procedures, laws, regulations, including any related investigations to ensure compliance or of any potential breaches;
    - establishing, exercising or defending GI's legal rights;
    - disclosures to other companies in the GI group of companies, including companies in other countries to the extent permitted by law, including for the following purposes: as required in connection with the duties of the employee; legal compliance; audit; group level management; in connection with the fulfilment of customer and partner contracts;

- any other reasonable purposes in connection with an individual's employment or engagement by GI;
- Providing and managing use of services provided by third parties, such as company provided mobile phones, company credit cards and company cars and billing for such services.

- GI may also collect and process personal information about your next of kin so they can be contacted in an emergency or in connection with use of a company car provided by GI. Their personal information will also be processed in accordance with the data protection laws and as described in the policy.

- In order to fulfil the purposes set out above, GI may disclose personal information to contractors and suppliers that provide services to GI and who may assist in the processing activities set out above and also to law enforcement agencies, regulatory bodies, government agencies and other third parties as required by law or for administration/taxation purposes, to the extent local law allows and requires.
- GI may disclose your personal information to third parties for the purposes of establishing and managing your employment relationship. For example, GI may disclose some of your personal information to:
  - benefits providers (for example, pension and insurance providers);
  - payroll and data processing suppliers and other service providers who assist us in establishing or managing your employment relationship with us;
  - insurance claims and medical related service providers; and
  - Parties requesting an employment reference.

- GI shall take appropriate measures to ensure that its contractors and suppliers also process personal information in a compliant way and such measures may include a data processing agreement.

- GI may transfer personal information to other group companies, partners, suppliers, law enforcement agencies and to other organisations in all cases that are located outside of the country where you are based for the purposes of:
  - HR administration (for example, staff recruitment);
  - payroll processing for employees working outside the country where they are based;
  - employee relocation;
  - security clearances;
  - visa applications;
  - taxation and registrations for employees working outside the country where they are based;
  - fulfilling GI's legal requirements;
  - fulfilling customer contracts for the provision of GI's services;
  - overseas legal proceedings;
  - Outsourcing GI functions.

- The laws of some jurisdictions may not be as protective as the laws in the country in which you are based. GI may transfer your personal information across provincial or national borders to fulfil any of the above purposes, including to service providers located in countries who may be

subject to applicable disclosure laws in those jurisdictions, which may result in that information becoming accessible to law enforcement and national security authorities of those jurisdictions.

5.13 Retention of records

- GI has a statutory duty to keep certain records for a minimum period of time. In other cases GI shall not keep personal information for longer than is necessary or as may be required by applicable law.

5.14 Monitoring

- Monitoring of GI's systems

- GI's IT and communications systems are intended to promote effective communication and working practices within our organisation.

- For business reasons, and in order to carry out legal obligations in our role as an employer, use of GI's systems on whatever platform including the telephone (mobile and fixed) and computer systems (including email and internet access), and any personal use of them, is monitored. If you access services by the use of passwords and login names on GI's IT and communication systems this might mean that your personal access details are seen by GI.

- Monitoring is only carried out if and to the extent permitted or as required by law and as necessary and justifiable for business purposes. The resulting log files may be used so that instances of attempted misuse and other security events can be detected and that information is available to support any subsequent investigation. To the extent permitted by law and, where breaches of this and other GI policies or applicable law are found, action may be taken under the disciplinary procedure.

- The employees are informed that the telephone system used by the Company allows identification of all dialled numbers and received calls.

- GI reserves the right to retrieve the contents of messages, check searches which have been made on the internet, require the immediate return of devices supplied by GI and access data stored on such devices for the following purposes (this list is not exhaustive):
    - to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy (and employees acknowledge that the Company can use software to monitor the identity of senders and receivers of emails);
    - to find lost messages or to retrieve messages lost due to computer failure;
    - to assist in the investigation of wrongful acts; or
    - to comply with any legal obligation.

- If evidence of misuse of GI's IT systems is found, GI may undertake a more detailed investigation in accordance with GI's disciplinary procedures, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the disciplinary procedure. If necessary such information may be handed

to the police in connection with a criminal investigation. Investigations and disclosure of information to the relevant authorities shall be carried out only to the extent permitted by law.

5.15 CCTV

- Some of GI's buildings and sites use CCTV systems to monitor their exterior and interior 24 hours a day for security reasons. This data is recorded. Use of CCTV and recording of CCTV data is only carried in accordance with GI approved guidelines.

- GI shall take reasonable efforts to alert the individual that the area is under electronic surveillance.

6. Language

This Standard is published in Spanish and English, the former being prevalent in case of divergence between the two.

7. Control of versions

Version	Date	Description	Prepared by	Review by
Version 1	19th July 2018	Initial Version of the Document	Privacy Officer	Compliance Committee

8. Approval and entry into force

This Standard has been approved by the Compliance Committee of Gonvarri Industries Group on July the 19th of 2018, and takes effect 20 calendar days after its approval. As of the entry into force, the previous provisions existing in their case that regulate the same content are repealed.

SIGNED BY COMPLIANCE COMMITTEE


Gonvarri
Industries