


|   |   |
|---|---|
|  <p><b>Graphic Packaging</b><br/>INTERNATIONAL</p> | <p><b>Reference:</b><br/>CI- XX</p>   |
| <p><b>Global Privacy Policy</b><br/><b>CORPORATE INSTRUCTION</b></p>  | <p><b>Date Last Issued:</b><br/>March 01, 2024</p> <p><b>Reissued Date:</b><br/>XX – XX - XXXX</p> <p><b>Effective Date:</b><br/>March 01, 2024</p> |

## Table of Contents

|   |   |
|---|---|
| Table of Contents .....   | 1 |
| Policy Statement .....  | 3 |
| Scope .....   | 3 |
| Key Terminology .....   | 3 |
| Personal Data Processing .....  | 4 |
| Data Minimization, Privacy by Design, and Sensitivity Reduction ..... | 4 |
| Maintaining Records of Processing .....                               | 4 |
| Data Protection Impact Assessments (DPIAs) and Risk .....             | 5 |
| Legal Bases of Processing Personal Data .....                         | 5 |
| Data Security .....   | 6 |
| Confidentiality and Authorization .....                               | 6 |
| Encryption and Pseudonymization .....                                 | 6 |
| Regular Security Audits and Testing .....                             | 6 |
| Monitoring .....  | 6 |
| Social Media .....  | 6 |

Mobile Device Management (MDM) ..... 7

Data Retention ..... 7

Data Subject Rights ..... 7

Special Categories and Sensitive Personal Data ..... 7

Data Sharing and Third Parties ..... 8

Data Breach Notification ..... 8

International Data Transfer ..... 8

Compliance with Laws and Regulations ..... 8

Training, Awareness and Enforcement ..... 9

Data Protection Officer (DPO) ..... 9

Roles and Responsibilities ..... **Error! Bookmark not defined.**

Version Control ..... 9

## Policy Statement

Graphic Packaging is committed to safeguarding employee and customer Personal Data. To ensure transparency and compliance with global privacy laws, this privacy policy outlines:

- The types of Personal Data Graphic Packaging collects;
- Why Graphic Packaging collects this Personal Data;
- How the Personal Data is used and processed;
- Rights and choices regarding Personal Data;
- Protection of Personal Data; and
- Privacy-related authority contacts.

## Scope

This Policy applies to all Graphic Packaging personnel, locations and other assets globally, including but not limited to:

- All Graphic Packaging business units, departments and functions;
- All Graphic Packaging contractors, consultants and other third-party service providers, except where employee-specific requirements are indicated;
- All Graphic Packaging leased or owned facilities where Graphic Packaging business is operating; and
- All Graphic Packaging technology and network infrastructure, including its information systems, applications, system platforms, and computer operations employed in the normal operation of Graphic Packaging.

Certain policies referenced or linked herein are internal and exclusively accessible to designated employees. If you are an employee and cannot access a linked policy, please contact [law.department@graphicpkg.com](mailto:law.department@graphicpkg.com) to obtain a copy.

## Key Terminology

**“Data Subject”** is a natural living person whose Personal Data has been or is being processed.

**“Personal data”** includes all information relating to an identified or identifiable natural person, for example, an employee’s name and employment record, a customer representative’s name and business contact details, a vendor representative’s name and business contact details, and data relating to our website visitors’ viewing preferences on our website.

**“Processing”** is a very broad term and essentially means anything that is done to, or with, Personal Data (including simply collecting, storing, accessing, or deleting Personal Data).

## Personal Data Processing

Graphic Packaging is committed to conducting transparent Personal Data processing practices. Individuals will be informed about what Personal Data is collected, why it is collected, and how it will be used through clear and concise privacy notices and consent mechanisms. Personal data may be collected only for specific, explicit, and legitimate purposes and may not be further processed contrary to such intended purpose. Changes of purpose are permissible only with the consent of the individual or if otherwise permitted by law.

Graphic Packaging only collects Personal Data necessary to achieve our stated purposes and avoids the collection of excessive or irrelevant information. Data collection processes will include appropriate security measures to protect data from unauthorized access, disclosure, alteration, and destruction.

## Data Minimization, Privacy by Design, and Sensitivity Reduction

One of the best ways to protect an individual's privacy is not to collect his or her Personal Data in the first place. Processing of Personal Data that Graphic Packaging possesses must be truly necessary for the intended purpose, and we will only collect the minimum amount needed to complete the purposes of that processing. In other words, we will never collect Personal Data that we have no need for.

It is also Graphic Packaging's explicit goal to implement new applications, services, and products based on the principles of privacy by design and privacy by default. Privacy by design means that privacy must be considered from the beginning and throughout the life cycle of any system, service, product, feature, or process, which requires proactive engagement with technological innovations, risk identification and mitigation in the planning and design phase, and continuous review and reassessment. Privacy by default means that every IT system, service, product, or business practice in our organization is configured to safeguard Personal Data. This means that Data Subjects should not need to perform any extra measures to secure their privacy, and that the default settings in applicable systems should be set to the most protective by default.

Graphic Packaging further minimizes the risk of data exposure by reducing the sensitivity of stored information, wherever possible, by:

- Reducing the precision of the data retained after it has been collected. For example, if a customer phone number is to be used for statistical analysis, only a subset of the digits will be retained, such as the area code.
- Converting Personal Data to a less sensitive form. For example, when using the customer's IP address to determine location for statistical analysis, the IP address will be discarded after mapping it to a city or town.
- Restricting access to large amounts of Personal Data. For example, employees who have a need to access individual records of Personal Data do not automatically have access to batches of Personal Data.

## Maintaining Records of Processing

Certain laws and regulations require Graphic Packaging to maintain accurate records of how and why Personal Data is used, stored, and otherwise processed (these records of processing and the process of creating them

is also known as data mapping). Among other things, the records of processing activities must include the categories of Personal Data that we process, a list of relevant vendors and services providers that we use, the purposes for which we use Personal Data, and any transfers of such Personal Data abroad (such as to vendors located in foreign countries). Data mapping is a fundamental obligation of the EU and UK General Data Protection Regulation (GDPR). Certain U.S. state privacy laws also generally require that organizations such as Graphic Packaging to be able to demonstrate how it uses Personal Data, and the data mapping exercise easily accomplishes this requirement. Graphic Packaging is committed to maintaining an accurate, up-to-date, and comprehensive data map.

## Data Protection Impact Assessments (DPIAs) and Risk

Graphic Packaging's privacy management program aims to control and mitigate privacy risk. Privacy risk focuses on the impact on an individual related to that individual's Personal Data processed by Graphic Packaging. It is part of the greater business risk assessment for Graphic Packaging.

To enable transparency and control in jurisdictions where it is required, Graphic Packaging conducts privacy impact assessments (PIAs) or data protection impact assessments (DPIAs). A PIA or DPIA is conducted as part of the project calendar admission requirements checklist, when required under Graphic Packaging policies, or when otherwise requested by legal or compliance.

The terms PIA and DPIA are often used interchangeably, but typically a DPIA refers to a specific legal obligation under the EU and UK GDPR, while a PIA often refers to a general privacy risk assessment conducted either in accordance with another privacy law or as a privacy program best practice. At Graphic Packaging, we use the term PIA to refer to the initial assessment of risk performed within our OneTrust compliance portal, the results of which determine whether a full DPIA must be conducted.

Conducting a DPIA is not mandatory for all projects that Graphic Packaging may undertake. A DPIA is required by law whenever a project is likely to result in a high risk to the rights and freedoms of individuals, in particular where new technologies are being used.

A DPIA is therefore essentially a risk assessment, which must take into account the nature, scope, context, and purposes of the processing of Personal Data, and must be carried out prior to the start of processing. Regardless of whether a specific Graphic Packaging project is internal or is a process, product, or system provided by a third party, the DPIA should be commenced as early as practically possible in the procurement or design of the project, even if some of the project operations are still uncertain.

More information can be found in the Graphic Packaging ***DPIA Policy and Procedure***, located here: [Data Privacy Impact Assessment Policy](#).

## Legal Bases of Processing Personal Data

Processing of Personal Data is permitted only if Graphic Packaging has a valid lawful basis to do so. There are several available lawful bases for processing Personal Data. It is important that we determine the lawful basis that will be utilized before beginning any processing activities.

Our privacy notices will set out the lawful basis for processing Personal Data for particular purposes. Graphic Packaging should also document our decision on which lawful basis applies for specific processing activities, in order to demonstrate compliance with applicable data privacy laws and regulations.

Typical lawful bases for processing Personal Data include the following:

- **Consent:** This is when the individual (the data subject) has given clear consent to process their Personal Data for a specific purpose. The consent shall be declared in writing or with other legally permissible means, whereby the individual must be informed in advance about the purpose of such processing of Personal Data and any possible transfer. The declaration of consent must be highlighted when included as part of other statements to be clear to the individual.
- **Contract:** This is when processing is necessary for a contract Graphic Packaging has with another organization or individual.
- **Legal Obligation:** This is when the processing of Personal Data is necessary for Graphic Packaging to comply with the law (this does not include contractual obligations).
- **Legitimate Interests:** This is when the processing of Personal Data is necessary for Graphic Packaging's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's Personal Data which overrides those legitimate interests.

## Data Security

### Confidentiality and Authorization

Only the authorized staff of Graphic Packaging, who are obligated to observe the requirements regarding data confidentiality, are allowed to be involved in the processing of Personal Data. It is prohibited for them to use such Personal Data for their own private purposes, to transfer Personal Data to unauthorized parties or to make it accessible in any other improper way to unauthorized people.

"Unauthorized" includes, within this context, any access to or other use of Personal Data by employees that is not to fulfill their employee duties. The confidentiality obligation survives termination of the employment relationship.

### Encryption and Pseudonymization

Anonymization or pseudonymization of Personal Data is used at an early stage, when possible, and where the cost in relationship to the intended protective purpose is reasonable. Enabling pseudonymization is achieved by a balanced measure set, including masking (static and/or dynamic), tokenization and/or encryption.

### Regular Security Audits and Testing

Graphic Packaging conducts regular security audits and assessments to identify vulnerabilities, assess risks, and strengthen security measures. Penetration testing and vulnerability scanning are performed to proactively identify and address potential security weaknesses. Details can be found in the Audit and Compliance Assessment Policy, located here: [Audit and Compliance Assessment Policy](#)

### Monitoring

Graphic Packaging reserves the right to monitor email and web traffic to the extent permitted by law. Additional details can be found in the Acceptable Use of Assets Policy, located here: [Acceptable Use of Assets Policy](#)

### Social Media

Graphic Packaging acknowledges that employees participate in social media activities. Graphic Packaging reserves the right to monitor social media activities to the extent permitted by law, but it will also strive to

protect employees' privacy where possible. Details can be found in Graphic Packaging's Acceptable Use of Social Networking Policy, located here: [Acceptable Use of Social Networking Policy](#)

## **Mobile Device Management (MDM)**

Employees of Graphic Packaging use mobile devices such as smartphones and tablets. Graphic Packaging will strive to protect Personal Data where possible and where the use of these devices for personal reasons is permitted. Details can be found in the following policies:

- **Asset Management Policy**, located here: [Asset Management Policy](#)
- **Mobile Computing Security Policy**, located here: [Mobile Computing Security Policy](#)
- **Personally Owned Devices Policy**, located here: [Personally Owned Devices Policy](#)

## **Data Retention**

The longer that Personal Data is retained, the higher the likelihood of accidental disclosure, loss, theft, and/or information growing stale. In other words, time is a critical success factor for a data breach. At Graphic Packaging, the goal is to retain Personal Data only for the minimum amount of time necessary to support the business purpose or to meet legal requirements.

Any Personal Data kept by Graphic Packaging is managed under the Records Management Program that states how long the data is being kept and why, and the manner in which it will be removed from all data stores.

More information can be found in the Graphic Packaging Records Management Program Policy, located here: [Records Management Program Policy](#)

## **Data Subject Rights**

Graphic Packaging is dedicated to upholding the highest standards of data protection and privacy. As an integral aspect of our commitment to transparency and accountability, Graphic Packaging complies, recognizes and respects the rights of data subjects as outlined in applicable data protection laws and regulations.

## **Special Categories and Sensitive Personal Data**

Special categories of Personal Data may include information revealing racial origin, sexual orientation, political opinions, religious or philosophical beliefs, citizenship and immigration status, trade union membership, and data concerning health or sex life. Such sensitive personal information is defined by and handled in accordance with applicable local data privacy laws.

Taking into account context and attribution, volume, and intended usage, other processing activities of Personal Data at Graphic Packaging may be considered sensitive as well, following the privacy risk assessed. Financial information in the context of Graphic Packaging's salary administration, for example, requires additional protection and security controls.

More information about data classification can be found in the Information Classification Policy, located here: [Information Classification Policy](#)

## Data Sharing and Third Parties

Graphic Packaging may decide to contract with a third party for the collection, storage or processing of data, including Personal Data. The third party may offer services such as hosting, outsourcing, or private or public cloud computing services.

If Graphic Packaging decides to contract with a third party for the processing of Personal Data, this must be reviewed by the IT Project Management Office (PMO) before any contract is executed. Upon approval of the third party for the processing, the relationship with the third party must be regulated by a written agreement in which the rights and duties of Graphic Packaging and of the subcontractor are specified. A subcontractor shall be selected that will guarantee the technological and organizational security measures required in this privacy policy, and provide sufficient guarantees with respect to the protection of the Personal Data and the exercise of rights of data subjects.

The subcontractor must be contractually obligated to process Personal Data only within the scope of the contract and the directions issued by Graphic Packaging. A Data Protection Addendum approved by the Law Department must accompany any contract involving the processing of Personal Data. Processing of Personal Data may not be undertaken for any other purpose. Graphic Packaging remains responsible and accountable for the Personal Data processed by the contract partner.

## Data Breach Notification

Preventing a Personal Data breach is the responsibility of all Graphic Packaging's staff and contracted workforce. In addition, everyone is encouraged to notify the legal counsel responsible for privacy matters or in certain geographies, the data privacy officer, in case of an irregularity in relation to Personal Data processing activities.

A timely discovery, response, treatment, and notification (of both regulatory authorities and potentially the individuals impacted) policy is outlined in Graphic Packaging's Data Breach Response Policy, located here: [Data Breach Response Policy](#) and the Security Incident Response Policy, located here: [Security Incident Response Policy](#)

## International Data Transfer

Personal data that is transferred within or outside the organization is done securely using approved protocols and secure channels. Graphic Packaging complies with relevant legal and regulatory requirements for international data transfers, and ensures that the correct valid data transfer mechanism is used prior to transferring Personal Data internationally. This includes ensuring that Graphic Packaging enters into contracts that comply with applicable data protection laws and regulations with all third party vendors and service providers that may be processing Personal Data on Graphic Packaging's behalf.

## Compliance with Laws and Regulations

Graphic Packaging complies with relevant international, national, and local laws and regulations governing the processing and protection of Personal Data, including, without limitation, the EU GDPR, the UK GDPR, the Brazilian General Data Protection Law, and U.S. federal and state privacy laws.



## Training, Awareness and Enforcement

Graphic Packaging will ensure that the general principles set forth in this privacy policy are observed. In this respect, managerial staff of Graphic Packaging shall ensure that this policy is implemented, which includes, in particular, providing policy information to employees.

Employees are also required to acknowledge their understanding of, and commitment to follow, this privacy policy.

If additional training is required, a request should be made of the Privacy Committee. Policy information shall also include a reminder that violating the general principles of this privacy policy may entail, under certain circumstances, legal consequences, such as criminal penalties, liability and employment consequences.

## Data Protection Officer (DPO)

Graphic Packaging has appointed a global DPO to supervise and ensure compliance with data protection laws and regulations. Where applicable or necessary, Graphic Packaging has also appointed local DPOs to fulfill local compliance requirements. The DPOs' contact information, including full name, position, and contact details, is provided for individuals to reach out regarding any data protection concerns, questions, or requests. The DPO collaborates with management, employees, and relevant stakeholders to ensure a comprehensive approach to data protection throughout the organization and serves as a point of contact for inquiries regarding data protection at Graphic Packaging.

## Version Control

| <b>Date</b> | <b>Description of Change</b> | <b>Author</b> |
|-------------|------------------------------|---------------|
| XX          | XX                           | XX            |
|             |                              |               |