Document Owner: Legal-Compliance
Subject Matter Experts: Sr. Legal Counsel Europe

Data Protection Policy

1.0 INTRODUCTION

1.1. Plastipak's Data Protection Policy ("DPA") applies to all representatives and Associates (defined as any person who is employed by the Company), including but not limited to supervisors, managers, consultants, directors, officers and any other persons whose business activities are conducted for or on behalf of Plastipak Holdings, Inc. and/or any of its subsidiaries located in the European Union ("Plastipak").

1.2. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards.

2.0 PURPOSE

2.1. Plastipak is committed to compliance with all relevant EU laws in respect of personal data, and to protect the "rights and freedoms" of individuals whose personal information Plastipak processes in accordance with the General Data Protection Regulation ("GDPR"). Plastipak is committed to provide each Associate with information about his/her personal data processing in a concise, transparent and intelligible manner, which is easily accessible, distinct from other undertakings between Plastipak and Associate, using clear and plain language.

2.2. This data protection policy ensures that Plastipak:

- complies with data protection law and follows good practice;
- protects the rights of Associates;
- is transparent and open about how it stores and processes individuals' data.

3.0 APPLICABILITY

This policy applies to all Associates and interested parties of Plastipak such as outsourced suppliers, partners and any third parties working with or for Plastipak, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy.

4.0 PERSONAL DATA

4.1. As the employer, Plastipak is required to process and maintain information for employment purposes.

The following personal data may be processed by Plastipak (this list is not exhaustive):

- Name(s) and surname(s), date of birth, residence (address), national security number of the Associate and his/her family;

- Employee photograph for organizational charts, organizational announcements, internal media or intranet;
- CV, application form and references during the recruiting and onboarding of the Associate;
- Contract of employment and any amendments to it;
- Compensation and Benefits: bank account details, salary, information needed for payroll, compensation and benefits and expenses purposes; pension scheme/plan/contributions;
- Transferring personal data to third parties if Plastipak is legally obliged to do so or needs to comply with its contractual duties to you, for instance need to pass on certain information to external payroll providers, pension or health insurers and providers, and Governmental Authorities;
- Employment administration: records of holiday, sickness (medical certificate and other absence information), attendance and time management and business travel management;
- Correspondence with or about Associates, for example letters about a pay raise or, at Associate's request, a letter to mortgage company confirming the contact;
- Emergency contact details; personal data for health and safety and occupational health obligations;
- Records related to career history, such as training records, appraisals, other performance measures and, where appropriate, disciplinary and grievance records.

4.2. Processing such personal data is necessary for entering into an employment relationship with Plastipak or working under an existing contract or employment relationship with the Associates. Therefore, conducting ordinary business activities will be considered a legal basis that permits processing this personal data. The information we hold and process will be used for our management and administration only. We will keep and use it to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately, during the recruitment process, employment and post-employment legal obligations. This includes processing information to enable us to comply with the employment contract, and all legal requirements. If Plastipak does not process this kind of personal information, Plastipak may be unable in some circumstances to comply with our (contractual or legal) obligations.

5.0 DISCLOSURE

According to the GDPR, Plastipak may disclose personal information without individual consent so long as the data is requested for one or more of the following purposes:

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, this refers to life and death situations.

6.0 PLASTIPAK'S COMMITMENT

Plastipak is committed to complying with the GDPR and good practice including:

- processing personal data only where this is strictly necessary for contractual and legitimate organizational purposes;

- collecting only the minimum personal data required for these purposes and not processing excessive personal data;
- providing clear data to Associates about how their personal data will be used and by whom;
- only processing relevant and adequate personal data;
- processing personal data fairly and lawfully;
- maintaining an inventory of the categories of personal data processed by Plastipak;
- keeping personal data accurate and secure;
- retaining personal data only for as long as is necessary for legal or regulatory reasons or, for legitimate and contractual organizational purposes;
- respecting individuals' rights in relation to their personal data, including their right of subject access;
- only transferring personal data outside the EU in circumstances where it can be adequately protected under the EU-U.S. Data Privacy Framework Principles and subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC);
- developing and implementing awareness and training to enable the policy to be implemented;
- where appropriate, identifying internal and external stakeholders and the degree to which these stakeholders are involved in the governance of this policy.

7.0 RIGHTS AND OBLIGATIONS OF ASSOCIATES

7.1. Associates have the following rights regarding data processing, and the data that is recorded about them by Plastipak:

- to make subject access requests regarding the nature of data held and to whom it has been disclosed and to receive a copy upon request;
- the right to rectification. When personal data is inaccurate, Plastipak must employ means to correct it;
- the right to erasure or right to be forgotten subject to statutory obligations;
- the right to restriction of processing: the right to limit the processing of his/her personal data;
- the right to be informed of the usage and collection of personal data;
- the right to data portability: to obtain and reuse their personal data for their own purposes across different services;
- the right to object to the processing of inaccurate or irrelevant personal data;
- the right to be informed within 72 hours in case of a data breach.

7.2. Associates have the following obligations regarding data processing;

7.2.1. All Associates are responsible for ensuring that any personal data which Plastipak holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorized by Plastipak to receive that data and has entered into a data protection agreement.

7.2.2. All Associates should exercise caution when asked to disclose personal data held on another individual to a third party and may be required to attend specific training to enable them to deal effectively with any such risk.

8.0 COMPLAINTS AND EXCERCISE RIGHTS

Associates

- who have questions related to the GDPR;
- have any regulatory concerns as to how personal data is processed;
- who want to exercise their rights under the GDPR,

may inquire directly with the Data Protection Team by sending an e-mail to GDPR_Questions@plastipak.eu.

9.0 DATA BREACH

9.1. There is an obligation on Plastipak to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the Associate. If there has been a data breach which compromises an Associate's personal data, the Associate has a right to be informed within 72 hours of first having become aware of the breach.

9.2. In case of a data security breach, there is an obligation of the Plastipak personnel to report these data security breaches to the Data Protection Team immediately.

10.0 EU-U.S. Data Privacy Framework (Principles)

10.1. Plastipak complies with the EU-U.S. Data Privacy Framework Principles as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. Plastipak has certified to the Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles. If there is any conflict between the terms in this privacy policy and the EU-U.S. Data Privacy Framework, the EU-U.S. Data Privacy Framework Principles shall govern. To learn more about the EU-U.S. Data Privacy Framework (Principles), and to view our certification, please visit Data Privacy Framework-website.

10.2. In compliance with the EU-U.S. Data Privacy Framework (Principles)

10.2.1. Plastipak commits to resolve complaints about the collection or use of your personal information. EU individuals with inquiries or complaints regarding the EU-U.S. Data Privacy Framework Principles should first contact the Data Protection Team by sending an e-mail to GDPR_Questions@plastipak.eu.

10.2.2. Plastipak has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) with regard to unresolved EU-U.S. Data Privacy Framework complaints concerning human resources data transferred from the EU in the context of the employment relationship.

10.2.3. Plastipak has responsibility for the processing of personal information it receives under the EU-U.S. Data Privacy Framework and subsequently transfers to a third party acting as an agent on its behalf. Plastipak shall remain liable under the EU-U.S. Data Privacy Framework if its agent processes such personal information in a manner inconsistent with the EU-U.S. Data Privacy Framework, unless the organization proves that it is not responsible for the event giving rise to

the damage.

10.2.4. An Associate may initiate binding arbitration under the EU-U.S. Data Privacy Framework for unresolved complaints and to attempt to resolve the issue.

11.0 DOCUMENT OWNER AND APPROVAL

The Legal Department and Data Protection Team is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all Associates on the corporate intranet and is published in the following link.

12.0 DEFINITIONS

Associate – any individual who is the subject of personal data held by an organization.
Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.
General Data Protection Regulation (GDPR) – The GDPR replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of living individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.
Personal data – any data relating to an identified or identifiable natural person ('Associate'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to mental, physical, physiological, genetic, economic, cultural or social identity of that person.
Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the Associate.
EU-U.S. Data Privacy Framework (Principles) or DPF Program – Framework that was designed by the U.S. Department of Commerce and the European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States.
Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Territorial scope – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of Associates, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behavior to Associates who are resident in the EU.

13.0 REVISION HISTORY

Revision	Date	Description of Changes	Requested By
1	15/10/2018	Compliancy Privacy Shield Framework	Matthias M.
2	17/12/2018	Compliancy Privacy Shield Framework	Matthias M.
3	09/12/2024	Compliancy DPF Program	Matthias M.