June 12, 2025

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is entered into and effective as of the Effective Date defined under the Agreement (the "**DPA Effective Date**''), by and between the recipient of the services under the Agreement ("**Controller**") and Avery Dennison Corporation or its relevant Affiliates ("**Processor**" or "**Avery Dennison**"), collectively referred to as the "**Parties**".

WHEREAS, the Controller and Processor wish to enter into an agreement that governs the processing of personal data on behalf of the Controller (the "**Data**"), as more fully set forth herein;

NOW, THEREFORE, for good and valuable consideration, the adequacy of which is hereby acknowledged, Controller and Processor hereby agree as follows:

1. Definitions

In this Data Processing Agreement, the following terms shall have the following meanings:

(a) "**Agreement**" means the services agreement between Controller and Processor (or their respective Affiliates) to which this DPA is incorporated.

(b) "**Affiliate**" means any legal entity that directly or indirectly controls, or is controlled by, or is under common control with a Party. For the purposes of this definition, control will mean the direct or indirect ownership of, (a) in the case of corporate entities, securities authorized to cast more than fifty percent (50%) of the votes in any election for directors or (b) in the case of non-corporate entities, more than fifty percent (50%) ownership interest with the power to direct the management and policies of such non-corporate entity

(c) "**Controller**", "**Processor**", "**data subject**", "**personal data**", "**processing**" (and "**process**"), **‘’data breach”** and "**special categories of personal data**" shall have the meanings given in the data protection laws applicable to the processing of personal data under the Agreement, including, where relevant, the EU Data Protection Law and other comparable legal frameworks.

(d) **‘’Data”** in the context of this DPA refers to personal data as defined under the applicable data protection law, and shall be interpreted in accordance with the relevant privacy and data protection regulations governing the processing of such data, including, but not limited to, the EU Data Protection Law.

(e) "**Applicable Data Protection Law**" means all worldwide data protection and privacy laws and regulations that apply to the processing of personal data under this Agreement, including, but not limited to, the EU Data Protection Law, as well as any other local, regional or international legislation or regulation applicable to the relevant jurisdictions involved.

(f) **‘’EU Data Protection Law”** means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing

of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "**GDPR**")

2. Relationship of the Parties

2.1. Customer appoints Avery Dennison as a processor to process the Data described in this DPA, as detailed further in Appendix A, for the purposes described in this DPA (or as otherwise agreed in writing by the parties). Each party shall comply with the obligations that apply to it under Applicable Data Protection Law, and Avery Dennison shall promptly inform Customer if, in Avery Dennison's opinion, the Customer's processing instructions infringe Applicable Data Protection Law.

3. Purpose and Scope

3.1. The purpose of this DPA is to ensure the lawful and transparent processing of personal Data described under Appendix A, for the sole purpose of providing the services described under the Agreement.

3.2 The Processor will process the Data in accordance with the documented instructions of the Controller, except where otherwise required by any applicable law to the Processor. In no event Processor processes the personal data for its own purposes or those of any third party.

4. Confidentiality of processing

The Processor shall implement technical and organizational measures as set out in Appendix B to protect the personal data from (i) accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to the Data (a "**Security Incident**").

5. Subprocessing

5.1. The Controller authorizes Processor and each Processor Affiliate to appoint Subprocessors (listed in Appendix A) in accordance with this Section 5 and any restrictions established under this DPA.

5.2. The Processor shall not subcontract any processing of the personal data to a third party subprocessor without the prior written authorization of the Controller.

5.3 The Processor shall impose the same data protection obligations as set out in this DPA by way of a contract or other legal act that is binding to the Parties and ensures the processing will meet the requirements of the Applicable Data Protection Law.

6. Data Breach

6.1. Upon becoming aware of a Data Breach, Processor shall inform Controller without undue delay and in any event within seventy-two (72) hours of becoming aware of a Data Breach, providing Controller with sufficient information to allow Controller and each Controller Affiliate (as applicable) to report or

inform supervisory authorities and data subjects of the Data Breach under the Applicable Data Protection Laws.

6.2. Processor shall take all such measures and actions as are necessary to remedy or mitigate the effects of the Data Breach and shall keep Controller informed of all developments in connection with the Data Breach.

7. Deletion or Return of Data

Upon termination or expiry of this DPA, the Processor shall, at Controller's request, destroy or return to the Controller all personal data (including all copies of the personal data) in its possession or control. This requirement shall not apply to the extent that Processor is required under the applicable data protection law, including the EU law, or any other applicable local, regional or international legal obligation, to retain some or all of the personal data, in which event Processor shall isolate and protect the personal data from any further processing except to the extent required by such law.

8. Cooperation and Data Subject Rights

The Processor shall provide all reasonable and timely assistance to the Controller in fulfilling its obligations to respond to (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including, without limitation, its rights of access, correction, objection, erasure and data portability, as applicable) and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the personal data. In the event that any such request, correspondence, enquiry or complaint is made directly to the Processor, the Processor shall inform the Controller providing full details of the same without undue delay.

9. Processor and Processor Personnel

Processor and each Processor Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to personal data, ensuring in each case that access is limited to those individuals who need to know/access the relevant personal data and to comply with applicable laws in the context of that individual's duties to Processor or the Processor Affiliate, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

10. Audit and Inspection

10.1. The Processor shall respond to any written audit questions submitted to it by the Controller, provided that the Controller shall not exercise this right more than once per year. However, if a Data Breach has occurred by a breach of Processor’s security measures, the Controller may exercise this right as reasonably necessary to ensure the security of the personal data.

10.2. The Processor shall permit the Controller (or its appointed third party auditors) to audit the Processor's compliance with this DPA, and shall make available to the Controller all information, systems and staff necessary for the Controller (or its third party auditors) to conduct such audit. The Controller shall give a prior notice of at least 10 working days of its intention to audit, conduct its audit during normal business hours, and take all reasonable measures to prevent unnecessary disruption to the Processor's operations. The Controller will not exercise its audit rights more than once in any twelve (12)

calendar month period, except (i) if and when required by instruction of a competent supervisory authority; or (ii) the Controller believes a further audit is necessary due to a Data Breach suffered by the Processor.

11. **International transfers**

11.1 If personal data originates from the European Economic Area (''EEA'') under this DPA, Avery Dennison shall not transfer the personal data outside of the EEA unless it has taken such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Such measures may include (without limitation) transferring the personal data to a recipient (a) in a country the the European Commission has decided provides adequate protection for personal data, (b) that has achieved binding corporate rules authorisation in accordance with Applicable Data Protection Law, (c) that has executed standard contractual clauses adopted or approved by the European Commission.

11.2. Onward transfers of Personal Data by the Processor shall be made in strict compliance with Applicable Data Protection Law and - if applicable, and to the extent that the EU law applies - the Processor shall ensure that the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 (Module Three for processor to processor transfers) are incorporated into the contract with the Sub-Processor before the onwards transfer takes place. The Processor shall sign a written agreement with each Subprocessor that imposes obligations on that Subprocessor that are no less stringent than those required under this DPA.

12. Term and Termination

12.1. This DPA will remain in effect as long as the Processor processes Data on behalf of the Controller.

12.2. The DPA can be terminated by either party with a written notice in accordance with the terms set out in the Agreement.

13. Limitation of Liability

Any liability arising out of or in connection with this DPA shall follow, and exclusively be governed by, the liability provisions set forth in, or otherwise applicable to, the Agreement.

14. Effect of the DPA

This DPA supplements the terms of the Agreement and to the extent there is conflict between this DPA and the Agreement, the terms of this DPA shall prevail. Notwithstanding this, nothing in this DPA shall be construed to diminish the rights of either party under the Agreement.

15. Governing Law and Jurisdiction

15.1. The Parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity.

15.2. This DPA shall be governed by the laws of the country or territory stipulated for this purpose in the Agreement.

16. General Terms

16.1 Nothing in this DPA reduces Processor's or any Processor Affiliate's obligations under the Agreement in relation to the protection of Personal Data or permits Processor or any Processor Affiliate to Process (or permit the Processing of) personal Data in a manner which is prohibited by the Agreement.

16.2. With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including without limitation, the Agreement, the provisions of this DPA shall prevail.

Appendix A

Details of Data Processing
The following sets out details of the Personal Data which will be processed under this DPA: ● **Data Subjects** - End users of Controller's services ● **Categories of Data** – IP addresses of end users and their device name, operating system internet browser information, product information ● **Special categories of data (if applicable)** – Not applicable. ● **Processing operations** - Collection, storage, access, conversion, transfer, erasure of Data for the purpose of delivering the services to the Controller. ● **SubProcessors** - Controller authorize the Processor engaging the following third party subprocessor to process the personal data for hosting services: Microsoft Azure Corporation, Ireland. ● **Transfers of personal data outside the European Economic Area** – The agreement will specify the countries to which data of individuals in the European Economic Area can be transferred.

International Data Transfers <u>(only applicable for the transfer of personal data outside the EEA)</u>
Controller (as ''data exporter'') and Processors (as ''data importer''), as appropriate, (as ''data importer'') shall enter into the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 (Module Two for controller to processor transfers)Standard Contractual Clauses in respect of any Restricted Transfer from Controller to that Contracted Processor. The Parties agree to incorporate the Standard Contractual Clauses (SCCs) as follows: ● In Clause 7 of the SCCs, the optional docking clause will apply; ● In Clause 9 of the SCCs, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Clause 5 of this DPA; ● In Clause 11 (a) of the SCCs, "Redress" will not apply; ● In Clause 17 of the SCCs, Option 1 will apply, and the SCCs will be governed by Controller's governing law; ● In Clause 18(b) of the SCCs, disputes shall be resolved before the competent courts where the Controller is established within the European Economic Area. ● Annex I of the SCCs shall be deemed completed with (as to Part A) information set out in the DPA with respect to the Parties thereto, (as to Part B) with the information set out in Appendix B to this DPA and (as to Part C) with the Dutch supervisory authority. ● Annex II of the SCCs shall be deemed completed with the information set out in this Annex. ● Annex III of the SCCs shall be deemed completed with the information set out in Appendix A to the DPA.

Appendix B

Security Measures

Processor and any applicable Processor Affiliate shall implement adequate organizational and security measures to protect Personal Information. Such security measures should include without limitation those set forth below:

Software Development

1. All software engineers receive software security training that covers security best practices including OWASP Top Ten and Mobile Security best practices.
2. Use of static code analysis tools to analyze code for security vulnerabilities.
3. All source code is developed in accordance with a standard Software Development Life Cycle (SDLC) process that includes:
    (a) Software and Security code review before being promoted to production use;
    (b) Running through a continuous integration test suite; and
    (c) Manual quality assurance testing

Hosting Environment

1. All hosting environments use carrier class data centers having high availability standards and redundancy. Typical certifications for these data centers include:
    (a) PCI DSS Level 1 Service Provider;
    (b) SOC 1 Type II & SOC 2 Type II; and
    (c) ISO 27001

Confidentiality

1. Personal Information is not made available or disclosed contrary to as provided in this Addendum.
2. Personal Information is processed only in accordance with this Addendum and only as required for the performance of the Services.
3. Processor takes precautions to prevent viewing of computer screens that may contain Personal Information. When outside of a Processor facility, Processor employees and sub-processors may only access Personal Information in a private space or utilize a privacy screen to obscure the Personal Information from unauthorized viewing.
4. Processor ensures that all employees, agents, sub-processors, and representatives likely to handle Personal Information are under a duty of confidentiality and receive appropriate security awareness training.

Electronic Data

To protect Personal Information, Processor takes the following precautions when handling electronic data:
1. Personal Information, beyond communication of chatter and email, is not stored on a personal mobile-phone
2. Personal Information is never stored on transportable media that is not owned by the Processor or a Subprocessor. Any devices, discs, and other electronic storage media containing Personal Information must be destroyed once no longer needed in a manner that makes access to Personal Information stored on them impossible.
3. Any files temporarily stored on a laptop are deleted when the relevant work/project ends.

Paper Data

While most documentation and data is managed electronically, there are some circumstances that require printing of paper documents, such as validation documents that require a handwritten signature. When handling printing documents, the Processor will take every precaution to prevent its exposure to anyone outside of those individuals authorized to access the Personal Information contained within those printed documents.

Personal Information contained in printed form is shredded immediately after its use. For validation documents, documents are shredded after all approvals are hand-signed and the document has been scanned.

Passwords and Encryption

All Personal Information is encrypted to prevent unauthorized access and access to such Personal Information is password protected. The encryption key and passwords are kept secure at all times.

All web traffic is encrypted by TLS 1.2 or greater. The Processor follows NIST recommendations for hashing symmetric and asymmetric encryption.

Security Incidents

If the Processor becomes aware of unauthorized access or disclosure of Personal Information under its control, it will adhere to the instructions described in this Agreement.

Audit

Provider executes internal security audits in accordance with its internal audit policies and procedures. Any remedial measures identified in an audit will be fully and promptly implemented.

Access Control

Access to Personal Information is restricted pursuant to Processor's internal access control policies and procedures. Authorized personnel will be permitted to access Personal Information only to the extent necessary for the performance of their duties.