GLOBAL DATA PROTECTION TERMS GLOSSARY

Version 2.0 This document was last updated on July 2nd, 2024.

The definitions provided in this Glossary apply specifically and exclusively to agreements, including but not limited to any master agreements and work orders or similar documents thereunder entered into by any entity that is part of Kenvue and its affiliates. These definitions may not be exactly the same as external industry standards. Therefore, it is imperative that the terms outlined in this Glossary be strictly interpreted as described herein when entering into agreements with Kenvue.

While the terms included in this Glossary may not be present in all Kenvue Data Protection Exhibits, they are commonly encountered in such agreements, serving to elucidate recurring concepts pertinent to privacy and data protection. This enhances the accessibility and comprehensibility of the agreements in this regard.

"Aggregated Data" are data of multiple individuals that have been combined to show general trends or values and data identifying a particular individual has been removed.

"Anonymization" is the process of removing all identifiers linked to a particular individual such that a code or other association for re-identification no longer exists under Applicable Data Protection Laws.

"**Applicable Data Protection Laws**" are any laws including national implementing legislation, regulations and binding lawful orders of a competent public authority relating to data protection including data privacy, cybersecurity, electronic communications or the Processing of Personal Data. Applicable Data Protection Laws may also include without limitation HIPAA, GDPR, CCPA, LGPD, PIPL.

"**Assistance Expenses"** are the reasonable expenses related to investigations or remediations of a Data Incident. The expenses may include but are not limited to costs associated with forensic analysis, legal consultations, notice to Data Subjects and any other activities necessary to resolve Data Incidents, whether initiated by the Processor or in response to requests from the Controller or regulatory/competent authority.

"Biometric Data" are Personal Data coming from technical Processing relating to the physical, physiological or behavioral characteristics of an individual, which allow or confirm the unique identification of that individual, such as facial images, DNA or voice.

"Business Continuity and Disaster Recovery Plan" is the plan and processes for preventing catastrophic data and/or operations loss and resume operations timely in the event of system failure, damage, or destruction, to ensure fulfillment of products and services to Buyer.

"**Company Confidential Information**" Unless otherwise defined in the Agreement, is data that the Company has or will develop, acquire, create, compile, discover or own, that has value to the

Company's business which is not generally known to the public and which the Company wishes to maintain as confidential. For example, trade secrets, marketing plans or patent filings.

"**Confidentiality**" Unless otherwise defined in the Agreement, is the obligation to protect Personal Data and Company Confidential Information and not misuse or wrongfully disclose that information.

"**Consent**" is the permission or authorization given by the Data Subjects for the Processing of their personal data for specific purposes. It must be voluntary, informed, and unambiguous, meaning the person must fully understand what they are consenting to and must have the freedom to accept or refuse without negative consequences.

"Consumer Health Data – US only" are consumer health data which identify or can identify an individual, even if identification requires third party assistance (such as Meta Pixel or Google Analytics) and can be used to identify the past, present, or future physical or mental health status of an individual; and can include a health-related inference derived from non-health information by any means, including algorithms or machine learning.

"**Controller**" is the individual or legal entity which, alone or jointly with others, determines the purposes and means of Processing Personal Data.

"Data Incident" is any confirmed or suspected unauthorized access, use, alteration, disclosure, loss, damage or destruction of Personal Data and/or Company Confidential Information which negatively impacts that data's confidentiality, integrity or accessibility, or any "breach" as defined in the Applicable Data Protection Laws.

"**Data Protection Authorities**" are the official public bodies which are responsible for monitoring and enforcing compliance with Applicable Data Protection Laws and investigating alleged Data Incidents of these laws.

"**Data Protection Officer**" is an individual appointed by a company who advises on the implications of Applicable Data Protection Laws and oversees the development of the company's data protection policies and represents it to Data Protection Authorities.

"Data Subject" is any individual person whose Personal Data is Processed.

"**De-identification**" is the process of rendering data Pseudonymized or Non-Personal Data.

"**EU SCCs**" are the currently applicable EU Standard Contractual Clauses approved by the EU Commission and their respective Annexes.

"Gen AI" is a category of artificial intelligence (AI) algorithms that generate new outputs based on the data on which they have been trained. Examples of Gen AI include, but are not limited to: ChatGPT, Promethean AI, Google Gemini, Baidu Ernie, Microsoft 365 Copilot and Anthropic's CLAUDE.

“Government Identifiers” are government-issued personal identifiers such as a social security number, passport number, tax number, national identification number, birth certificate, or driver’s license number.

“HIPAA” is the Health Insurance Portability and Accountability Act (HIPAA), a U.S. law passed to create national standards for electronic healthcare transactions, among other purposes. The U.S. Department of Health and Human Services has promulgated regulations to protect the privacy and security of Protected Health Information.

“Non-Personal Data” are data that do not or no longer fall in scope of Personal Data definitions under Applicable Data Protection Laws and may include Company Confidential Information and Anonymized Data.

“**Opt-in**” is an active affirmative indication of choice of the Data Subject relating to the Processing of their Personal Data such as checking a box or electronically signing a form.

“**Opt-out**” is either an active affirmative indication of the Data Subject to stop the Processing of their Personal Data (e.g. selecting to unsubscribe from an email communication) or a lack of action after they are informed about their Personal Data Processing.

“**Personal Data**” is any information which is directly or indirectly related to, linked or reasonably linkable, independently or by combining with other data elements, to an identified or identifiable person.

“Privacy Designee” is a resource within the Kenvue Privacy team who, as part of their role, are responsible for advising on Personal Data protection matters for a specific region, country or specific operation.

“Privacy Notice” is a statement to a Data Subject that describes how their Personal Data is Processed.

“**Process,**” “**Processed,**” and “**Processing**” is any operation on Personal Data whether or not by automatic means, including its collection, use, access, disclosure, transfer, storage, deletion or any other operation on Personal Data according to Applicable Data Protection Laws.

“**Processor”** is any third party such as an individual or a legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

“Protected Health Information”, "**PHI**", or "**Individually identifiable health information**" is information, including demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number, medical information on medical records such as diagnosis or treatment). Note: The Personal Data must be combined with medically related

information or be derived or Processed in a medical setting for it to fall under HIPAA (Health Insurance Portability and Accountability Act) or the definition of PHI.

"Pseudonymized Data" is Personal Data that can no longer be attributed to a specific individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures, to ensure the Personal Data is not linked to an identified or identifiable individual.

"Public Data" is information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

"Secondary Use" is Processing of existing Personal Data or Company Confidential Information for a purpose different from the purpose for which the data were initially collected or in a manner which is not explicitly covered by the Agreement or Services.

"Sensitive Personal Information" (or "**Sensitive Personal Data")** is Personal Data that may affect the more intimate sphere of its owner, or whose improper use may give rise to discrimination or a serious risk to the individual. This includes but is not limited to information concerning health, sexual orientation, biometric information, precise geolocation, racial or ethnic origin, political views or any other Personal Data defined as sensitive or special category under Applicable Data Protection Laws.

"Shared Data" is Personal Data or Company Confidential Information shared with another party/(ies).

"**Sub-Processor**" is any third party who is Processing of Personal Data on behalf of the Processor.

"**State Comprehensive Privacy Law**" is a body of regulations enacted by an individual state that governs the protection and processing of Personal Data by entities operating within that state.