## 1. PURPOSE AND SCOPE

This Protecting Personal Data Policy ("Policy") describes responsibilities of Perrigo Personnel with respect to protecting, handling and using Personal Data.

"**Personal Data**" means any information that can directly or indirectly identify an individual. Examples of Personal Data include, but are not limited to, a person's name, address, telephone number, email address, date of birth, social security/insurance number or other equivalent, genetic or biometric data, photographs, racial or ethnic origin, marital status, employee identification number, salary and other remuneration details, bank account information, citizenship, and benefit information.

This Policy applies to all **Perrigo Personnel,** including employees, temporary employees, contractors, consultants, operating groups, subsidiaries, and departments worldwide.

## 2. RESPONSIBILITIES

In the course of their job duties, Perrigo Personnel may come in contact with Personal Data of others, for example, Perrigo employees, consumers, customers and vendors. Perrigo Personnel must handle Personal Data to ensure it is safeguarded and kept confidential in accordance with data protection principles and guidelines in this policy.

Failure to comply with the Policy puts Personal Data at risk. Violations may be investigated and may result in disciplinary action, up to and including termination of employment or contract.

## 3. DATA PROTECTION PRINCIPLES

Data protection laws and regulations describe what organizations must do when they collect, use, store, disclose and destroy. Personal Data. These rules apply to all Personal Data, whether it is stored electronically, on paper, or another means.

Generally, laws protecting privacy require organizations to:

- Have a legal basis to collect or process Personal Data
- Be transparent about how Personal Data is used or disclosed
- Use Personal Data for the purpose(s) it was obtained
- Hold Personal Data only for as long as necessary
- Take reasonable efforts to secure Personal Data
- Ensure that Personal Data is only transferred to other authorized parties
- Respect individuals' privacy rights

Certain types of Personal Data that Perrigo may collect are considered particularly sensitive ("**Sensitive Data**") because individuals may be put at a significant risk if the data is misused, for example:

- Health, genetic, and biometric data
- Financial account information
- Government-issued identification number, such as a National ID or Social Security number
- Information related to children or minors
- Race or ethnic origin
- Political opinions
- Religious and philosophical beliefs
- Sex life and sexual orientation

- Criminal history

Perrigo Personnel should make every attempt to safeguard Sensitive and Personal Data and keep it secure and confidential by following the **Global Information Security Policy,** the **EU Information Security Policy** and related standards and procedures.

## 4. DATA COLLECTION

Perrigo only collects Personal Data to accomplish specific business purposes or where there is a legitimate business need to do so. Consistent with jurisdictionally-specific privacy laws, when Perrigo collects data from individuals, it will provide them with notice about how Perrigo may collect, use, store, transfer, or disclose their Personal Data and seek their consent where appropriate. Perrigo will also provide individuals with information on how to withdraw that consent or opt-out of certain uses or disclosures of their Personal Data when applicable.

## 5. DATA USE

Perrigo Personnel may only process Personal Data to accomplish the purposes for which it was collected. Therefore, Perrigo Personnel must not process Personal Data other than for the business purpose for which it was lawfully obtained. If Personnel are uncertain for what purpose(s) they can process Personal Data, they must consult their supervisor or the Global Privacy Office.

In some instances, Perrigo may be able to process Personal Data for a new purpose when:

- Those other purposes are appropriate and directly related to the original business purpose or
- The individual has provided consent for the other purpose

However, processing Personal Data for a new purpose must be notified to the Global Privacy Office at globalprivacyoffice@perrigo.com

Only Personal Data that is accurate, complete, and up-to-date should be used to accomplish these purposes. If Perrigo Personnel are concerned that Personal Data are not accurate, complete, and up-to-date, they should consult their manager or the Global Privacy Office.

When these purposes for which Personal Data were collected have been accomplished, Perrigo Personnel should delete or destroy Personal Data as described in the **Data Destruction Security Standard** and within the time period set out in the **Global Records Management & Retention Policy**.

## 6. DATA STORAGE

Personal Data must be stored in a way that protects it from inappropriate alteration, accidental deletion, unauthorized access, or malicious hacking attempts. Perrigo Personnel should be familiar with the restrictions and obligations on storing and transmitting Perrigo Data (which includes Personal Data) set out in the **Global Information Security Policy** and the **EU Information Security Policy** which explains that Personal Data may not be stored on or transferred to any location, system, account, computer, server, removable media, other device, or cloud service unless it is owned or approved by Perrigo IT&S.

If Personal Data exists on hard-copy print outs, those papers must be kept in a secure place where unauthorized individuals cannot access the documents, for example in a locked drawer or

filing cabinet. Perrigo Personnel must not leave any papers containing Personal Data out in the open or unattended where it may be accessed or visible to unauthorized individuals.

## 7. DATA SECURITY

Perrigo Personnel have an obligation to ensure they collect, use, or store Personal Data in a way that protects the Data's confidentiality, integrity, and availability. Perrigo Personnel should review and understand obligations set forth in the **Global Information Security Policy** or the **EU Information Security Policy** and related standards or procedures.

As explained in the **Global Information Security Policy** and **the EU Information Security Policy**, Perrigo Personnel are required to immediately report to IT&S or the Global Privacy Office any incident or suspected incidents of unauthorized access and/or disclosure of Perrigo Data, including Personal Data.

## 8. DATA TRANSFERS

Laws protecting privacy generally prohibit sharing, disclosing, or otherwise transferring Personal Data to other parties or companies unless certain conditions have been met. Perrigo Personnel must not transfer Personal Data to any other individuals or business units within Perrigo unless those parties are authorized to receive the data.

Similarly, Perrigo Personnel must not transfer Personal Data to any vendors, service providers, or other external third parties unless they are authorized to receive Personal Data. Perrigo Personnel may only engage in agreements to transfer Personal Data to such third parties after contacting Perrigo's Legal Department (Legal@perrigo.com) .

If Perrigo Personnel have questions about whether they are permitted to transfer Personal Data within Perrigo, a third party, or service provider, they should seek advice from their manager, Legal Department or the Global Privacy Office.

## 9. INDIVIDUALS' PRIVACY RIGHTS

Laws protecting privacy provide individuals with certain rights over their Personal Data. These rights vary by country, state, province, or municipality and Perrigo Personnel should be familiar with their obligations under Local Laws. If Perrigo Personnel become aware of an individual's request to exercise their rights over their Personal Data, Personnel should immediately refer the request to globalprivacyoffice@perrigo.com

## 10. RELATED DOCUMENTS

Please refer to **Inside Perrigo** (Global Policies) for the following documents:

- Global Information Security Policy
- EU Information Security Policy
- Global Records Management & Retention Policy
- Data Destruction Security Standard

For questions relating to this Policy please contact the Global Privacy Office at: globalprivacyoffice@perrigo.com.

## 11. VERSION CONTROL

| | |
|---|---|
| **VERSION NO** | VERSION 2.0 |
| **DEPARTMENT** | GLOBAL ETHICS & PRIVACY |
| **REVIEW DATE** | 17 February 2020 |
| **EFFECTIVE DATE** | 1 March 2020 |
| **APPROVED BY** | Compliance and Corporate Values Committee (CCVC) |