1. PURPOSE AND SCOPE

This policy describes how Personal Data that Perrigo holds on employees, contractors, customers, suppliers and others is collected, used and stored to comply with applicable privacy laws and regulations around the globe.

Personal Data means any data that can directly or indirectly identify an individual and includes, without limitation, name, address, telephone number, photograph, marital status, email address, date of birth, social security/insurance number or other equivalent, employee identification number, salary and other remuneration details, bank account information, citizenship, job/position title, and benefit information.

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

All Perrigo Personnel are expected to comply with this policy. Violations will be investigated and may result in disciplinary action, up to and including termination of employment or contract.

Please refer to the document "Privacy Definitions & Terms" available on Inside Perrigo (under Global Policies).

2. DATA PROTECTION PRINCIPLES

Data protection laws and regulations describe what companies and organizations must do when they collect, use and store Personal Data. These rules apply when Personal Data is stored electronically, on paper, or by any other means.

Privacy principles require that Personal Data must be:

- Processed fairly and lawfully, in accordance with the rights of individuals
- Obtained only for specific, lawful purposes
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Held only for as long as necessary (please refer to the Records and Information Management Policy)
- Protected in appropriate ways

3. RESPONSIBILITIES

All Perrigo Personnel are responsible for ensuring that Personal Data is collected, stored and handled appropriately and processed in line with this policy and all related procedures.

Perrigo Personnel must:

- Keep all Personal Data secure by taking sensible precautions and following the guidelines below regarding storage;
- Not disclose Personal Data to unauthorized individuals, either within the company or externally;

- Give access to Personal Data only to Perrigo Personnel who have a business requirement to access that personal data and have been trained to appropriately protect it; and
- Follow formal procedures and approved processes when granting access to Personal Data.

4. DATA COLLECTION

Perrigo attempts to limit its collection of Personal Data only to the purpose(s) for which it is intended. Where required by law, Perrigo will provide notice or obtain written acknowledgement/consent from an individual for the collection, use, transfer, storage and disclosure of personal data.

Additionally, Perrigo will provide information on how to withdraw that consent and stop the collection and/or processing of this Personal Data.

Personal Data that is collected for one business purpose may not be used for other business purposes without obtaining additional written consent.

Certain types of Personal Data are considered particularly sensitive such as:

- Any information related to children
- Criminal convictions and allegations of crimes
- Genetic and biometric data
- A government-issued identification number (National ID number, Social Security number, etc.)
- Health data
- Political opinions
- Race or ethnic origin
- Religious and philosophical beliefs
- Sex life and sexual orientation
- Trade union membership

Perrigo provides appropriate privacy protection and confidentiality for this type of data and will only collect and use this sensitive information when there is a legal basis or when Perrigo has obtained the individual's written consent.

5. DATA USE

Perrigo will only collect or process Personal Data based on explicit written consent, contract, legal obligation, vital interests, public interest, official authority or other legitimate interests.

Explicit written consent must also be obtained from the individual to whom the Personal Data belongs if it is to be used by Perrigo for any other purpose(s) (e.g. direct marketing etc.) than originally intended.

Perrigo Personnel have an obligation to protect Personal Data against the risk of loss, corruption and theft. For example, personnel must keep their computers secure, e.g. lock screen when leaving the computer unattended.

6. DATA STORAGE

Personal Data stored electronically (e.g. in a spreadsheet, on a hard drive, in a database), must be protected from unauthorized access, accidental deletion and malicious hacking attempts.

Responsibilities of Perrigo Personnel working with Personal Data include:

- Personal Data must be protected by strong passwords that are changed regularly (in line with the Corporate Information and Security Policy) and never shared between Perrigo personnel or external parties;
- If Personal Data is stored on removable media (like a CD or USB stick), these must be encrypted and locked away securely when not in use.

Personal Data must only be stored on Perrigo-approved drivers, servers, devices, and cloud computing services.

If Personal Data is stored on paper, or electronically stored Personal Data has been printed, it must be kept in a secure place where unauthorized personnel cannot access it, e.g. in a locked drawer or filing cabinet. Perrigo Personnel must not leave any printed material containing Personal Data unattended, e.g. use secured printing options where available.

All records, whether electronic or paper, should be disposed of securely according to the Global Records and Information Management Policy.

7. DATA SUBJECT ACCESS REQUEST

Local law may allow individuals who have Personal Data held by Perrigo to exercise their Data Subject rights. This is known as a **Data Subject Access Request**.

These individuals may:

- Ask what information Perrigo holds about them, why and for what purpose;
- Ask to access that information;
- Request their Personal Data to be updated;
- Request to be informed on how Perrigo meets its data protection obligations.

In order to comply with strict regulatory timelines, all Perrigo personnel must notify the DPO **as soon as possible but no later than 2 business days** by emailing globalprivacyoffice@perrigo.com.

Data Protection Officer
c/o Global Privacy Office
globalprivacyoffice@perrigo.com,
Phone: +353 1 709 4343 (Ireland)

Where allowed under local law, a small fee may be charged for each Data Subject Access Request. The Global Privacy Office will aim to provide the relevant Personal Data information within a reasonable period of time in line with applicable local laws.

Individuals can make an online Data Subject Access Request:
https://perrigo.ethicspointvp.com/custom/perrigo/forms/data/form_data.asp?lang=en

The identity of anyone making a Data Subject Access Request will be verified before initiating the data collection process.

8. RESOURCES

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

- Privacy Definitions & Terms
- Records and Information Management Policy
- Corporate Information and Security Policy

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

Version No:	Version 1.0
Department:	Global Privacy Office
Review Date:	May 2, 2018
Effective Date:	May 2, 2018
Approved by:	CCVC