This policy sets our global privacy principles and the minimum standards to which we shall adhere. Nevertheless, local laws and industry codes we agree to follow and written agreements with data vendors are examples of situations that may require higher standards than those set out in this policy.
Purpose

Teva’s Global Data Privacy Policy is intended to support compliance with laws and regulations applicable to Teva’s Processing of Personal Data throughout the world. This policy is based on internationally-accepted privacy principles as embodied by the Organization of Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the U.S. Federal Trade Commission’s (FTC) Fair Information Practices, Article 8 of the European Convention on Human Rights and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. It establishes mandatory standards that must be followed and also sets out additional considerations that Teva should take into account when Processing Personal Data.

Teva is committed to complying with the applicable data privacy requirements in the countries in which it and its subsidiaries operate.

While this policy sets out our global approach, it does not specifically address every local privacy or data protection law across the world. To the extent that local privacy laws or our written agreements with third party representatives (third parties) require higher standards than those generally described in this policy, Teva will comply with those higher standards. You should consult your Regional Privacy Officer for more detailed guidance on the specific requirements.
Teva is committed to doing business the right way, the ethical way...

*Our Way.*
Application

This policy applies to all Teva business functions and departments in all locations worldwide (“Teva”). Teva must also ensure that third parties conduct their activities on behalf of Teva in accordance with this policy.

More specifically, this policy applies to:

- all Teva employees and Contingent Workers who receive Personal Data from Teva; have access to Personal Data Processed by or on behalf of Teva; or manage or otherwise have responsibility for any processes that involve Personal Data;
- all activities conducted by or on behalf of Teva that involve Personal Data; and
- Personal Data in all formats (i.e., electronic, hard copy, verbal, etc.).

Responsibility

Employees and Contingent Workers are responsible for knowing and complying with all aspects of this policy and reporting any suspected violation of this policy to their manager, Human Resources, Compliance & Ethics, Legal, or the Teva Integrity Hotline.

Our Commitment

Teva is committed to doing business the right way. Teva’s Code of Conduct, our compliance and ethics principles, and local compliance and ethics policies describe our vision for doing business in a legal and ethical manner. This Global Data Privacy Policy is a guide for helping Teva employees and Contingent Workers put our values into practice when Teva is involved in the Processing of Personal Data.

To support Teva’s commitment to data privacy, Teva’s Global Compliance & Ethics organization has established the Global Data Privacy Team. The Global Data Privacy Team is coordinated by the Global Privacy Officer, who reports to Teva’s Global Chief Compliance & Ethics Officer.
Our Privacy Principles and Standards

The principle that Teva will process Personal Data fairly and lawfully forms the foundation of this policy. To support this, Teva has adopted the following standards to govern its Processing of Personal Data:

Notice and Consent

At or before the time of collection, Teva will give notice to Data Subjects about Teva's collection of Personal Data and/or get Consent from the Data Subject, if required by and in accordance with local law or Company policies.

The notice will explain: the purposes for collection and Processing, how Teva will use and share Personal Data, with whom Teva may share the Personal Data, what rights Data Subjects have, and any other information as required by local law.

- We will only collect, use, and disclose Personal Data for purposes consistent with the purposes specified in the notice and/or Consent unless Teva otherwise has the lawful authority to process the Personal Data.
- If Teva wants to use or disclose Personal Data for purposes not consistent with the purposes specified at or before the time of collection, Teva will give additional notice to Data Subjects and/or get additional Consent, if required by and in accordance with local law or Company policy.

Individual Rights

Teva will recognize and honor Data Subject’s rights, such as to request access, correction, restriction, or deletion, and to revoke consent (or opt-out) and to object to Teva’s Processing of Personal Data. The business owner will respond to Data Subjects’ requests in accordance with local law.

Security

Teva will implement and maintain administrative, technical, and physical safeguards in accordance with our Global Corporate Security Policy and Standards, Global IT Security Policy and Standards, and applicable local law, to reduce the risks of loss, unauthorized...
access, destruction, use, modification, and disclosure of Personal Data.

Data Quality

Teva will only collect Personal Data that is necessary for the business purpose and take reasonable measures to ensure that the Personal Data is accurate and current.

- Examples of reasonable measures Teva can take to ensure that Personal Data is accurate and current are: allowing individuals to update information in their profiles (such as their email address, postal address, and/or phone number), and providing a toll-free phone number or an on-line option where individuals can request changes to Personal Data about themselves.

Data Retention

Teva will not keep Personal Data in a form that permits identification of the Data Subject for longer than necessary to accomplish the permitted and/or specified purposes.

- We will maintain Personal Data in accordance with local law and Teva’s record retention policies.
- This requirement does not supersede any other Company requirements, such as legal holds or “do not destroy” alerts. The business owner must consult with Teva Legal or Records Management for further guidance.

Privacy-by-Design

Teva will design and embed privacy controls that are consistent with this policy and applicable law into activities, processes, technologies, and relationships with third parties that process Teva’s Personal Data.
Privacy by Design is an approach that is characterized by proactive rather than reactive measures. It is important to involve the Global Data Privacy Team in the early stages of any initiative involving the processing of Personal Data.
Additional Considerations

Sensitive Data
Local, national, and regional law may impose additional requirements or restrictions around the collection and use of Sensitive Data, notice and Consent, and additional levels of security to protect Sensitive Data. Teva will comply with any relevant laws regarding Sensitive Data.

Direct Marketing
Teva will comply with any relevant laws, including those which require us to obtain Consent, provide opt-outs, or include specific wording in our notices or communications, when sending marketing communications to individuals, including healthcare professionals and business contacts.

Local law may impose additional requirements or restrictions for certain communication channels such as text message, electronic mail, fax, or robocalls.

Third Parties
Teva will ensure that third parties comply with applicable Company policies, written agreements, and data protection laws when Processing Personal Data on Teva's behalf.

- Teva business functions are encouraged to perform due diligence during the third party selection process and consider whether third parties have adequate privacy controls, including sufficient security measures, to protect Personal Data.
- Teva will enter into written agreements with third parties Processing Personal Data on our behalf, requiring them to comply with applicable Company policies and data protection laws.

Teva will only permit Personal Data to be transferred to third parties if reasonable and appropriate steps have been taken to maintain the required level of data protection under the written agreement, Company policies, and local law.

Teva will only permit third parties to process Personal Data on our behalf for reasons consistent with the purposes for which the data were originally collected or other purposes authorized by applicable law.
Transfers

Teva will not transfer Personal Data out of a country or territory that restricts such transfer (e.g., through data residency, data blocking, or localization requirements) unless the transfer is made to a country or territory that is recognized as having an adequate level of protection or is made in compliance with a mechanism recognized by local law (such as Privacy Shield or Data Transfer Agreements).

Notification to Data Protection Authorities

Teva will notify or register with data protection authorities and obtain the necessary approvals, in accordance with local law.

Breach and Incident Response

For any incident that compromises the privacy or security of Personal Data, Teva’s Global Data Privacy Team should be included in determining how to address such incident, including any incident response team convened in accordance with Teva’s Incident Response Standard. Teva will provide notifications to affected individuals, governmental agencies, law enforcement, and/or others, and take appropriate action in response to the incident, as required by law and/or as determined by the business with input from the Global Data Privacy Team and Teva legal. For more information, please reference the Global Privacy Incident and Breach Reporting Policy.

Training

All employees and Contingent Workers will complete training on this policy. Additional privacy training at a local, regional, or global level may be provided as determined by the business or Global Data Privacy Team.

Contact the Data Privacy Team for any Questions

EU Privacy: EUPrivacy@tevaeu.com

NA Privacy: USPrivacy@tevapharm.com

IM Privacy: IL_Privacy.Tevail@teva.co.il
General Overview: This policy establishes standards for Teva’s Processing of Personal Data throughout the world.

Domain: Compliance & Ethics

Effective Date: June 1, 2020

Version Date: May 27, 2020

Owner: Vice President, Compliance & Ethics Global Privacy Officer & Third Party Due Diligence

Approved by: Senior Vice President, Global Chief Compliance & Ethics Officer

Signature: ____________________________

Name: Tali Guy

Signature: ____________________________

Name: Lori Queisser

This Policy is subject to all Applicable Laws and Codes. In the event of any doubt or if questions should arise, the advice of Compliance & Ethics should be sought.
Appendix:

Glossary of Terms

The following definitions are used in this Policy:

Consent: A legally binding expression of will, given voluntarily, in which the Data Subject signifies his/her agreement to the Processing of Personal Data

Contingent Worker: Non-employee person who is self-employed or employed by a temporary staffing agency or professional service provider that assigns him/her to Teva to perform services on Teva's behalf

Data Privacy Lead: Member of the Global Data Privacy team responsible for a specific location (such as International Markets, Europe, LATAM, or North America)

Data Subject: The person Personal Data is about

Personal Data: Information in any format that can be used, directly or indirectly, alone or in combination with any other information, to identify a person

Process: Any action that can be performed on Personal Data. By way of example, Processing includes collection, storage, revision, deletion, correction, review, analysis, organization, consultation, combination, and transmission

Sensitive Data: A special category of Personal Data defined by local, national, and/or regional law that often includes information about, for example, someone’s health or sex life, race or ethnic origin, religious or political beliefs or affiliations, labor or trade union membership, national identification numbers, bank account or credit card numbers, and criminal offenses