Table of Contents

1. Purpose

Takeda Pharmaceutical Company Limited and all of its affiliates (collectively, “Takeda” or "We") are committed to compliance with applicable laws and regulations in each country in which they operate.

In the course of conducting its business globally, Takeda collects, creates, uses, accesses and otherwise Processes Personal Data. In some instances, Personal Data may include Sensitive Personal Data.

We value the trust that individuals place in us when they provide their Personal Data to Takeda. To promote and preserve that trust, Takeda has established this Global Privacy Policy (“Policy”).

2. Scope

This Policy applies equally to directors, officers, employees, consultants, contractors, and temporary personnel resources of Takeda (hereinafter referred to as “Personnel” or “you”) who have access to Personal Data or have decision-making authority impacting the Processing of Personal Data. This Policy reflects Takeda’s commitment to privacy and data protection practices, establishes standards and controls to protect Personal Data, and applies to all Personal Data in any format, including verbal, written or electronic.

Personnel, regardless of their position or role, must handle and safeguard Personal Data in accordance with this Policy. This includes the responsibility to prevent unauthorized access to, disclosures or loss of, Personal Data and to appropriately protect the security and confidentiality of, Personal Data. Personnel are required to Process Personal Data in accordance with this Policy, and to maintain the confidentiality of Personal Data, both during and after their employment with Takeda.

Takeda also works with third parties, including fulfilment partners, payroll service providers, marketing or other specialist agencies and organizations. These third parties are often referred to as “Processors” since they Process Personal Data on behalf of Takeda, also referred to as “Controller”. Takeda shall bind third party Processors by contract to standards for the Processing and safeguarding of Personal Data that meet or exceed applicable data protection requirements.

This Policy provides a uniform standard for Personnel worldwide. However, Takeda recognizes that certain laws may impose requirements that are stricter than those described in this Policy. Where applicable law, regulation or contractual requirements provide a greater level of protection of Personal Data than that established by this Policy, or any implementation standards, or where such law, regulation or contractual requirements directly conflict with this Policy or any implementation standards, Takeda shall follow the applicable law, regulation or contractual requirements. Where applicable law, regulation or contract provides a lower level of protection or treatment of Personal Data than that established by this Policy, then the requirements of this Policy shall apply.

3. Key Principles

Takeda is committed to the protection of Personal Data. In support of this commitment, Takeda has adopted a set of Privacy Principles to guide us regarding the Processing and protection of Personal Data in the course of

our work. The related Requirements (see 4. below) establish controls needed to support compliance with this Policy.

The below Takeda Privacy Principles are based on internationally recognized standards relating to the treatment of Personal Data and are consistent with Takeda's commitment to conduct business in a highly ethical and legally compliant manner. The Privacy Principles, together with the entirety of this Policy, as well as global, regional and/or local policies and/or Standard Operating Procedures (SOPs), express and support Takeda's commitment to patients, healthcare professionals, our employees and all other individuals with whom we interact in the course of our business.

Takeda's Privacy Principles are as follows:

1. **Lawfulness, Fairness and Transparency -** We Process Personal Data lawfully, fairly and in a transparent manner in relation to the individual who is the subject of Personal Data.
2. **Purpose Limitation** - We collect Personal Data for specified, explicit and legitimate purposes. We do not further Process Personal Data in a manner that is incompatible with those purposes.
3. **Data Minimization** - We collect and Process Personal Data that are adequate, relevant and limited to only what is necessary in relation to the purposes for which they are Processed.
4. **Accuracy** - Personal Data are accurate and, where necessary, kept up to date. We take reasonable steps to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are Processed, are erased or rectified without delay.
5. **Storage Limitation** - We maintain Personal Data for no longer than is necessary for the purposes for which the Personal Data are collected and further Processed. We may retain Personal Data for longer periods for purposes of archiving in the public interest, scientific or historical research or statistical purposes, subject to implementation of appropriate technical and organisational measures to safeguard that data.
6. **Security (Confidentiality, Integrity and Availability)** - We implement appropriate technical and organizational security measures to protect Personal Data against unauthorized or unlawful Processing and against accidental loss, destruction or damage.
7. **Individuals' Rights** - We respect the rights of individuals about whom we Process Personal Data to access that Data (in accordance with applicable laws) and to request correction or erasure of inaccurate Personal Data, or to object to its Processing in specified circumstances.
8. **Accountability** - We are responsible for, and are able to demonstrate compliance with, these Privacy Principles.

4. Requirements, Guidelines and Procedures

In support of our Privacy Principles, and as may be further detailed in SOPs, Takeda requires the following:

Fairness and Transparency

1. Where appropriate or legally required, we provide individuals with or make publicly available, Privacy Notice(s), presented in a clear and easy to understand manner, about how and why Takeda collects, stores,

discloses and otherwise Processes Personal Data. Privacy Notices will be drafted to meet applicable requirements, but generally will include the following (unless it is evident from the context, or the individual already has the information):

a) the types of Personal Data collected;

b) the purposes for which Personal Data are collected and Processed;

c) whether Personal Data will be disclosed to third parties, including the specific recipients or categories of recipients;

d) choices offered to individuals, including the right to request access to, and rectification or erasure of Personal Data; and

e) how to contact Takeda with privacy inquiries or complaints.

2. We obtain individuals' Consent for the collection, use and disclosure of Personal Data, where required by applicable laws. If such Consent is withdrawn, subject to applicable laws, we shall cease Processing unless required, or otherwise permitted, by law to continue Processing, for example, where Personal Data must be maintained for audit purposes; or in order to meet Good Clinical Practice (GCP) requirements.

Lawfulness

1. Takeda and their Personnel are responsible for Processing Personal Data consistent with the requirements of applicable laws. In particular, we shall observe any additional requirements imposed by applicable laws for Processing Sensitive Personal Data.

2. Personal Data can be shared within Takeda in accordance with Takeda's Global Data Transfer Agreement (Global DTA) and applicable laws and regulations.

   Under the terms of the Global DTA, a disclosure and/or international transfer of Personal Data between Takeda is generally permitted provided that there is a clear legal basis, a legitimate business need to Process and transfer the Personal Data in the course of our work, and the Personal Data is adequately protected by the recipient Takeda Company.

3. We only disclose Personal Data to third parties where legally required or otherwise lawfully permitted (for example pursuant to contract). This includes disclosures made in line with Privacy Notices and, where required under applicable laws, with the Consent of the individual to whom the information pertains.

   a) A disclosure of Personal Data to a third party is permitted when such third party is Processing Personal Data either on behalf of Takeda as Processor, or jointly with Takeda as a Controller, and such Processing is reasonably necessary to meet Takeda's legitimate business needs or to comply with a legal requirement.

   b) In limited instances, and subject to individuals' Consent, or where otherwise lawfully permitted, Personal Data may be transferred to a third party that will Process the data as a sole Controller (e.g., a pension benefit provider).

   c) Where applicable, we adhere to local laws, policies and procedures that impose additional requirements with regard to the qualification and use of third parties to Process Personal Data on behalf of, or jointly with, Takeda.

   d) International transfers of Personal Data to any third party are subject to applicable laws which vary from country to country. In particular, transfers of Personal Data from the European Economic Area ("EEA"),

Switzerland and Japan to any third party located outside the EEA, Switzerland and Japan are subject to country-specific and regional regulations.

Purpose Limitation

We collect and Process Personal Data that is relevant and not excessive for the legitimate business purposes specified in the Privacy Notice.

Data Minimization

Personnel are expected to thoughtfully consider Personal Data collection practices and limit collection, access and use to only that Personal Data that is relevant and reasonably necessary to accomplish our intended purposes.

Accuracy

We use reasonable efforts to keep Personal Data accurate and up to date. Such efforts are further supported by the rights of individuals to have inaccurate information updated or otherwise rectified.

Security (Confidentiality, Integrity and Availability)

1) We use reasonable efforts to protect Personal Data against accidental loss, destruction, unauthorized access, use, modification or disclosure.
   a) Takeda has implemented a formal information security program consisting of administrative, technical and physical safeguards, policies and controls establishing specific requirements for the security of all Takeda's information assets, including all Personal Data. The program is reasonably designed to protect Personal Data from:
      i) anticipated threats or hazards, and
      ii) unauthorized access or use.
   b) Takeda strives to provide security that is proportionate to the sensitivity of the Personal Data being protected, with the most significant effort being focused on protecting Personal Data from any compromise that could result in substantial harm or inconvenience to individuals about whom the Personal Data pertains.
   c) Only personnel who are authorized to access Personal Data in order to perform their job duties are to be granted access to such Data.

Storage Limitation

We are committed to retaining Personal Data for no longer than necessary for the purposes for which such Data are collected and further Processed.

Individuals' Rights

We provide individuals with reasonable access to Personal Data about them and with the opportunity, where appropriate, to correct, amend, or delete inaccurate Personal Data. We also respect the rights of individuals to object to Processing of Personal Data or restrict Processing in circumstances provided by applicable law.

Accountability

We are accountable for Takeda's data protection and privacy practices and the Processing of Personal Data. We maintain a team of data protection and privacy professionals and through our policies, procedures, training and communications programs, build responsible data protection and privacy practices into our culture.

Where deemed necessary by Privacy Office, or as required by applicable law, initiatives or activities that involve or impact the Processing of Personal Data will undergo appropriate risk assessments (Privacy Impact Assessments) to evaluate, report, mitigate and monitor risks associated with the proposed purposes and means of Processing.

The classification (nature and type) of Personal Data (see Glossary of terms) will inform Takeda's approach to assessment of data protection and privacy risk under this Policy.

Privacy Incidents

Takeda's reputation is at stake whenever we are entrusted with Personal Data and we may be held accountable if a Privacy Incident occurs, irrespective of whether it was due to the acts of Takeda, a third party Processor, or other events.

If Personnel suspect or become aware that a Privacy Incident has or may have occurred, that Personnel must immediately report such incident to privacyoffice@takeda.com or cybersecurity@takeda.com pursuant to applicable SOPs addressing Privacy Incidents.

5. Compliance: Governance, Accountability, Monitoring and Control

Takeda has established a Privacy Office function in Legal responsible for:

- Establishing a framework of data protection and privacy policies, processes and procedures to further implement this Policy;
- Interpretation and guidance on application of this Policy and applicable data protection and privacy laws;
- Reporting and escalation of known and emerging data protection and privacy risks and incidents to Senior Leadership (TET/BoD).

Takeda Business Function and Region/LOC Leadership (collectively "Business Leaders") are responsible for:

- Ensuring compliance of their respective organizations with this Policy and applicable laws; and
- Establishing and maintaining adequate functional and/or local resources to ensure compliance with this Policy and all applicable laws, pursuant to guidance, procedures and/or recommendations issued by the Privacy Office.

If Personnel fail to comply with any applicable Takeda policy relating to Personal Data and compliance with the applicable laws, they will be subject to appropriate disciplinary action, up to and including dismissal.

Compliance with this Policy is subject to auditing and monitoring. Group Internal Audit may be asked by the Chief Privacy Officer, or designate in the Privacy Office, to conduct an internal audit of a Business Function's, or LOC's, adherence to this Policy and any related guidance, policy or procedure.

6. Glossary of terms

Term	Definition
Business Leader	Takeda Management with primary budgetary ownership and responsibility for the relevant Processing of Personal Data in a Business Function, Region or LOC.
Consent	Any freely given, specific, informed and unambiguous indication of an individual's wishes by which that individual signifies their agreement to Personal Data relating to them being Processed.
Controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Encrypted Personal Data	Personal Data that has been the subject of encryption. Encryption is a technical security measure that can be implemented to mitigate risk related to unauthorized access to Personal Data. Encryption of Personal Data may provide exceptions to data protection obligations in certain instances (e.g., theft, loss or unauthorized access to Encrypted Personal Data may not trigger obligations to notify authorities or individuals as long as the integrity of the encryption key is maintained).
Personal Data	Any information which relates to an individual or which can be used to identify, locate or contact an individual, either on its own or when combined with other information under Takeda's control. Depending on the applicable laws, Personal Data (sometimes called 'personally identifiable information' or 'PII' in the U.S.) may include, for example, an individual's name, email address, postal address, geolocation information, IP address, telephone number, performance evaluations in any media or format, including paper files and electronic records. Personal Data includes Encrypted Personal Data, Pseudonymized Data and Sensitive Personal Data.
Privacy Impact Assessment (PIA)	A process used to identify and document risks and recommended mitigations associated with the Processing of Personal Data.
Privacy Incident	Any event that might compromise the privacy, security or confidentiality of Personal Data. This includes, for example, unauthorized access to a Personal Data system, as well as unauthorized access, use, disclosure, or any loss or destruction of Personal Data.
Privacy Notice (or Notice)	A description of Takeda's practices provided to an individual with respect to Takeda's Processing of Personal Data.
Process or Processing	Any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, receipt, viewing, accessing, storing, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Processor	A natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.
Pseudonymized Data	Personal Data that has been Processed in such a way that Personal Data can no longer be attributed to a specific individual without the use of additional information, which must be kept separately and subject to technical and organizational security measures, to ensure that the Personal Data are not attributed to an identified or identifiable individual. An example of Pseudonymized Data is key-coded clinical trial data held by Takeda as Sponsor.
Sensitive Personal Data	A subset of Personal Data that, due to its nature, has been classified by law or policy as deserving additional privacy and security protections. Depending on the applicable laws, Sensitive Personal Data may include, for example: • government-issued identification numbers, • individual financial account numbers and details, • individual health information and medical records, including genetic and biometric data. In some countries, including EU member states, Sensitive Personal Data (also known as “special category data”) includes: • racial or ethnic origin, • political opinions, • religious or philosophical beliefs, • trade-union membership, • sexual life and orientation, and • criminal records or allegations.