GLOBAL POLICY FRAMEWORK (GPF)

ASTRAZENECA STANDARD – DATA PRIVACY (ENGLISH)

KEY PRINCIPLES

- **We respect and protect privacy by collecting, using, retaining, sharing, and/or disclosing Personal Data fairly, transparently and securely.**
- **We respect data subject rights and respond to queries and requests made by individuals about their Personal Data.**
- **We hold third parties with whom we work to the same expectations as described in this AZ Standard.**

1. WHY IT MATTERS AND TO WHOM

This Standard procedural document is managed in the **Global Policy Framework (GPF)** and sets out the requirements for processing Personal Data at AstraZeneca (AZ), aligned to AZ Code of Ethics.

This Standard applies to all entities within the AstraZeneca group of companies. Hence, unless the context otherwise requires, any reference to "AZ" herein, shall be deemed to be a reference to entities within the AstraZeneca group of companies.

At AstraZeneca the requirements described in this document apply to:

- AstraZeneca employees and temporary staff who have access to Personal Data as part of their business activities
- AstraZeneca managers who are accountable for ensuring that appropriate privacy controls are in place within their business function, and
- AstraZeneca programme/project sponsors who are responsible for ensuring appropriate privacy requirements are assessed at an early stage and incorporated into processes, systems, and services wherever necessary.

Third parties who perform services for or on behalf of AstraZeneca are expected to embrace standards of conduct consistent with the principles of this Standard.

The principles outlined in this Standard matter because at AZ we value the Personal Data entrusted to us, and we are committed to collecting, using, retaining, and disclosing Personal Data in a fair, transparent and secure way, to meet company and legal requirements, for processing Personal Data.

2. WHAT YOU NEED TO KNOW AND WHY

Personal Data is any information about an identified or identifiable natural person including, but not limited to, our employees, patients, shareholders, contractors, or the staff of our suppliers, visitors to our buildings, or website users). In some jurisdictions, the concept of Personal Data is interpreted broadly and expansively to include information that is not obviously an identifier of an individual, for example, IP addresses and unique device IDs.

This AstraZeneca Standard aligns with and, in some cases, exceeds the requirements of applicable laws and regulations. Local laws and regulations that apply to the activities described in this Standard may be more restrictive than this Standard. Where that is the case, the more restrictive rules must be followed.

AstraZeneca Standard - Table of Contents (ToC)

3. REQUIREMENTS

3.1 Privacy Risks

To ensure that AstraZeneca is meeting the requirements below, we will consider the privacy risks before we collect, use, retain, or disclose Personal Data, such as in a new system or as part of a project.

Any new project or initiative, including new systems, infrastructure, websites, and mobile apps, which will collect and/or host Personal Data and will be assessed for the privacy risks associated with the project, or initiative, prior to implementation.

3.2 Data Collection, Transparency and Consent

We will only collect Personal Data by fair, lawful, and transparent means, and we will be open with individuals about how we use their Personal Data, with whom we share it, and where it may be sent.

We must ensure that individuals are provided with a privacy notice concerning the processing of their Personal Data. Privacy notices, as a minimum, must include the information listed below, in addition to any other information, required by applicable local law:

- The identity of the AstraZeneca affiliate collecting the information;
- The use(s) to be made of the Personal Data;
- Whether the information will be shared with or disclosed to third parties or other AstraZeneca affiliates;
- Whether the information will be transferred from its country of origin; and
- Where legally required, how individuals can exercise their rights of access, correction, or deletion of their Personal Data. Under certain circumstances, individuals may have other possible rights, such as the right to object to further processing and the right to data portability.

When required by law, AstraZeneca will obtain the consent of individuals to collect, use, retain, and disclose their Personal Data. Many countries require consent before collecting and/or using any Sensitive Personal Data. Sensitive Personal Data includes information about a person's:

- Race or ethnic origin;
- Political opinions;
- Religious or other similar beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Commission (or alleged commission) of any offence, or proceedings relating to an offence
- Genetic information; or
- Biometric Data.

There are additional categories of Personal Data, which are generally considered sensitive, including official identification information, such as passport or Social Security numbers, as well as financial information other than basic transactional data such as bank accounts to support making contractual payments or managing employee expenses.

Financial information that is used for more than making payments must be treated as Sensitive Personal Data. This includes information relating to an individual's assets or debts, their spending habits or patterns or credit score.

Where we wish to use Personal Data for a purpose for which we had not previously notified the individual, we must notify the individual of the new purpose and, in some cases, gain their consent.

In some countries and where legally required, we will notify or gain pre-approval from the local privacy regulator, prior to collecting and using any Personal Data.

3.3 Data Minimisation

We will only collect and use the minimum amount of Personal Data to support the specific business activities that we notified to the individual and will not make Personal Data available to anyone, including internal staff, who are not authorized to access the Personal Data, or do not have a legitimate business need to access the Personal Data.

3.4 Legitimacy

We will only use Personal Data where we have a legitimate business need or a legal obligation. We will only process Personal Data in the way described in the applicable privacy notice and in accordance with any consent we have obtained from the individual.

3.5 Accuracy

We will keep Personal Data accurate and up-to date. Personal Data must be maintained in an accurate and up-to-date form during any processing, such as, transfer, storage, and retrieval, to fulfil the purposes for which it was collected.

3.6 Security

We will protect any Personal Data collected, used, retained, and disclosed to support our business activities by following the relevant usage, technical, and organisational policies, standards, and processes.

Safeguards must be put in place to protect Personal Data against a variety of threats, including:

- Loss or theft;
- Unauthorized access, use, or disclosure;
- Improper copying, modification, or tampering;
- Improper retention or destruction; and
- Loss of integrity, availability, and access to Personal Data.

Employees must take appropriate steps to prevent the misuse or loss of Personal Data, to prevent unauthorised access to it, and to report any known or suspected instance of misuse, loss, or unauthorised access to their line manager, their local Privacy Representative and through AZ’s Information Incident reporting process.

3.7 Data Subject Rights and Requests

We will respond to queries or requests made by individuals about their Personal Data, and, where required by law, we will provide individuals with the ability to access, correct, and delete their Personal Data. We will provide the ability for individuals to object to further processing and to request data portability, where permitted by laws in their respective country.

If AstraZeneca does not agree that the information is incorrect or must be deleted, we will record that the individual considers the information to be incorrect, or wishes to have it deleted. In such situations, the individual may have a right to object to any further processing.

3.8 Retention

We will only keep Personal Data necessary to support a specific business activity or legal or regulatory requirement. Personal Data must be:

- Kept only for as long as it is necessary to meet or support a business activity or comply with a legal or regulatory requirement;
- Kept in accordance with **AZ's Global Retention and Disposal (GRAD)** schedule.
- Securely disposed of or destroyed at the end of the specified retention period.

3.9 International Transfers

We will ensure that any transfer of Personal Data outside the jurisdiction where it was collected, including transfers within the AstraZeneca group of companies, complies with applicable laws. Where required by law, we will obtain individuals' consent for transferring their Personal Data outside their country of residence and, in some cases, notify or gain approval from the relevant privacy regulator, prior to the transfer taking place.

3.10 Third Parties

We must ensure that access to and transfers of Personal Data to third parties are carried out for legally justifiable reasons and with suitable privacy safeguards, which may include contractual protections.

We must ensure that any third parties or suppliers who will have access to AstraZeneca Personal Data:

- Go through a due diligence process which assesses their privacy and information risks; and
- Enter into a written contract with AstraZeneca that contains appropriate privacy clauses.

3.11 Marketing and Promotional Activities

We will abide by any relevant laws that require the consent of consumers when sending marketing communications and carrying out promotional activities.

In some markets, AstraZeneca sends marketing communications directly to patients/the public via email, direct mail, telephone, and SMS text messaging. In most markets, we also send promotional content to Healthcare Professionals, via some or all of these channels. Where legally required, we must ensure that such communications are only sent with the individual's prior consent (or equivalent opt-in/opt-out).

An opt-out mechanism will be included, or be readily available to the individual in each communication, for example, an unsubscribe function in an email.

Where an individual unsubscribes from receiving communications, we must honour their request promptly and ensure we maintain a list of individuals who have opted-out from receiving communications from AstraZeneca.