

ASTRAZENECA GLOBAL POLICY

DATA PROTECTION AND PRIVACY

THIS POLICY SETS OUT THE REQUIREMENTS FOR ENSURING THAT WE MEET OUR COMMITMENT TO PROTECTING PERSONAL INFORMATION COLLECTED OR HELD DURING THE COURSE OF OUR BUSINESS ACTIVITIES BY ENSURING HIGH STANDARDS OF DATA PROTECTION WORLDWIDE.

PERSONAL INFORMATION IS INFORMATION THAT CAN BE USED TO IDENTIFY LIVING INDIVIDUALS (WHETHER STAFF, CUSTOMERS, SHAREHOLDERS, CONTRACT/SUPPLIER'S STAFF OR CLINICAL STUDY PARTICIPANTS).

WHO IS THIS POLICY FOR?

All employees who manage personal information as part of their business activity.

Managers who are responsible for ensuring that appropriate controls are in place.

To give effect to this Policy, **all SET areas** are expected to follow any global standards and procedures or, provided they are consistent with this policy, their own local or functional standards and procedures.

KEY POLICY PRINCIPLES

- > We must protect personal information collected, recorded, stored, altered, retrieved, disclosed, shared, combined, backed-up, destroyed or otherwise used ("processed") during the course of our business activities.
- > Each SET/functional area will establish clear responsibilities and accountabilities for the custodianship of the personal information it processes.
- > At least one person per SET/functional area will be appointed and made accountable for the development and implementation of controls, consistent with the objectives of this global policy, appropriate to the personal information that that SET/functional area processes ("Privacy Champion"). The Privacy Champion will be supported in this regard by a representative of the Global Privacy Office.
- > Local or SET/functional specific policies, standards and procedures may reflect more stringent legal and/or regulatory requirements than those set out in this policy. Where this is the case, those more stringent requirements must be met.
- > The efficient use of the personal information that the Company processes demands that SET/functional areas co-operate to ensure the optimum balance between local and/or functional-specific needs and overall corporate benefit. This may lead to the imposition of more rigorous requirements in certain areas in some markets than local laws may otherwise dictate.

DOCUMENTED STANDARDS AND PROCEDURES

Each SET/functional area, supported by a representative of the Global Privacy Office, will develop and implement policies, standards and procedures that describe the behaviours it adopts

to govern the handling of the personal information it processes in accordance with this global policy and local applicable law.

TRANSPARENCY

Privacy Champions must implement procedures within their SET/functional area to ensure that:

- > Where legally required, individuals receive, or have made readily available to them, “collection notices” concerning personal information about them that the Company processes.
- > The Company’s collection notices will provide the identity of the AstraZeneca affiliate collecting the information and describe the uses to which it will be put, including whether it will be shared with and/or disclosed to third parties or affiliates at home or abroad. Where legally required, they will also describe individuals’ rights to access personal information and to delete or correct any inaccurate personal information.
- > The Company only processes personal information in the way described in collection notices and/or any associated privacy statement (eg on-line privacy statement) and in ways, or for purposes, that are inherent from that description or are obvious to the individual.
- > The Company may use personal information for purposes not declared in collection notices, where we have previously de-identified the data.

- > The Company only collects the minimum amount of personal information necessary to satisfy our legitimate business, human resources, scientific, legal and/or regulatory purposes.
- > Where the Company purchases information about individuals from reputable third parties (eg list vendors), the individual is made aware that we are processing personal information about them.

As part of the provision of IS/IT services to our staff, third parties and affiliates, the Company’s systems automatically record personal information about how individuals use such systems (eg Internet access and telephone call logs). Unless legally permissible, this type of information will not be viewed or actively used on a continuous or routine basis. However, where applicable laws permit, this information will be used to facilitate our compliance with legal and/or regulatory obligations and/or to establish, exercise or defend legal rights (and other associated purposes).

SENSITIVE PERSONAL INFORMATION

Privacy Champions must implement policies, standards and/or procedures within their SET/functional area to ensure that, where legally required, we only process personal information that is classified as, or is widely held to be, “sensitive” (eg bank account or passport details, health information, social security or credit card

number), if we have the individual’s consent. Privacy Champions must maintain procedures to record and evidence that such consent has been obtained. The Company’s default information classification for sensitive personal information is “Strictly Confidential”.

PORTABLE MEDIA

Staff must encrypt personal information temporarily stored on portable media (eg USB memory sticks, CDs/DVDs and flash memory cards) and protect it with a strong password. Portable media should only be used to store personal information for short periods of time where there is no more secure method of transmission available and there is a legitimate business need for such transmission. Portable media containing personal information must be exchanged in person or by secure courier; it is not acceptable to send them through any form of postal service, whether internal or external. As soon as possible after the transfer is completed, the personal information must be deleted, if necessary by destroying the media.

Personal information must never be stored on non-Company devices (including home/private PCs), nor should it be placed on portable media in order to facilitate access to the information from a non-Company device. Personal information must never be sent to personal email accounts such as Hotmail.

For more information see [Using WinZip To Protect AZ Information](#).

MARKETING AND PROMOTIONAL ACTIVITIES

In some markets, the Company sends marketing communications directly to consumers 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, Privacy Champions must have policies, standards and/or procedures in place to ensure that such communications are only sent with the individual's prior consent

(or equivalent opt-in). An opt-out mechanism will be included in each communication (eg "unsubscribe functionality" in an email) or will be readily available to the individual. Lists must be maintained of consumers and healthcare professionals who have opted out.

ACCESS, ACCURACY, CORRECTION AND RETENTION

Where legally required, Privacy Champions must implement procedures within their SET/functional area to ensure that the Company provides individuals with access to the personal information that we process about them. Where legally permitted, the Company may charge a fee for granting such access.

Privacy Champions must ensure that their SET/functional area has procedures in place to ensure that the personal information that it processes is:

- > Only shared with third party partners or disclosed to staff or suppliers who have a right, or legitimate need, to see it. Third parties will be obliged, by written contract, to deploy appropriate organisational and technological measures to protect the integrity and confidentiality of the personal information while it is in their hands.

- > Corrected, if individuals contact the Company and so request, and is otherwise kept up to date.
- > Deleted once the purpose for which it was collected has been fulfilled, unless it is kept in order to comply with a legal, regulatory or policy requirement. Deleted information may be restored from back-up media for a time before being permanently put beyond use.

For more information see the applicable global or SET area records management and security policies, such as the Archives and Records Management Policy and the Information security section of the Global Policy: Safeguarding Company Assets and Resources.

PERSONAL INFORMATION SHARING

The Company will share or otherwise disclose personal information in response to legally binding, regulatory, governmental or law enforcement requests, or where it is in its legitimate interest and legally permissible to do so – eg in the event of a sale or merger of a business.

In common with many international organisations, the efficient use of our IS/IT systems involves moving the personal information we process around our network and sharing it with and disclosing it to

our worldwide affiliates and approved third parties. The Company must use appropriate organisational and technological measures to protect the integrity and confidentiality of the personal information as it moves around its network.

TRAINING

Any training run by the Privacy Champion's SET/functional area will include an element of data protection and privacy awareness appropriate to that SET/functional area's processing activities. The awareness materials will be developed in conjunction with a representative of the Global Privacy Office.

RISK

In consultation with a representative of the Global Privacy Office, Privacy Champions will ensure that their SET/functional area's Risk Register accurately reflects any data protection and privacy risks run by their business area, and that appropriate remediation plans are in place to manage/eliminate these risks.

For more information see the Global Policy: Safeguarding Company Assets and Resources.