AstraZeneca

Owner
Ageborg, Katarina

Approvals

Approval Reason	Performer	Date
Management Approval	Martino, Marie	2013/01/23 21:11:25

ASTRAZENECA GLOBAL POLICY
DATA PRIVACY

This Global Policy sets out the requirements for ensuring that we collect, use, retain and disclose personal data in a fair, transparent and secure way.

Personal Data is any information about an identified or identifiable natural person (whether our employees, patients, shareholders, contractors or the staff of our suppliers, visitors to our buildings or website users).

Who is this Policy for?

All Company employees and temporary staff who have access to Personal Data as part of their business activities.

Managers, who are accountable for ensuring that appropriate privacy controls are in place within their business function.

Programme and project sponsors, who are responsible for ensuring that 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 the Company are expected to embrace standards of conduct consistent with the principles of this Policy.

KEY POLICY PRINCIPLES

1. This Policy represents the minimum standards that the Company has set with respect to data privacy. It aligns with (and in some cases exceeds) the requirements of applicable laws and regulations. In some cases local laws and regulations that apply to the activities described in this Policy may be more restrictive than this Policy. Where that is the case, the more restrictive rules must be followed.

2. This policy is aligned to other Global Policies relating to the collection and use of information.

3. AstraZeneca values 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.

    - Data Collection: We must only collect Personal Data by fair, lawful and transparent means. We must be open with individuals about how we use their Personal Data, with whom we share it and where it may be sent.
    - Data Minimisation: We must only collect the minimum amount of Personal Data to support our business activities and we must not make Personal Data available to anyone (including internal staff) who are not authorised, or do not have a business need to know the information.
    - Data Use: We must only use Personal Data where we have a legitimate business need and, where required by law, where we have the individual's consent. We must 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.

- Accuracy: We must endeavour to keep Personal Data accurate and up-to-date.
- Security: We must 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.
- Access and Correction: We must be receptive to queries or requests made by individuals in connection with their Personal Data and where required by law, we must provide individuals with the ability to access, correct and delete their Personal Data.
- Retention: We must only keep Personal Data for as long as necessary to support a specific business activity or legal or regulatory requirement in accordance with the Global Retention and Disposal (GRAD) Schedule.
- International Transfers: We must ensure that any transfer of Personal Data outside the AstraZeneca group of companies provides adequate protection for Personal Data.
- 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 contractual protections. Due diligence activities must check that the third party has appropriate privacy practices in place in advance of any commitment.
- Marketing and Promotional Activities: Where we send marketing communications to consumers we must abide by any relevant law that requires the consent of these consumers.

DATA COLLECTION AND MINIMISATION

4. Personal Data must only be collected by fair and lawful means and in a transparent manner. Only the minimum amount of Personal Data required to support an AstraZeneca business activity should be collected.

5. Where legally required, we must ensure that individuals are provided with a “privacy notice”, concerning the processing of their Personal Data. Privacy notices should provide:
    - The identity of the AstraZeneca Affiliate collecting the information;
    - The uses to be made of the Personal Data;
    - Whether the information will be shared or disclosed to third parties or AstraZeneca Affiliates;
    - Whether the information will be transferred from its country of origin;
    - Where legally required, how individuals can exercise their rights of access, correction or deletion of their Personal Data.
6. In some countries we may have to notify or gain pre-approval from the local privacy regulator prior to collecting and using any Personal Data.

7. Personal Data must not be made available to anyone, including individuals in other business functions within AstraZeneca, who are not authorised to have the information or have no business reason to access it.

DATA USE

8. AstraZeneca must have a legitimate business reason to use Personal Data as part of our business activities.

9. Where required by law, AstraZeneca may need to obtain the consent of individuals in order to collect, use, retain and disclose their Personal Data. In particular, many countries require consent before collecting and/or using any Sensitive Personal Data. Sensitive Personal Data may include 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.

10. There are also a number of additional categories of Personal Data, which are generally considered sensitive, including financial information such as bank account or credit card details, as well as official identification information such as passport or social security numbers.

11. AstraZeneca will only process Personal Data (including Sensitive Personal Data), in the way described in our privacy notices and in accordance with any consent we have obtained from the individual.

12. Where we wish to use Personal Data for a new purpose that has not been notified to the individual we may need to notify the individual of the new purpose, and in some cases, gain their consent.

ACCURACY

13. Personal Data must be maintained in an accurate and up-to-date form during any processing (i.e. transfer, storage and retrieval) to fulfil the purposes for which it is to be used.

SECURITY

14. 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;
    - Loss of integrity.

15. Employees must take appropriate steps to prevent the misuse or loss of Personal Data and to prevent unauthorised access to it, and to report any known or suspected instance of misuse, loss or unauthorised access to their line manager and their local Privacy Representative.

ACCESS AND CORRECTION

16. Where required by law, AstraZeneca must respond to requests from individuals to disclose information relating to the Personal Data that we hold about them. This may include providing access to the individual's Personal Data. Where legally permitted, AstraZeneca may:
    - Charge a fee for granting access;
    - Refuse a request (for example where an individual makes the same request on several occasions in quick succession);
    - Apply any relevant exemptions outlined in law to withhold Personal Data.
17. Individuals may verify and challenge the accuracy and completeness of their Personal Data and have it amended or deleted if appropriate.
18. If AstraZeneca does not agree that the information is incorrect or should be deleted, we will record that the individual considers the information to be incorrect or wishes to have it deleted.

RETENTION

19. 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 the GRAD Schedule;
    - Securely disposed of or destroyed at the end of the specified retention period.

THIRD PARTIES

20. 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 risk;
    - Enter into a written contract with an AstraZeneca Affiliate that contains appropriate privacy clauses.

INTERNATIONAL TRANSFERS

21. We must never carry out international transfers of Personal Data outside AstraZeneca's group companies without ensuring adequate protection for those data. Where required by law we may need to obtain individuals consent for transferring their Personal Data overseas, and in some cases notify or gain pre-approval from the relevant privacy regulator prior to the transfer taking place.

MARKETING AND PROMOTIONAL ACTIVITIES

22. 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 must also be included in each communication (e.g. an unsubscribe function in an email) or will be readily available to the individual.

23. Where an individual un-subscribes 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.

REVISION HISTORY

Section	Paragraph	Reason for Change
Introduction	All	To align it to the Data Privacy section of the Code of Conduct and to ensure it is clear that data privacy obligations go beyond just protecting Personal Data
Who Is this Policy For	All	To align to recent global policy format and to specifically reference important obligations for consultants/contractors, programme/project leads and 3rd parties
Key Policy Principles	All	Aligning of key principles to the data privacy section in the Code of Conduct and to clearly reflect the key principles of data privacy
Documented Standards and Procedures	All	Removal of this section as key aspects are covered in the 'Who Is This Policy For?' section and other functional policies/SOPs.
Transparency, Sensitive Personal Information, Marketing and Promotional Activities, Access, Accuracy, Correction and Retention, Personal Information Sharing	All	Realignment of these sections to clearly reflect the key principles of data privacy.
Portable Media	All	Removal of section as key aspects are covered in separate policies.
Training	All	Removal as these aspects should fit within functional policies or other SOPs.
Risk	All	Removal as these aspects should fit within functional policies or other SOPs.