POLICY PROTECTION OF PERSONAL DATA

OBJECTIVE

The main purpose of this policy is to ensure that Actelion is in full compliance with regulations on the protection of personal data, worldwide.

As a global organization, Actelion collects and processes data in all sectors and exchanges data within the group and with third parties. Increasing economic and scientific cooperation and the mutual provision of data-processing services also entails the exchange of personal data. Actelion must ensure that personal data are carefully processed and used appropriately for the purpose of their collection.

In adopting the present policy on the protection of personal data, Actelion is pursuing three objectives:

- Establishing a uniform standard to be applied by all Actelion companies in processing personal data and to lay down a basis for contractual agreements with third parties
- Providing preventive safeguards against the infringement of personality and privacy rights through the inappropriate processing of personal data
- Providing an adequate level of protection of personal data as required by the laws.

SCOPE AND APPLICABILITY

Based on this policy, Actelion declares that compliance with data protection principles in the processing of personal data (e.g. data on patients, health professionals, customers, suppliers and employees) is a corporate objective.

As a healthcare group, Actelion treats personal medical data (e.g. data collected in connection with clinical trials or registries, etc.) with special care.

Where personal data are processed on Actelion's behalf by third parties, appropriate measures shall be taken to ensure the full compliance of third parties with the principles set forth in this policy.

National legislations providing more comprehensive safeguards of personal data must be followed and implemented in all specific instances where such legislation applies.

This policy applies to all Actelion headquarter and affiliates employees. All Actelion employees involved in processing data are responsible for implementing and enforcing compliance with this policy.

REVIEW AND APPROVAL

Global Security 22-Nov-10 signed [1]
Group Compliance Office 24-Nov-10 signed [2]
Legal 07-Dec-10 signed [2]
CEO 09-Dec-10 signed [3]

1 Author, signs for correctness and completeness
2 (Only if applicable) Reviewer, signs for control of correctness and completeness
3 Approver, signs for the release of this document

CONTENT

DEFINITIONS

For the purpose of this policy the following definitions apply:

Personal Data: any information relating to an identified or identifiable natural or legal person.

Data subject: the natural or legal person to which the personal data refer.

Processing: any operations or set of operations on personal data carried out with or without electronic instruments. Such operations can be including but not limited to: collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, interrogation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Data Processor: any natural or legal person, public administration, body, association or other organization or entity that processes the personal data on the data controller's behalf.

Data Controller: the natural or legal person, public administration, body, association or other organization or entity that is responsible for determining the purposes and methods of the processing of personal data.

ACTELION

HIGHLY SENSITIVE DATA

The following personal data are classed as highly sensitive: Racial or ethnic origin; political or ideological opinions or activities; religious or philosophical beliefs; trade unionrelated views or activities; physical or mental health, intimate sphere or sexual life; social security measures, administrative or criminal proceedings and sanctions.

If processing of such data is not avoidable, these data may only be held in strictly defined situations or where explicit consent of the data subjects has been obtained, and particular measures must be implemented to ensure their maximum protection under any circumstance.

PRINCIPLES

When processing personal data, the following principles apply:

Purpose Specification: Personal data are obtained and processed only where this is strictly necessary for specified, fair and legitimate purposes. The personal data may not be used further for any purpose it was not explicitly obtained for.

Collection Limitation: The collection of personal data must be adequate, lawful, relevant and not excessive. No personal data may be collected which does not serve immediately the purpose as originally defined. The collection of personal data and the purpose of its processing must be evident to the data subject.

Accurate and up to date: All personal data must be kept both accurate and up to date. Errors must be corrected effectively and promptly.

Restricted access: The access to and use of personal data must be limited to those persons within Actelion who require access according to a "need to know" principle.

Not kept any longer than necessary: The personal data are deleted / destroyed when they are no longer needed, accurate or correct.

Personal data may be retained only for as long as is necessary for legal or regulatory reasons or for the relevant legitimate purpose.

Securely kept: the personal data are kept secure at all times; the data controller and the data processor must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of personal data over a network, and against all other unlawful forms of processing.

Compliance with applicable law: All processing must be in compliance with applicable data protection and privacy law.

RIGHTS OF DATA SUBJECTS

Persons from whom personal data have been processed are to be accordingly informed upon request. In particular, they have a right to be informed of the purposes for which the data are being processed, the category of data involved and the identity of the recipients of the data. Where appropriate, data subjects also have a right to require that personal data be corrected, blocked or deleted in a timely fashion.

The aforementioned rights may be restricted only where such restriction is provided for by law.

TRANSMISSION OF PERSONAL DATA TO THIRD PARTIES

A third party is any external person or legal entity, within or outside Actelion, in or outside the country where personal data are processed, who does not process the personal data on behalf of the data controller.

Transfer and disclosure to third parties is subject to the applicable local data protection laws and the following restrictions: necessary or legally required on important public interest grounds / legal claims, necessary for the performance of a contract between the data subject and data controller, necessary for the performance of a contract concluded in the interest of the data subject (between the data controller and a third party), necessary in order to protect the vital interests of the data subject.

Transferring personal data to third parties constitutes a transaction which must be covered by a transaction agreement. To such agreements the Legal Policy applies.

The data controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect with the principles set forth in this policy, and providing appropriate technical and organizational measures to protect personal data, and must ensure compliance with those measures.

If at any time a third party is determined to be unable to ensure the adequate security of personal data, the collaboration must be terminated.

EXPORT OF PERSONAL DATA TO OTHER COUNTRIES

Transfers of personal data are subject to specific safeguards when the recipient is located in a country outside the country where the personal data are originally processed.

Transfer of personal data from one territory to another requires strict legal compliance. Therefore Legal must be consulted prior transferring any data outside the originating territory.

CONSENT

In data protection terminology, consent refers to any freely given, specific and informed indication of the wishes of a data subject, by which he/she agrees to personal data relating to him/her being processed.

Consent is an important term in data protection legislation: "unambiguous consent" is one of the criteria that can legitimize the processing of personal data. If it is relied upon, the data subject must unambiguously have given his/her consent to a specific processing operation.

Apart from having to be given freely, consent must be specific and there may be no doubts as to whether it was given or not.

Before a data subject can be considered to freely have given consent to a specific processing operation, he or she must receive sufficient information to be able to understand the scope and consequences of consent, including the advantages and/or disadvantages of the processing.

Moreover, consent is strictly linked to the processing that the data subject was informed of. It cannot be extended by someone else thereafter, and consent can thus never be given to something the data subject was not aware of.

RESPONSIBILITIES

The affiliates of the Actelion group are responsible for data processing activities within their organization and must ensure compliance with the requirements of this policy and the applicable local data protection laws. The affiliates may call upon the assistance by the Group Compliance Officer of Actelion.

All employees must be regularly informed regarding the requirements under the data protection laws applicable to their activities. Employees must be advised that breaches may constitute a criminal or administrative offence and may lead to claims for damages, fines and other consequences.

Data privacy and data security breaches or suspected cases of such breaches must immediately be notified to the responsible local data protection official and the Group Compliance Officer of Actelion.

REFERENCES

- 235.1 Swiss Federal Act of 19 June 1992 on Data Protection (FADP)
- 235.11 Ordinance of 14 June 1993 to the Swiss Federal Act on Data Protection (OFADP)
- Charter of Fundamental Rights of the European Union (2000/C 364/01) - Article 8 protection of personal data
- Directive 95/46/EC of the European parliament and of the Council
- US Health Information Portability and Accountability Act of 1996 (H.R. 3103; Standards for Privacy of Individually Identifiable Health Information, Final Rule- 45 CFR parts 160 and 164)
- California Database Breach Act (SB 1386, 2002)

Policy: Protection of Personal Data
Version No: 01 Status: Effective
Document Date: 15-Nov-10
Effective Date: 14-Dec-10

Actelion Pharmaceuticals Ltd is a global biopharmaceutical company headquartered in Allschwil/Basel, Switzerland. Actelion concentrates on discovering, developing and marketing innovative drugs for high unmet medical needs. The company is quoted on the SIX Swiss Exchange (tickersymbol: ATLN).

Actelion Pharmaceuticals Ltd Gewerbestrasse 16 / CH-4123 Allschwil Switzerland / investor.relations@actelion.com / Phone +41 61 565 62 62 Fax +41 61 565 65 07 / www.actelion.com