Privacy principles observed by Akastor

Akastor has implemented a set of legally binding rules which provide principles for Processing of Personal Data throughout the Akastor group of companies. As such, Akastor has implemented a Data Protection Standard which sets out how Akastor shall operate in order to comply with such binding corporate rules ("BCR").

The following general principles are in accordance with the principles of the EU Data Protection Directive 95/46/EC. Akastor has by implementing its Data Protection Standard as well as the below privacy principles established a basis for internal control and procedures that ensures compliance with these principles when Processing Personal Data.

1 Fair and lawful Processing

Personal Data shall be processed fair, lawfully and pursuant to the principles stipulated in the Data Protection Standard. This means that Personal Data shall be processed in accordance with law, and that the legitimate interests of the Data Subject should be taken into account when Processing Personal Data.

2 Purpose specification

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

3 Data quality and proportionality

Personal Data shall be:

- adequate, relevant and not excessive in relation to the purposes for which they are collected and /or further processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- kept in a form which permits identification of Data Subjects for no longer than what is necessary for the purposes for which the data were collected or for which they are further processed.

4 Criteria for making Data Processing legitimate

4.1 Processing of Personal Data

Personal Data may be processed only if:

- the Data Subject has given his Consent; or
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract; or
- Processing is necessary for compliance with a legal obligation to which the Controller is subject; or
- Processing is necessary in order to protect the vital interests of the Data Subject; or
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the Data Subject which require protection under Article 1 (1) of the European Data Protection Directive.

4.2 Processing of special categories of data (Sensitive Data)

It is prohibited to process Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the Processing of data concerning health or sex life.

The special categories of data mentioned above may only be processed if:

- the Data Subject has given his explicit consent to the Processing of those data, except where the local laws applicable to the Legal Entity provide that the prohibition above may not be lifted by the Data Subject's giving his consent; or
- Processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by local law providing for adequate safeguards; or
- Processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving his consent; or
- the Processing relates to data which are manifestly made public by the Data Subject or is necessary for the establishment, exercise or defense of legal claims.
- allowed according to other national rules than a)-d) above that have been established in accordance with the Data Protection Directive article 8 no. 4 and 5.

Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under law, subject to derogations which may be granted by local law providing suitable specific safeguards.

4.3 National identification numbers

National identification numbers shall be processed in accordance with the relevant provisions in local laws.

5 Information to be given to the Data Subject

5.1 Information in cases of collection of data from the Data Subject

The Controller must provide a Data Subject from whom data relating to him are collected with at least the following information, except where he already has it:

a) the identity of the Controller and of his representative, if any;

b) the purposes of the Processing for which the data are intended;

c) any further information such as

- the recipients or categories of recipients of the data,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair Processing in respect of the Data Subject.

5.2 Information where the data have not been obtained from the Data Subject

Where the data have not been obtained from the Data Subject, the Controller must at the time of undertaking the recording of Personal Data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the Data Subject with at least the following information, except where he already has it:

a) the identity of the Controller and of his representative, if any;
b) the purposes of the Processing;
c) any further information such as
   - the categories of data concerned,
   - the recipients or categories of recipients,
   - the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair Processing in respect of the Data Subject.

This provision shall not apply where, in particular for Processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law.

6 The Data Subject's right of access to data

Every Data Subject shall have the right to obtain from the Controller:

a) without constraint at reasonable intervals and without excessive delay or expense:
   - confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the Processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
   - confirmation to him in an intelligible form of the data undergoing Processing and of any available information as to their source,
   - knowledge of the logic involved in any automatic Processing of data concerning him at least in the case of automated decisions referred to in Section 7;
b) as appropriate the rectification, erasure or blocking of data the Processing of which does not comply with the provisions of Akastor's BCR, in particular because of the incomplete or inaccurate nature of the data;
c) notifications to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with b), unless this proves impossible or involves a disproportionate effort.

7 Automated individual decisions

The Data Subject has the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated Processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

The Data Subject may be subjected to a decision of the kind referred to above if that decision:

a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the Data Subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

b) is authorized by a law which also lays down measures to safeguard the Data Subject's legitimate interests.

8 Confidentiality of Processing

Any person acting under the authority of the Controller or of the Processor, including the Processor himself, who has access to Personal Data must not process them except on instructions from the Controller, unless he is required to do so by law.

9 Security of Processing

9.1 Appropriate technical and organizational security measures

The Controller 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 data over a network, and against all other unlawful forms of Processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the Processing and the nature of the data to be protected.

9.2 Use of Data Processors

The Controller must, where Processing is carried out on his behalf, choose a Processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the Processing to be carried out, and must ensure compliance with those measures.

The carrying out of Processing by way of a Processor must be governed by a contract or legal act binding the Processor to the Controller and stipulating in particular that:

- the Processor shall act only on instructions from the Controller,
- the obligations set out in 9.1 shall also be incumbent on the Processor.

9.3 Documentation

For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in Section 9.1 and 9.2 shall be in writing or in another equivalent form.

10 Transfer of Personal Data to Controllers and Processors that are members of the group (internal transfer)

10.1 Transfer from Controller to Controller

Transfer of Personal Data between Controllers that are bound by the BCR may take place, provided that:

- it is not incompatible with the purpose for which the Personal Data were collected, cf. 2;
- it is in accordance with the principle of data quality and proportionality, cf. 3;
- the criteria for making Data Processing legitimate is fulfilled, cf. 4;
- if applicable, information is given to the Data Subject in accordance with 5.2;

- appropriate security measures protect the data during transfer and further Processing by the receiving Controller, cf. 9.

10.2 Transfer from Controller to Processor

Transfer of Personal Data from a Controller to a Processor, both bound by Akastor's BCR may take place, provided that:

- the Processor provides sufficient guarantees in respect of the technical security measures and organizational measures governing the Processing to be carried out, cf. 9.1;
- the carrying out of Processing by way of a Processor is governed by a contract or legal act binding the Processor to the Controller and stipulating in particular that:
    - the Processor shall act only on instructions from the Controller,
    - the obligations set out in 9.1 shall also be incumbent on the Processor.

11 Transfer of Personal Data to external Controllers not bound by the Data Protection Standard

11.1 Transfer to external Controllers established within the EEA

Transfer of Personal Data from a Controller established in the EEA to another Controller established in the EEA may take place, provided that:

- it is not incompatible with the purpose for which the Personal Data were collected, cf. 2;
- it is in accordance with the principle of data quality and proportionality, cf. 3;
- the criteria for making data Processing legitimate is fulfilled, cf. 4;
- if applicable, information is given to the Data Subject in accordance with 5.2;
- appropriate security measures protect the data during transfer and further Processing by the receiving Controller, cf. 9.

Applicable local law may have additional requirements and should always be considered before making such transfers.

11.2 Transfer to external Controller established outside the EEA

Transfer of Personal Data from a Controller established within the EEA to a Controller established outside the EEA is prohibited, except when one of the following requirements is fulfilled:

- the receiving Controller is established in a country which the EU Commission has considered having an adequate level of protection, cf. the Commission's decisions on the adequacy of the protection of Personal Data in third countries provided at: http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm;
- the receiving Controller is established in the US and has endorsed the Safe Harbour Principles;
- one of the derogations in the EU Data Protection Directive article 26 applies;
- the transfer is regulated by the EU standard contractual clauses for Controller to Controller transfer of Personal Data.

12 Transfer of Personal Data to external Processors

12.1 Transfer to external Processors established within the EEA

Transfer of Personal Data from a Controller established in the EEA to a Processor established in the EEA may take place, provided that:

- the Processor provides sufficient guarantees in respect of the technical security measures and organizational measures governing the Processing to be carried out, cf. 9.2;
- the carrying out of Processing by way of a Processor is governed by a contract or legal act binding the Processor to the Controller and stipulating in particular that:
    - the Processor shall act only on instructions from the Controller,
    - the obligations set out in 9.1, cf. the Data protection directive art 17, shall also be incumbent on the Processor.

12.2 Transfer to external Processor established outside the EEA

Transfer of Personal Data from a Controller established within the EEA to a Processor established outside the EEA is prohibited, except when:

- the receiving Controller is established in a country which the EU Commission has considered having an adequate level of protection, cf. the Commission's decisions on the adequacy of the protection of Personal Data in third countries provided at: http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm; or
- the Processor is established in the US and has endorsed the Safe Harbour Principles; or
- one of the derogations in the Data Protection Directive article 26 applies;

and;

- the Processor provides sufficient guarantees in respect of the technical security measures and organizational measures governing the Processing to be carried out, cf. 9.2;
- the carrying out of Processing by way of a Processor is governed by a contract or legal act binding the Processor to the Controller and stipulating in particular that:
    - the Processor shall act only on instructions from the Controller,
    - the obligations set out in 9.1, cf. the Data protection directive art 17, shall also be incumbent on the Processor.

or

- the transfer is regulated by the EU standard contractual clauses for Controller to Processor transfer of Personal Data.