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 General Data Protection Regulation 2016/679 (GDPR). 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, lawful and transparent Processing

Personal Data shall be processed fairly, lawfully, in an transparent manner 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 limitation

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

3 Data minimization, accuracy and storage limitation

Personal Data shall be:

- adequate, relevant and limited to what is necessary 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, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified without delay;
- 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 at least one of the following legal bases applies:

a) the Data Subject has given his Consent to the Processing of his/her Personal Data for one or more specific purposes. In order to rely on Consent, the conditions in Section 4.4 must be fulfilled. Following from this, Akastor will generally not rely on consent for any Processing relating to employee data, except when consent can be given in a clearly voluntary manner;

b) 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;

c) Processing is necessary for compliance with a legal obligation to which the Controller is subject; or

d) Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;

e) 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

f) Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data.

4.2 Processing of special categories of data (Sensitive Data)

Processing of Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall as a general rule be prohibited in Akastor.

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

a) the Data Subject has given explicit Consent to the Processing of those data for one or more specified purposes, except where the local laws applicable to the Legal Entity provide that the prohibition above may not be lifted by the Data Subject. In order to rely on Consent, the conditions in Section 4.4.4 must be fulfilled;

b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller in the field of employment and social security and social protection law in so far as it is authorized by local law or a collective agreement pursuant to local law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject;

c) Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving Consent;

d) the Processing relates to Personal Data which are manifestly made public by the Data Subject;

e) Processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;

f) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of local law or pursuant to a contract with a health professional that is subject to the obligation of professional secrecy or another person subject to an equivalent obligation of secrecy; or

g) allowed according to GDPR Article 9 or other national rules than a)-f) above that have been established in accordance with GDPR Article 9.

4.3 Processing of Personal Data relating to criminal convictions and offences

Processing of data relating to criminal convictions, offences or related security measures based on Article 6(1) of the GDPR may only be carried out in accordance with applicable law.

4.4 Conditions for Consent

If Consent is allowed or required under applicable law for the Processing of Personal Data or Processing of Sensitive Data, the following conditions apply:

a) Akastor must be able to demonstrate that the Data Subject has Consented to the Processing of his/her Personal Data. Where Processing is undertaken at the request of the Data Subject, he/she is deemed to have provided Consent to the Processing;

b) Akastor must inform the Data Subject in accordance with the provisions set forth in Section 5.1 below;

c) If the Data Subject's Consent is given in the context of a written declaration which also concerns other matters, the request for Consent shall, where applicable law so requires, be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. and

d) The Data Subject may withdraw his/her Consent at any time and the Data Subject shall, where applicable law so requires, be informed of his or her right to withdraw the Consent. The withdrawal of Consent shall

not affect the lawfulness of the Processing based on such Consent before its withdrawal. It shall be as easy to withdraw as to give Consent.

Consent is only to be used when it is likely to be valid as a legal basis for the Processing. With regard to employment relationships. Consent should therefore not be used as a legal basis, unless it is clear that it is freely given. This may typically be when the Data Subject voluntarily participate in a survey or event arranged by Akastor, register for a newsletter or otherwise participate in activities or make use of resources (such as summer cabins and sports activities) provided by Akastor.

4.5 Processing which does not require identification

If the purposes that Controller processes Personal Data for do not or no longer require the identification of a Data Subject, the Controller shall not be obliged to maintain, acquire or process additional information in order to identify the Data subject for the sole purpose of complying with applicable EU/EEA data protection law. This applies for example to big data analysis and statistics where the Personal Data have been anonymized.

When the Controller is able to demonstrate that it is not in a position to identify the Data Subject, Section 6.1 to 6.6 shall not apply except where the Data Subject, for the purpose of exercising his/her rights under those Articles, provides additional information enabling his/her identification. In such cases, the Controller shall inform the Data Subject accordingly, if possible.

4.6 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 Personal Data from the Data Subject

Where Personal Data are collected from the Data Subject, the Controller shall, at the time when Personal Data are obtained, provide the Data Subject with all of the following information:

a) the identity and the contact details of the Controller;

b) the contact details of the Global or Local Privacy Officer;

c) the purposes of the Processing for which the Personal Data are intended as well as the legal basis for the Processing;

d) where the Processing is based on point f) set out in 4.1 above, the legitimate interest pursued by the Controller or by a third party; and

e) where applicable, the fact that the Controller intends to transfer such Personal Data to a Third Country or an international organization, with a reference to the appropriate safeguards cf. Section 15.2 and the means by which to obtain a copy of such safeguards or where they are made available if the Third Country or organization in question is not recognized by the EU Commission as ensuring an adequate level of protection.

In addition, where required by applicable law and if necessary to ensure fair and transparent Processing, the Controller shall provide the Data Subject with the following further information:

a) the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;

b) the existence of the right to request from the Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to the Processing as well as the right to data portability;

c) where the processing is based on Data Subject's Consent, the existence of the right to withdraw Consent at any

time, without affecting the lawfulness of Processing based on Consent before its withdrawal;

d) the right to lodge a complaint with a supervisory authority;

e) whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data;

f) the existence of automated decision-making, including profiling, referred to in Section 7 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

Where a Controller intends to further Process the Personal Data for a secondary purpose, the Controller shall, if applicable law so requires, provide the Data Subject prior to the further Processing with information about the secondary purpose and any relevant information as set out in paragraph 2 of this Article 5.1.

It is not necessary to provide the information mentioned above to the Data Subject if he/her already has it.

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

If applicable local law so requires, where the Personal Data have not been obtained from the Data Subject, the Controller shall within the timeframes set out below provide the Data Subject with the following information:

a) the identity and the contact details of the Controller;

b) the contact details of the Global or Local Privacy Officer;

c) the purposes of the Processing for which the Personal Data are intended as well as the legal basis for the processing;

d) the categories of Personal Data concerned;

e) the recipients or categories of recipients of the Personal Data, if any;

f) where applicable, the fact that the Controller intends to transfer such Personal Data to a Third Country or an international organization, with a reference to the appropriate safeguards cf. Section 15.2 and the means by which to obtain a copy of such safeguards or where they are made available if the Third Country or organization in question is not recognized by the EU Commission as ensuring an adequate level of protection.

In addition, when required by applicable law and if necessary to ensure fair and transparent Processing, the Controller shall provide the Data Subject with the following further information:

a) the period for which the Personal Data will be stored, or the criteria used to determine that period;

b) where the Processing is based on Section 4.1(f), the legitimate interests pursued by the Controller or by a third party;

c) the existence of the right to request from the Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to the Processing as well as the right to data portability;

d) where the processing is based on Data Subject's Consent, the existence of the right to withdraw Consent at any time, without affecting the lawfulness of Processing based on Consent before its withdrawal;

e) the right to lodge a complaint with a Data Protection Authority;

f) from which source the Personal Data originate, and if applicable, whether it came from publicly accessible sources;

g) the existence of automated decision-making, including profiling, referred to in Section 7 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

The information mentioned above shall be provided:

a) within a reasonable time after obtaining the Personal Data, at the latest within one month from obtaining the Personal Data;

b) if the Personal Data are used for communication with the Data Subject, at the latest at the time of the first communication with the Data Subject;

c) if a disclosure to another recipient is envisaged, at the latest when the Personal Data are first disclosed.

Where a Controller intends to further Process the Personal Data for a secondary purpose, the Controller shall, if applicable law so requires, provide the Data Subject prior to the further Processing with information about the secondary purpose and any relevant information as set out in paragraph 2 of this Section 5.2.

The requirements of this Section 5.2 may be set aside where and insofar:

a) the Data Subject already has the information;

b) it is impossible or would involve a disproportionate effort to provide the information to Data Subjects or providing the information would be likely to render impossible or seriously impair the achievement of the objectives of the Processing. In such cases, the Controller shall take appropriate measures to protect the Data Subject's rights and freedoms and legitimate interest, including making the information publicly available;

c) obtaining or disclosure is expressly laid down by applicable EU/EEA law to which the Controller is subject and which provides appropriate measures to protect the Data Subject's legitimate interests; or

d) where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by applicable EU/EEA law, including a statutory obligation of secrecy.

6 The Data Subject's rights

6.1 Data Subject's right of access

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

a) confirmation as to whether or not data relating to him are being processed and where that is the case, access to the Personal Data processed by the Controller;

b) information about the purposes of the Processing, the categories of data concerned, and the recipients or categories of recipients to whom the data aredisclosed, in particular recipients located in a Third Country. If the Third Country is not recognized by the EU Commission as ensuring an adequate level of protection, the Data Subject shall have the right to be informed of the appropriate safeguards referred to in Section 15.2;

c) where possible, information about the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;

d) information about the existence of the right to request from the Controller rectification or erasure of Personal Data or restriction of the Processing of Personal Data concerning the Data Subject or to object to such Processing;

e) information about the right to lodge a complaint with a Data Protection Authority;

f) where the Personal Data have not been collected from the Data Subject, any available information as to their source; and

g) the existence of automated decision-making, including profiling, referred to in Section 7 and, at least in those cases, meaningful information about the logic involved in any automatic Processing as well as the significance and the envisaged consequences of such Processing for the Data Subject.

6.2 Data Subject's right of rectification

The Data Subject shall have the right to obtain from the Controller without undue delay the rectification of inaccurate Personal Data concerning him/her. Taking into account the purposes of the Processing, the Data Subject shall further have the right to have incomplete Personal Data completed, including by means of a supplementary statement.

6.3 Data Subject's right of erasure

Where required by applicable law, the Data Subject shall have the right to obtain from the Controller the erasure of Personal Data concerning him or her without undue delay. The Controller shall have the obligation to meet such a request by erasing Personal Data without undue delay when one of the following grounds applies:

a) the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise Processed;
b) the Data Subject withdraws his or her Consent to the Processing and where there is no other legal basis for the Processing;
c) the Data Subject objects to the Processing pursuant to Section 6.6 (a) and there are no overriding legitimate grounds for the Processing, or the Data Subject objects to the Processing pursuant to Section 6.6 (b);
d) the Personal Data have been unlawfully Processed;
e) the Personal have to be erased for compliance with a legal obligation in applicable EU/EEA law to which the Controller is subject.

The Data Subject's right to erasure shall not apply to the extent that Processing is necessary for:

a) exercising the right of freedom of expression and information;
b) compliance with a legal obligation which requires processing by applicable EU/EEA law to which the Controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
c) the establishment, exercise or defense of legal claims.

6.4 Data Subject's right of restriction of Processing

Where required by applicable law, the Data Subject shall have the right to obtain from the Controller restriction of Processing where one of the following applies:

a) the accuracy of the Personal Data is contested by the Data Subject for a period enabling the controller to verify the accuracy of the Personal Data;
b) the processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;
c) the Controller no longer needs the Personal Data for the purposes of the Processing, but they are required by the Data Subject for the establishment, exercise or defense of legal claims;
d) the Data Subject has objected to the Processing under section 6.6 pending the verification whether the legitimate grounds of the Controller override those of the Data Subject.

Where Processing has been restricted under paragraph 1, such Personal Data shall, with the exception of storage, only be Processed by the Data Subject's Consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the EU/EEA or of a EU/EEA country where the Controller is established. The Controller shall inform the Data Subject who has obtained restriction of Processing, prior to the lifting the restriction.

6.5 Notification obligation regarding rectification or erasure of Personal Data or restriction of Processing

Where required by applicable law, the Controller shall communicate any rectification or erasure of Personal Data or restriction of Processing carried out in accordance with Section 6.2 to 6.4 above to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort.

Where required by applicable law, the Controller shall inform the Data Subject about those recipients if the Data Subject requests it.

6.6 Data Subject's right to object to the Processing

The Data Subject has the right to object at any time, on grounds relating to his/her particular situation, to the Processing of data concerning him or her in the cases referred to in Section 4.1 e) and f), save where otherwise provided by national legislation. This includes profiling based on those provisions.

If a Data Subject objects to the Processing, the Controller shall no longer Process the Personal Data unless:

a) the Controller demonstrates compelling legitimate grounds for the Processing which override the interests,

rights and freedoms of the Data Subject; or

b) the Processing is necessary for the establishment, exercise or defense of a legal claim.

The Data Subject shall, where Personal Data are Processed for the purposes of direct marketing, have the right to object at any time to Processing of Personal Data concerning him or her for such marketing. This includes profiling to the extent that it is related to such direct marketing. Where the Data Subject objects to Processing for direct marketing purposes, the Personal Data shall no longer be processed for such purposes.

The right to object shall be explicitly brought to the Data Subject's attention in a clear way and separately from any other information, at the latest at the time of the first communication with the Data Subject.

6.7 Procedure for handling Data Subjects' requests

Requests in accordance with Section 6.1 to 6.6 should be filed in writing to the relevant Privacy Officer. Prior to fulfilling the Data Subject's request, the Controller may, where appropriate, request the Data Subject to:

a) specify the IT system in which the Personal Data are likely to be stored;

b) specify the circumstances in which the Controller obtained the Personal Data; and

c) show proof of his or her identity.

Further, in the case of an access request, the Controller may, where appropriate, request the Data Subject to specify the categories of Personal Data to which he or she requests access. Any provision of Personal Data to the Data Subject shall be provided in a secure manner.

In the case of a request for rectification, erasure or restriction, the Controller may, where appropriate, request the Data Subject to specify the reasons why the Personal Data are incorrect, incomplete or not processed in accordance with applicable law or the Data Protection Standard.

In the case of an objection in accordance with Section 6.6, the Controller may, where appropriate, request the Data Subject to specify the processing operation to which the objection relates.

When a request has been made by electronic form means, the response shall be provided by electronic means where possible and secure, unless otherwise requested by the Data Subject. The request shall be responded to without undue delay and in any event within one month of receipt of the request. This period may be extended by two more months where necessary, taking into account the complexity and number of the requests. In such cases, the Data Subject shall be informed of any such extension within one month from receipt of the request, together with the reasons for the delay.

In the case of an objection, the relevant Privacy Officer shall respond by confirming whether or not the particular Processing will be stopped. If the Processing is not stopped, the communication must be accompanied with the reasons for continuing the Processing.

If Data Subjects are not satisfied with the response to their requests, they may file a complaint in accordance with Section 9 of the Data Protection Standard.

7 Automated individual decisions

The Data Subject has the right not to be subject to a decision which produces legal effects concerning him/her, or significantly affects him/her and which is based solely on automated Processing of Personal Data. Such Processing may for example consist of evaluation of certain personal aspects relating to the Data Subject, such as his/her 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 necessary for entering into, or performance of, a contract between the Data Subject and the Controller;

b) is authorized by applicable law which also lays down suitable measures to safeguard the Data Subject's rights, freedoms and legitimate interests; or
c) is based on the Data Subject's explicit Consent.

In the cases referred to in a) and c) above, the Controller shall implement suitable measures to safeguard the Data Subject's rights, freedoms and legitimate interests, and at least the right to obtain human intervention on the part of the Controller, to express his or her point of view and to contest the decisions.

The automated decisions referred to in this Section 7 shall not be based on the Processing of Sensitive Personal Data unless point a) of Section 4.2 applies and suitable measures to safeguard the Data Subject's rights, freedoms and legitimate interests are in place.

8 Data protection by design and by default

Where required by applicable law, the Controller shall, both when determining the means for Processing and at the time of the Processing, implement appropriate technical and organizational measures, which are designed to implement data protection principles, such as data minimization, in an effective manner, in order to integrate the necessary safeguards into the Processing for protecting Data Subjects' rights. These measures shall be implemented by taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of Processing, as well as the severity and likelihood of the risks posed by the Processing to the rights of the Data Subjects.

The Controller shall, where required by applicable law, implement appropriate technical and organizational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are processed. This obligation applies to the amount of Personal Data collected, the extent of their Processing, the period of their storage and their accessibility. These measures shall particularly ensure that by default, Personal Data are not made accessible without intervention to an indefinite number of persons.

9 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.

10 Security of Processing

Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

10.1 Appropriate technical and organizational security measures

The Controller and 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 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.

10.2 Personal Data Breach notification

If a Personal Data Breach has occurred, the Deviation Handling Procedure shall be followed and the competent Data Protection Authority and/or concerned Data Subjects shall be notified when required under applicable law.

10.3 Information Security Risk Assessment and Data Protection Impact Assessment

In the event of new Processing activities, or changes to existing Processing activiites, the Controller shall follow the Data Protection Risk Assessment Procedure and assess whether an information security risk assessment and/or data protection impact assessment is necessary.

11 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 written contract or legal act binding the Processor to the Controller (Data Processing Agreement). The Data Processing Agreement shall set out the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of the Controller. The Data Processing Agreement shall stipulate, in particular that the Processor:

a) processes the Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country or international organization, unless required to do so by national law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;
b) ensures that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
c) implements physical, technical and organizational security measures to ensure a level of security appropriate to the risk of the Processing;
d) takes all measures required by law for engaging another Processor;
e) taking into account the nature of the Processing, assists the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights under applicable EU/EEA data protection law;
f) assists the Controller in ensuring compliance with the obligations relating to the security of Processing and related requirements as set out in the Data Protection Risk Assessment Procedure, taking into account the nature of the Processing and the information available to the Processor;
g) at the choice of the Controller, deletes or returns all the Personal Data after the end of the provision of services relating to Processing, and deletes existing copies unless applicable law requires storage of the Personal Data;
h) makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Data Protection Standard and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

For Processors established or with access from outside the EEA, the requirements set out in Section 13.2 or 15.2 must also be fulfilled.

12 Joint Controllers

In situations where two or more Controllers jointly determine the purposes and means of the Processing, they shall be Joint Controllers. Such situations may arise when two Legal Entities together determine the purposes and means of the Processing, such as in cases of research, innovation or use of joint facilities.

Whether there are Joint Controllers must be assessed on a case-by-case basis and depends on whether there is any joint determination in relation to the purposes and means of the Processing. In the cases of Joint Controllers, they shall in a transparent manner determine their respective responsibilities for compliance with applicable EU/EEA data protection law, in particular as regards the information requirements and the Data Subjects rights

referred to in Sections 5 to 6.

The responsibilities shall be described in an arrangement between the parties unless and in so far as, the respective responsibilities of the Controllers are determined by applicable EU/EEA data protection law. The essence of the arrangement shall be made available to the Data Subject.

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

13.1 Transfer from Controller to Controller

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

a) it is not incompatible with the purpose for which the Personal Data were collected, cf. 2;
b) it is in accordance with the principle of data minimization, accuracy and storage limitation, cf. 3;
c) the criteria for making Data Processing legitimate is fulfilled, cf. 4;
d) if applicable, information is given to the Data Subject in accordance with 5;
e) appropriate security measures protect the data during transfer and further Processing by the receiving Controller, cf. 10.

13.2 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:

a) the Processor provides sufficient guarantees in respect of the technical security measures and organizational measures governing the Processing to be carried out, cf. 10.1; and
b) 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 what is set out in Section 11 above.

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

14.1 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:

a) it is not incompatible with the purpose for which the Personal Data were collected, cf. 2;
b) it is in accordance with the principle of data minimization, accuracy and storage limitation, cf. 3;
c) the criteria for making data Processing legitimate is fulfilled, cf. 4;
d) if applicable, information is given to the Data Subject in accordance with 5;
e) appropriate security measures protect the data during transfer and further Processing by the receiving Controller, cf. 10.

Applicable local law may have additional requirements and should always be considered before making such transfers. Such transfer could include for example transfer of data to travel agencies or customers which have independent Controller responsibility.

14.2 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 the conditions in Section 14.1 are fulfilled and one of the conditions in Section 15.2 are met. Such transfer could include for example transfer to customers outside the EEA having an independent Controller

responsibility.

15 Transfer of Personal Data to external Processors

15.1 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. 10.1; and
- 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 what is set out in Section 11 above.

15.2 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 conditions in Section 15.1 are met (including the requirements set out in Section 10.1 and 11) and one of the legal basis in Article 45, 46, 47 or 49 of the GDPR applies, including:

a) the receiving Processor 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;

a) the Processor is established in the US and has been certified under the EU-US Privacy Shield or any other similar program that is recognized by the EU Commission as ensuring an adequate level of protection;

b) the Processor has implemented Binding Corporate Rules or a similar transfer mechanism that provides appropriate safeguards under applicable law;

c) the Controller and the Processor have provided appropriate safeguards by entering into EU Standard Contractual Clauses (model contract);

d) the Controller and the Processor have provided appropriate safeguards by entering into Standard Data Protection Clauses adopted by the EU Commission or a Data Protection Authority; or

e) an approved code of conduct or an approved certification mechanism pursuant to Article 46(1)(e) and (f) of the GDPR are provided for.

In specific situations where a transfer cannot be based on a) to f) above, transfer may take place on one or more of the following conditions:

a) the transfer is necessary for the performance of a contract between the Controller and the Data Subject or for taking necessary steps at the request of the Data Subject prior to entering into a contract;

b) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural and legal person;

c) the transfer is necessary for important reasons of public interest;

d) the transfer is necessary for the establishment, exercise or defense of a legal claim;

e) the transfer is necessary to protect a vital interest of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving Consent; or

f) the transfer is required by any law to which the relevant Controller is subject.

Transfers based on paragraph 2 litra b) and e) above require the prior approval of the Global Privacy Officer.

15.3 Data Subject's Consent for Transfer

If none of the conditions listed in Section 15.2 are met or Consent is allowed or required under applicable law, Akastor

shall (also) seek an explicit Consent from the Data Subject for the relevant transfer. The Consent must be requested prior to participation of the Data Subject in specific projects, assignments or tasks that require the transfer of Personal Data.

A transfer cannot be based on a Data Subject's Consent if it has foreseeable adverse consequences for the Data Subject. This means that Consent will as a main rule not be a valid basis for transfers relating to employees.

Prior to requesting Consent, the Data Subject shall be informed of the possible risks of the transfer due to the absence of appropriate safeguards and the fact that the EU Commission has not recognized this country as ensuring an adequate level of protection. When requesting Consent, the conditions in Section 4.4 shall apply.

15.4 Transfers between Legal Entities located in countries not covered by an adequacy decision from the EU Commission

Transfers from a Legal Entity located in a Third Country that is not covered by an adequacy decision from the EU Commission to another Legal Entity also located in a Third country not covered by such adequacy decision are permitted if one of the grounds in Section 15.2 applies or if the transfers are:

a) necessary for compliance with a legal obligation to which the relevant Legal Entity is subject;
b) necessary to serve the public interest; or
a) necessary to satisfy a legitimate purpose of the Legal Entity, such as recruitment, obtaining contracts etc..

If conditions a), b) or c) are fulfilled, use of EU standard clauses (or other legal basis for transfer listed in Section 15.2) are not necessary.

16 Revision Summary

Rev. No.	Issue date	Description of updates
0	8 May 2015	First Akastor edition
1	5 January 2018	Adapted to GDPR