1 Introduction

Aker Solutions is committed to protection of Personal Data of individuals by implementing the Data Protection Procedure, and related governing documents, constituting the Binding Corporate Rules (BCR). The BCR contains a set of legally binding rules within Aker Solutions which provide principles for Processing of Personal Data within the BCR Members. The BCR is binding on and shall be adhered to by Aker Solutions ASA and the subsidiaries set out in the list of members for which the BCR applies (attached), including their employees

This public extract of the BCR contains the key information and material provisions found in the BCR, hereunder the key principles of processing and rights of data subjects. For any questions related to this extract, the full text BCR or its member, please contact dataprotection@akersolutions.com. At this e-mail address, you may also reach the Group Privacy Officer of Aker Solutions.

2 Material Scope

The BCR is binding on and shall be adhered to by Aker Solutions ASA and the subsidiaries set out in the list of members for which the BCR applies, including their employees. The list is found on www.akersolutions.com. For the purpose of the BCR, the term “Aker Solutions” refers to the whole company group or each of the BCR Members as the case may be.

All Data Subjects (e.g. employees, contractors, customers and other third parties) whose Personal Data is being Processed under this Procedure shall benefit from the rights herein.

3 Data Protection Principles

The following general principles are based on the principles of the GDPR and Applicable EU/EEA Data Protection Law. Further details may be set out in data privacy and information security global procedures applicable to all Business Units.

3.1 Lawfulness, fairness and transparency

Personal Data shall be Processed fairly, lawfully, in a transparent manner and pursuant to the principles stipulated in the Data Protection Procedure. This means that Personal Data shall be Processed in accordance with law, and that the legitimate interests of the Data Subject shall be taken into account when Processing Personal Data.

3.2 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.

3.3 Data minimization, accuracy and storage limitation

Personal Data shall be:

a) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected and/ Processed ("data minimization");
b) 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 ("accuracy"); and
c) Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further Processed ("storage limitation").

3.4 Criteria for making data Processing lawful

3.4.1 Lawful Processing of Personal Data

Personal Data may be lawfully Processed only if at least one of the following legal basis applies:

a) The Data Subject has given Consent to the Processing of his or her Personal Data for one or more specific purposes. In order to rely on Consent, the conditions in Section 4.4.4 must be fulfilled;
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 under Applicable EU/EEA Law to which the Controller is subject;
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 in accordance with Applicable EU/EEA Law; 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.

3.4.2 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 to Process genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or sex life or sexual orientation.

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 Business Unit 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 or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorized by Applicable EU/EEA Law or a collective

agreement pursuant to Applicable EU/EEA 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 is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the Processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed outside that body without the consent of the Data Subjects;
e) the Processing relates to data which are manifestly made public by the Data Subject;
f) Processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
g) Processing is necessary for reasons of substantial public interest, on the basis of Applicable EU/EEA Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;
h) 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 Applicable EU/EEA 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
i) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR based on Applicable EU/EEA Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

3.4.3 Processing of Personal Data relating to criminal convictions and offences

Processing of Personal Data relating to criminal convictions, offences or related security measures may only be carried out in accordance with the conditions set out in Article 10 GDPR.

3.4.4 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) Aker Solutions 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 or she is deemed to have provided Consent to the Processing;
b) Aker Solutions must inform the Data Subject in accordance with the provisions set forth in Section 4.5.1 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) 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 shall therefore not be used as a legal basis, unless it is clear that it is freely given. This will typically be when the Data Subjects voluntarily participate in a survey, or events arranged by Aker Solutions or register for a newsletter from Aker Solutions.
e) 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.

3.4.5 National identification numbers

National identification numbers shall be Processed in accordance with the relevant provisions in local regulations in the Controller's country.

3.5 Information to be provided to the Data Subject

3.5.1 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 and of his representative, if any;
b) The contact details of the Group Privacy Officer or relevant 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 4.4.1 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 4.14.2 and 4.15.2 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 4.6.8 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 Section 4.5.1.

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

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

If Applicable 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 and of his representative, if any;
b) The contact details of the Group or 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 4.14.2 and 4.15.2 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 4.4.1(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;
a) 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 Data Protection Authority;
e) From which source the Personal Data originate, and if applicable, whether it came from publicly accessible sources;
f) The existence of automated decision-making, including profiling, referred to in Section 4.6.8 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 4.5.2.

The requirements of this Section 4.5.2 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.

3.6 The Data Subject's rights

3.6.1 Beneficiary rights

All Data Subjects (e.g. employees, contractors, customers and other third parties) whose Personal Data is being Processed under this Procedure shall benefit from the rights herein.

The Data Subject's rights include the right to enforce:

- Lawful, fair and transparent Processing
- Purpose limitation
- Data minimization, accuracy and storage limitation
- Criteria for making the Processing lawful
- Transparency and easy access to the Data Protection Procedure
- Rights of information, access, rectification, erasure, restriction of Processing, notification regarding rectification, erasure or restriction, objection to Processing, and not being subject to decisions based solely on automated Processing, including profiling
- Right to data portability
- Security and confidentiality, including Personal Data breach notifications
- Restrictions on onward transfers outside of the group of companies
- Obligations in case of local laws and practices affecting compliance with the Data Protection Procedure in case of government access requests
- Right to complain through the internal complaint mechanisms of the companies
- Cooperation duties with Data Protection Authority
- Liability and jurisdiction provisions
- The duty to inform the Data Subjects about any update of the Data Protection Procedure and of the list of members of the BCR
- This Section on third-party beneficiary rights
- Rights to judicial remedies, redress and compensation

Data Subjects' queries and complaints shall be handled in a timely manner by the relevant Privacy Officer in accordance with internal procedures, as set out in the Data Protection Procedure Complaint Mechanism.

3.6.2 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, a copy of the Personal Data Processed by the Controller and;

b) Information about the purposes of the Processing, the categories of Personal Data concerned, and the recipients or categories of recipients to whom the data are disclosed, 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 Sections 4.14.2 and 4.15.2;
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) Information about the existence of automated decision-making, including profiling, referred to in the Section 4.6.8 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.

The right to obtain access to the Personal Data Processed referred to above shall not adversely affect the rights and freedoms of others.

3.6.3 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 or 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.

3.6.4 Right of erasure

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 and there are no overriding legitimate grounds for the Processing
d) The Personal Data have been unlawfully Processed;
e) The Personal Data 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) Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing;
d) The establishment, exercise or defense of legal claims.

3.6.5 Right of restriction of Processing

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 pending the verification whether the legitimate grounds of the Controller override those of the Data Subject.

Where Processing has been restricted, such Personal Data shall, with the exception of storage, only be Processed with 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 an 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.

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

The Controller shall communicate any rectification or erasure of Personal Data or restriction of Processing carried out in accordance with the Data Protection Procedure to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort.

The Controller shall inform the Data Subject about those recipients if the Data Subject so requests.

3.6.7 Right of data portability

The Data Subject shall have the right to data portability, being the right to receive the Personal Data concerning him or her, which he or she has provided to the Controller, in a structured, commonly used and machine-readable form and have the right to transmit those data to another Controller without hindrance.

3.6.8 The 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 this Data Protection Procedure. 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.

3.6.9 Automated individual decisions

The Data Subject has the right not to be subject to a decision which produces legal effects concerning him or her, or significantly affects him or 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 or 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 EU/EEA 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 shall not be based on the Processing of Sensitive Personal Data unless point a) of Section 3.4.2 applies and suitable measures to safeguard the Data Subject's rights, freedoms and legitimate interests are in place.

3.7 Procedure for logging a Data Subject's requests

Requests in accordance with Data Subject Rights may be filed in writing to the relevant Privacy Officer by sending an e-mail to dataprotection@akersolutions.com. The address for delivering claims is Aker Solutions AS, Oksenøyveien 8, 1366 Lysaker.

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 and the time period the Personal Data pertain to;
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. 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 Procedure. In the case of an objection in accordance with Section 4.6.7, 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, 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 Data 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 3.5 and the Data Protection Procedure Complaint Mechanism Tool.

3.8 Complaint mechanisms

All Data Subjects, i.e. employees and third party beneficiaries, shall have the right to claim that any of Aker Solutions' Business Units is not complying with the Data Protection Procedure by making a written complaint about this.

Employees may file a complaint to the local People & Organization (HR) representative, to his or her manager, or to any appointed Privacy Officer, including the Group Privacy Officer. If the Data Subject is a third party beneficiary, the Data Subject may complain to the Group Privacy Officer either by clicking the link on the Aker Solutions web site [www.akersolutions.com], or by sending an email to dataprotection@akersolutions.com or by postal mail to Oksenøyveien 8, 1366 Lysaker, Norway (PO. Box 941325 Lysaker, Norway).

Data Subjects' queries and complaints shall be handled in a timely manner by the relevant Privacy Officer in accordance with internal procedures, as set out in the Data Protection Procedure Complaint Mechanism. The Privacy Officer shall provide information on actions taken to the complainant without undue delay, and in any event within one month. Taking to account the complexity and number of the requests, that one-month period may be extended at maximum by two further months, in which case the complainant shall be informed accordingly. The Data Protection Procedure Complaint Mechanism Tool published on the Aker Solutions' intranet provides for processes and further information.

Data Subjects are encouraged to first follow the complaints procedure set forth in this Section 3.5 before filing any complaint or claim with competent Data Protection Authorities or the courts, but following the complaints procedure is not mandatory.

In case of violation of this Data Protection Procedure or in the case the Data Subject does not receive a timely reply or a solution in a sufficient manner, the Data Subject may, at his or her choice, submit a complaint or a claim to:

- The Data Protection Authority, in particular in the EEA country of the Data Subject's habitual residence, place of work or place of the alleged infringement; and
- The competent court of the EEA country where the Controller or Processor has an establishment, or where the Data Subject has their habitual residence.

The Data Protection Authorities and courts shall apply their own substantive and procedural laws to the dispute. Any choice made by the Data Subject will not prejudice the substantive or procedural rights he or she may have under Applicable Law.

3.9 Security of Processing

3.9.1 Appropriate technical and organizational security measures

The Controller and Processor must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the Processing of the Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. In assessing the appropriate level of security, the Controller and Processor must take into account the risks presented by the Processing, in particular from accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure of or access to the Personal Data.

3.9.2 Personal Data Breach Notification

If a Personal Data Breach has occurred or is suspected to have occurred, the person who has become aware of or suspects the Personal Data Breach, shall immediately notify the Group Privacy Officer or the Privacy Officer who shall forward the notification to the Group Privacy Officer. Aker Solutions AS, as the liable BCR member cf. Section 3.1.3, and the Business Unit acting as Controller for the Processing concerned, shall be notified without undue delay in accordance with the applicable internal procedures and work instructions.

A Personal Data Breach occurs for example if the Controller's data systems are hacked, Personal Data is accidentally or intentionally sent to the wrong recipient, Personal Data is left in a place where unauthorized personnel can access the data, data theft and other kinds of data leaks.

Aker Solutions has established an Incident Response procedure and a work instruction on handling Personal Data Breaches. Please consult this procedure for details and timelines for determining when notification to the competent Data Protection Authority and the concerned Data Subjects is required. The procedure shall at a minimum contain the following requirements:

a) Aker Solutions shall without undue delay, and, where feasible, not later than 72 hours after having become aware of the Personal Data Breach to the competent Data Protection Authority, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons;
b) Aker Solutions shall without undue delay notify Data Subjects, where the Personal Data Breach is likely to result in a high risk to their rights and freedoms in line with the requirements of Article 34 GDPR.

Aker Solutions shall document all Personal Data Breaches, comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken. That documentation shall be made available to the competent Data Protection Authority upon request.

3.10 Transfer of Personal Data to Controllers and Processors bound by the Data Protection Procedure

In situations where the Transfer does not have a legal basis in an adequacy decision by the EU Commission in accordance with GDPR Article 45, the BCR provides a legal basis for Transfers of Personal Data from a Data Exporter bound by the Data Protection Procedure to a Data Importer bound by the Data Protection Procedure.

3.10.1 Transfer and Onward Transfer of Personal Data to external Controllers or Processors not bound by the Data Protection Procedure

In addition to the other requirements set out in the BCR, any Transfer or Onward Transfer of Personal Data to an external Controller or Processor 1) established in a Third Country and 2) not bound by the BCR must have a legal basis in accordance with the GDPR Chapter V, including, but not limited to:

a) An adequacy decision by the EU Commission in accordance with GDPR Article 45;
b) Appropriate safeguards pursuant to GDPR Article 46, such as standard data protection clauses adopted by the EU Commission; or
c) A derogation for specific situations under GDPR Article 49.

A disclosure of Personal Data to external Controllers or Processors that does not constitute a Transfer or Onward Transfer, is subject to Section 4.16 in the BCR.

The BCR contains obligations ensuring that the Controller shall use the BCR as a tool for Transfers only where they have assessed that the law and practices in the Third Country of destination applicable to the Processing of the Personal Data by the Data Importer, including any requirements to disclose Personal Data or measures authorizing access by public authorities, do not prevent it from fulfilling its obligations under this Data Protection Procedure. Suspension of data exports may be required as further described in the BCR.

4 Local laws and practices affecting compliance with the Data Protection Procedure

4.1 Relationship between national laws and the Data Protection Procedure

Nothing in this Data Protection Procedure shall be construed as a limitation of rights or remedies that Data Subjects may have under Applicable Law. This Data Protection Procedure provides supplemental rights and remedies to Data Subjects only.

4.2 Obligation to assess local law and practices

The Controller shall use the Data Protection Procedure as a tool for Transfers only where they have assessed that the law and practices in the Third Country of destination applicable to the Processing of the Personal Data by the Data Importer, including any requirements to disclose Personal Data or measures authorizing access by public authorities, do not prevent it from fulfilling its obligations under this Data Protection Procedure.

For the sake of clarity, laws and practices that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR, are not in contradiction with the Data Protection Procedure.

4.3 Assessment of local laws and practices when transferring Personal Data to Third Countries

In assessing the laws and practices of the Third Country which may affect the respect of the commitments contained in the Data Protection Procedure, Aker Solutions has taken due account, in particular, of the following elements:

a) The specific circumstances of the Transfers or set of Transfers, and of any envisaged onward Transfers within the same Third Country or to another Third Country, including:
    a. Purposes for which the Personal Data are Transferred and processed (e.g. marketing, HR, storage, IT support, clinical trials);
    b. Types of entities involved in the Processing (the Data Importer and any further recipient of any onward Transfer);
    c. Economic sector in which the Transfer or set of Transfers occur;
    d. Categories and format of the Personal Data Transferred;
    e. Location of the Processing, including storage; and
    f. Transmission channels used.
b) The laws and practices of the Third Country of destination relevant in light of the circumstances of the Transfer, including those requiring to disclose data to public authorities or authorizing access by such authorities and those providing for access to these data during the transit between the country of the Data Exporter and the country of the Data Importer, as well as the applicable limitations and safeguards.
c) Any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under the Data Protection Procedure, including measures applied during the transmission and to the Processing of the Personal Data in the country of destination.

4.4 Consultation

Where any safeguards in addition to those envisaged under the Data Protection Procedure should be put in place, Aker Solutions AS Aker, as the liable BCR member cf. Section 3.1.3, and the Group Privacy Officer will be informed and involved in such assessment.

4.5 Obligation to document the assessment

Aker Solutions must document appropriately such assessment, as well as the supplementary measures selected and implemented. The documentation must be made available to the competent Data Protection Authorities upon request.

4.6 Notification to the Data Exporter and supplementary measures

The Data Importer must promptly notify the Data Exporter if, when using this Data Protection Procedure as a tool for Transfers, and for the duration of the BCR membership cf. Section 3.7, it has reasons to believe that it is or has become subject to laws or practices that would prevent it from fulfilling its obligations under the Data Protection Procedure, including following a change in the laws in the third country or a measure (such as a disclosure request). This information shall also be provided to Aker Solutions AS.

Upon verification of such notification, the Data Exporter, along with Aker Solutions and the Group Privacy Officer, shall commit to promptly identify supplementary measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the Data Exporter and/or Data Importer, in order to enable them to fulfil their obligations under the Data Protection Procedure. The same applies if a Data

Exporter has reasons to believe that its Data Importer can no longer fulfil its obligations under this Data Protection Procedure.

4.7 Suspension of transfers

Where the Data Exporter, along with Aker Solutions AS and the Group Privacy Officer, assesses that the Data Protection Procedure – even if accompanied by supplementary measures – cannot be complied with for a Transfer or set of Transfers, or if instructed by the competent Data Protection Authorities, it commits to suspend the Transfer or set of Transfers at stake, as well as all Transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the Transfer is ended.

Following such a suspension, the Data Exporter has to end the Transfer or set of Transfers if the Data Protection Procedure cannot be complied with and compliance with the Data Protection Procedure is not restored within one month of suspension. In this case, Personal Data that have been Transferred prior to the suspension, and any copies thereof, shall, at the choice of the Data Exporter, be returned to it or destroyed in their entirety.

5 Government access requests

5.1 Notification of government access request

Without prejudice to the obligation of the Data Importer to inform the Data Exporter of its inability to comply with the commitments contained in Section 5, the Data Importer will promptly notify the Data Exporter and, where possible, the Data Subjects (if necessary with the help of the Data Exporter) if it:

a) Receives a legally binding request by a public authority under the laws of the country of destination, or of another Third Country, for disclosure of Personal Data Transferred pursuant to the Data Protection Procedure; such notification will include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided;

b) Becomes aware of any direct access by public authorities to Personal Data Transferred pursuant to the Data Protection Procedure in accordance with the laws of the country of destination; such notification will include all information available to the Data Importer.

5.2 Demonstration of best effort to waive prohibition to notify

If prohibited from notifying the Data Exporter and / or the Data Subjects, the Data Importer will use its best efforts to obtain a waiver of such prohibition, with a view to communicate as much information as possible and as soon as possible, and will document its best efforts in order to be able to demonstrate them upon request of the Data Exporter.

5.3 Information regarding the request

The Data Importer will provide the Data Exporter, at regular intervals, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If

the Data Importer is or becomes partially or completely prohibited from providing the Data Exporter with the aforementioned information, it will, without undue delay, inform the Data Exporter accordingly.

The Data Importer will preserve the abovementioned information for as long as the Personal Data are subject to the safeguards provided by the Data Protection Procedure and shall make it available to the competent Data Protection Authorities upon request.

5.4 Consideration of the legality of and challenging the request

The Data Importer will review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and will challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law, and principles of international comity.

The Data Importer will, under the same conditions, pursue possibilities of appeal. When challenging a request, the Data Importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the Personal Data requested until required to do so under the applicable procedural rules.

5.5 Documentation of assessment and challenge of the request

The Data Importer will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Data Exporter. It will also make it available to the competent Data Protection Authorities upon request.

5.6 Limitation of disclosure

The Data Importer will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

5.7 Prohibition against massive, disproportionate and indiscriminate Transfers

Transfers of Personal Data by Aker Solutions to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

6 Non-compliance

No Transfer can be made to Aker Solutions ASA or a Business Unit unless it is effectively bound by the Data Protection Procedure and can deliver compliance.

The Data Importer shall promptly inform the Data Exporter if it is unable to comply with the Data Protection Procedure, for whatever reason, including the situations further described under Section 5.

Where the Data Importer is in breach of the Data Protection Procedure or unable to comply with them, the Data Exporter shall suspend the transfer.

The Data Importer shall, at the choice of the Data Exporter, immediately return or delete the Personal Data that has been transferred under the Data Protection Procedure in its entirety, where:

a) The Data Exporter has suspended the Transfer, and compliance with this Data Protection Procedure is not restored within a reasonable time, and in any event within one month of suspension; or
b) The Data Importer is in substantial or persistent breach of the Data Protection Procedure; or
c) The Data Importer fails to comply with a binding decision of a competent court or competent Data Protection Authority regarding its obligations under the Data Protection Procedure.

The same commitments shall apply to any copies of the Personal Data. The Data Importer shall certify the deletion of the data to the Data Exporter. Until the data is deleted or returned, the Data Importer shall continue to ensure compliance with the Data Protection Procedure.

In case of local laws applicable to the Data Importer that prohibit the return or deletion of the Transferred Personal Data, the Data Importer shall warrant that it will continue to ensure compliance with the Data Protection Procedure and will only Process the Personal Data to the extent and for as long as required under that local law.

7 Termination

If a Data Importer ceases to be bound by the Data Protection Procedure, cf. Section 3.7, it may keep, return, or delete the Personal Data received under the Data Protection Procedure. If the Data Exporter and Data Importer agree that the data may be kept by the Data Importer, protection must be maintained in accordance with Chapter V GDPR.

8 Group Liability

Aker Solutions ASA has appointed Aker Solutions AS to take on the responsibility for any damages resulting from the violation of the BCR made by Business Units established outside the EEA. Further, it takes on the responsibility of taking necessary action in order to remedy the acts of such Business Unit, and, where appropriate to pay compensation for any material or non-material damages resulting from the violation of the BCR by any Business Unit bound by the rules herein.

Where the Data Subjects can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of a violation of the BCR, Aker Solutions AS takes on the responsibility of demonstrating that the Business Unit situated outside the EEA is not liable for the violation resulting in the damage claimed by the Data Subject.

Where Aker Solutions AS can prove that the Business Unit is not responsible for the breach of the BCR resulting in the damage claimed by the Data Subject, it may discharge itself from any responsibility.

If a Business Unit outside the EEA violates the BCR, the courts or other judicial authorities in the EEA will have jurisdiction, and Data Subjects will have the rights and remedies against Aker Solutions AS as if the violation had been caused by the latter in Norway, instead of the Business Unit outside the EEA.

9 Definitions

Term	Definition
Aker Solutions	Aker Solutions shall mean Aker Solutions ASA and its subsidiaries set out in the list of members for which the BCR applies. For the purpose of this procedure, the term “Aker Solutions” refers to all companies in the list of BCR members collectively or each of the companies on the list as the case may be
Applicable law	Applicable Law shall mean the law applicable to Aker Solutions ASA and/or the Business Unit. Applicable EU/EEA Law refers only to EU, national or local law in the EEA applicable to Aker Solutions ASA and/or the Business Unit. Applicable EU/EEA Data Protection Law refers to EU, national or local law in the EEA regarding data protection applicable to Aker Solutions ASA and/or the Business Unit.
Binding Corporate Rules (BCR)	BCR means this Data Protection Procedure.
Business Unit	Business Unit shall mean Aker Solutions ASA and subsidiaries set out in the list of members for which the BCR applies.
Consent	Consent means any freely given, specific, informed and unambiguous indication of a Data Subject's wishes by which the Data Subject, by a statement or a clear affirmative action, signifies his/her agreement to the Processing of Personal Data relating to him/her.
Controller	The Controller means the natural or legal person, e.g. Aker Solutions ASA and/or a Business Unit, which alone or jointly with others determines the purpose and means of the Processing of Personal Data
Data Exporter	Data Exporter means the Controller or Processor exporting/transferring the Personal Data to a Third Country.

Data Importer	Data Importer means the Controller or Processor importing the Personal Data to a Third Country.
Privacy Officer	A position within Aker Solutions, implemented to oversee and ensure compliance and supervision of compliance of the Data Protection Procedure. See roles and responsibilities in Section 3.3.
Data Subject	An identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. A Data Subject may for example be an employee or contractor of Aker Solutions, a client or supplier representative, a person applying for a job at Aker Solutions or subscribing to information by entering information on Aker Solutions' website or a representative from a business partner of Aker Solutions.
EEA	The European Economic Area, meaning the EU member states together with the EFTA countries Liechtenstein, Iceland and Norway.
GDPR	The GDPR shall mean the EU General Data Protection Regulation 2016/679.
Joint Controllers	Joint Controllers shall mean the situation where two or more Controllers jointly determine the purposes and means of the Processing.
Personal Data	Personal Data means any information relating to an identified or identifiable individual (the "Data Subject"). Personal Data includes all types of information that directly or indirectly may be linked to the Data Subject.
Personal Data Breach	Personal Data Breach shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed
Processor	A natural or legal person, public authority, agency or other body, which Processes the Personal Data on behalf of the Controller, for

	example an outsourcing partner or service provider which Processes Personal Data on behalf of a Business Unit.
Special Categories of data (sensitive data)	Special categories of data are Personal Data revealing or concerning: - Racial or ethnic origin - Political opinions - Religious or philosophical beliefs - Trade union membership - Genetic data - Biometric data for the purpose of uniquely identifying a Data Subject - Health - Sex life or sexual orientation
Third Countries	Third Countries shall mean countries outside the European Economic Area (EEA), i.e. all countries except the EU member states and the EFTA countries Liechtenstein, Iceland and Norway.
Transfer	For the purpose of this Data Protection Procedure, Transfer shall mean the situation where: a) A Controller or a Processor ("Data Exporter") is subject to the GDPR for the given Processing; b) The Data Exporter discloses by transmission or otherwise makes Personal Data, subject to this Processing, available to another Controller, joint Controller or Processor ("Data Importer"); and c) The Data Importer is in a Third Country, irrespective of whether or not this importer is subject to the GDPR for the given Processing in accordance with GDPR Article 3 or is an international organization.
Onward Transfer	For the purpose of this Data Protection Procedure, Onward Transfer shall mean the situation where Personal Data have previously been Transferred under the Data Protection Procedure, and a Business Unit discloses or otherwise makes the Personal Data available to an external Controller or Processor outside the EEA not bound by the Data Protection Procedure.