Data Protection Standard

Processing and Transfer of Personal Data in Aker Solutions

(Binding Corporate Rules)

Table of contents

1 Introduction

1.1 Scope

This Data Protection Standard contains a set of legally binding rules within Aker Solutions which provide principles for Processing of Personal Data within the company group. The Data Protection Standard applies to all Processing of Personal Data in Aker Solutions.

The Data Protection Standard applies to Aker Solutions ASA and its subsidiaries (including partly owned subsidiaries where Aker Solutions ASA directly or indirectly controls more than 50% of the voting interest). For the purpose of this standard, the term “Aker Solutions” refers to the whole company group or each of the companies as the case may be.

The Data Protection Standard is part of Aker Solutions People Policy, and applies to all personnel employed in Aker Solutions and the Business Units. In addition, third parties such as customers, contractors and others shall benefit from the rights granted to them herein.

The Data Protection Standard has two main purposes:

- Establishing a legal basis for authorization of transfer of Personal Data from Business Units established within the EEA to Business Units established outside the EEA (Third Countries).
- Ensure effective compliance (internal control) with the EU Data Protection Directive and the Norwegian Personal Data Act regarding Processing of all Personal Data in Aker Solutions.

1.2 Data Protection

Data Protection is about providing people with the right to control the use of any information concerning themselves, such as name, telephone numbers, preferences etc.

The Data Protection Standard is based on the Norwegian Personal Data Act and the EU Directive 95/46/EC. This legislation imposes certain requirements on the Processing of Personal Data. While conducting its day-to-day business Aker Solutions processes Personal Data about its employees, customers, business contacts and others.

The EU Directive does not allow for the transfer of personal information to countries outside the EEA (so-called third countries) which do not ensure an adequate level of data protection. Aker Solutions has Business Units placed in many countries where such requirements for an adequate level do not exist under local law. The purpose of the Data Protection Standard is to ensure that the Processing of Personal Data has such adequate level of protection.

The Data Protection Standard provides a legal basis (Binding Corporate Rules) for Data Protection Authorities in the EEA member states to authorise transfer of Personal Data from Business Units within the EEA to subsidiaries in third countries. Each Business Unit will be the controller deciding the means and purposes of the Processing for its company. The controller who transfers the Personal Data will be the data exporter, and the Business Unit established in a third country receiving the Personal Data from the data exporter, will be the data importer.

Aker Solutions’ Data Protection Standard is based on the following data protection principles:

- The Processing of Personal Data shall take place in a fair and lawful way.
- The collecting of Personal Data shall only be made for explicit and legitimate purposes and the use of them shall be made accordingly.
- The collecting of Personal Data shall be relevant and not excessive in relation to the purpose for which they are processed.
- The Personal Data shall be kept accurate and where necessary, up to date.
- Personal Data shall not be held longer than necessary.
- All Personal Data shall be kept confidential and stored in a secure way.
- Personal Data shall not be shared with third parties except when necessary in order for them to provide services upon agreement.
- Data Subjects shall have the right of access to and rectification of own Personal Data.

The routines described herein are supplementary to the security measures made in the Information Security Policy, and the Data Protection Standard has set out requirements for many of the routines established in the Information Security Policy.

1.3 Responsibility

This Data Protection Standard is part of the People Policy, and is as such under the responsibility of Corporate HR. Corporate HR is responsible for ensuring that the Data Protection Standard is applied in all Business Units. Each Local Data Protection Officer is responsible for the implementation of the Data Protection Standard. All employees are responsible for adhering to this standard.

Within the authority limits in Aker Solutions, and subject to local laws and regulations, the Business Units are responsible for all strategic and operational matters related to the day-to-day management of their business. It is the Business Unit's management's responsibility that the operations within the respective Business Units are conducted in compliance with the Data Protection Standard. This includes the responsibility for ensuring the establishment and maintenance of internal control procedures and update procedures in case of deficiencies, as outlined in this Data Protection Standard. In a situation where a Data Subject files a complaint because of a breach of the Data Protection Standard, the Business Unit that has made the breach shall be responsible for taking the necessary steps to become compliant with the Data Protection Standard, see complaint mechanism referred to in Section 3.5.

1.4 Definitions

1.4.1 Aker Solutions

Aker Solutions shall mean Aker Solutions ASA and its subsidiaries (including partly owned subsidiaries where Aker Solutions ASA directly or indirectly controls more than 50% of the voting interest). For the purpose of this standard, the term "Aker Solutions" refers to the whole company group or each of the companies as the case may be.

1.4.2 Binding Corporate Rules (BCR)

BCR is a set of rules which provides a suitable level of protection of Personal Data, in compliance with the European Directive 95/46 dated 24 October 1995. The purpose of these rules is to ensure an adequate level of protection of Personal Data in the Business Units situated in countries which are not members of the European Economic Area (EEA), Third Countries, in order to allow the Transfer of Personal Data from any Business Unit located within the EEA to a Business Unit located in a Third Country.

1.4.3 Business Unit

Business Unit shall mean all subsidiaries of which Aker Solutions ASA either directly or indirectly controls more than 50% of the voting interest.

1.4.4 Consent

Consent means any freely given specific and informed indication of his or her wishes by which the Data Subject signifies his/her agreement to Personal Data relating to him/her being processed and in accordance with the interpretation of the term "consent" as stated in WP 187 (Opinion 15/2011).

1.4.5 Controller

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.

1.4.6 Data Protection Officer

A position within Aker Solutions, implemented to oversee and ensure compliance and supervision of compliance of the Data Protection Standard. There is one Global Data Protection Officer and several Local Data Protection Officers. Please see section 3.4 for further details.

1.4.7 Data Subject

An identified or identifiable individual to whom the Personal Data being processed relates to, for example an employee of Aker Solutions, a person applying for a job at Aker Solutions by entering information on Aker Solutions' web site or a representative from a business partner of Aker Solutions.

1.4.8 EEA

The European Economic Area, meaning the EU member states together with the EFTA countries (Liechtenstein, Iceland and Norway).

1.4.9 Personal data

Personal Data means any information that may be related to an identified or identifiable individual (the "Data Subject"). An identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Personal Data includes all types of information that directly or indirectly may be linked to the Data Subject.

Personal data may include:

- Names and dates of birth
- Contact details such as addresses, e-mail addresses and telephone numbers
- Indirect information such as IP address, laptop name
- Expressions of opinions on living individuals
- Information concerning salary
- Client/Customer information (if linked to an individual)

For example, an IP address is deemed as Personal Data as long as the IP address in conjunction with additional information (such as an internet provider's billing information) can identify the individual using the IP address. Encrypted information is also deemed to be Personal Data if the information can be made readable and therefore identifies an individual.

1.4.10 Processing

Any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, alignment, storage and disclosure, or a combination of such use.

The definition is technology-neutral and includes the Processing of Personal Data that is wholly or partly performed with the aid of computers or similar equipment that is capable of automatically Processing Personal Data. The definition also includes manual registers or filing systems if the Personal Data is included in, or is intended to form part of, a structured collection making the Personal Data available for searching or compilation according to specific criteria.

1.4.11 Processor

Any natural or legal person, which processes the Personal Data on behalf of the Controller, for example an outsourcing partner or service provider of a Business Unit which processes Personal Data on behalf of the Business Unit. Frontica is a Processor for Aker Solutions, cf. Section 2.3.

1.4.12 Sensitive Data

Sensitive Data is defined as Personal Data concerning:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs
- trade union membership,
- health,
- sexual preference
- offences and criminal convictions

1.4.13 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).

1.4.14 Transfer

For the purpose of this Data Protection Standard, Transfer shall mean any Personal Data disclosure, copy or move via a network, or any Personal Data disclosure, copy or move from one medium to another irrespective of type of medium in accordance with article 25 and 26 of Directive 95/46/EC. The Business Unit who transfers the Personal Data will be the data exporter.

2 Description of the companies and Processing regulated by the Data Protection Standard

2.1 Material and geographical scope

The Data Protection Standard applies to Aker Solutions ASA and its subsidiaries (including partly owned subsidiaries where Aker Solutions ASA directly or indirectly controls more than 50% of the voting interest).

The official list of Aker Solutions Business Units and their location is maintained on a monthly basis by Corporate Legal. To get a copy of the current version, please contact Corporate Legal.

The Data Protection Standard applies to all Processing of Personal data in Aker Solutions.

2.2 Categories of Personal Data and purpose of the data Processing

Aker Solutions processes the following main categories of Personal Data, both concerning employees and third parties:

- General contact information: (e.g. name, address, email address, phone number, picture, date of birth etc)
- Employee - other information:
  - Key information necessary for the employment management, e.g. salary information, CV, education level, performance reviews, recruitment information, union membership, bank account number, details of next of kin etc)
  - Registration of hours worked, absences, holiday, overtime
  - Records of compulsory training, e-learning, and safety certificates
  - Employment history within Aker Solutions: e.g. start date, company and corporate seniority, job grade, position, organizational unit (department), immediate superior, contract details, employee type, job location, leaving date etc.
  - Other employee data for statistical purposes: (e.g. gender, nationality, age)
- Customer information (e.g. name, address, email address, phone number, picture etc)
- Sub-contractor's information (e.g. name, address, email address, phone number, picture etc)
- IT-related information (electronic logs regarding a person's use of IT-resources, user profile/account information etc)

The Processing has the following main purposes:

- Contact information
- Employee administration
- Customer administration
- Sub-contractors administration
- IT administration and information security administration
- Authentication and authorization
- Physical security
- Administer IT-costs per employee, and internal CRM-information
- Register and report on HSE related information (e.g. incidents, issues etc)
- Support the recruitment process (e.g. registering applications and CVs etc)

- Collaboration tool for internal projects and organizational teams and activities (e.g. document and content management)
- Provide input to the organization regarding trends and reasons for leaving the company (e.g. exit interview)

A detailed list of Processing purposes is available on the Data Protection Site (shared services portal). The list shall be updated annually as part of the procedures to update the Data Protection Standard, cf. Section 3.8.

An overview of information registers and data flow is set on the Data Protection Site (shared services portal).

2.3 Frontica as main data Processor for Aker Solutions

Aker Solutions has authorized Frontica (formerly known as Aker Business Services) to operate and deliver IT services, facilities management, finance, HR and administration management services to Aker Solutions' Business Units worldwide.

When providing services to Aker Solutions, Frontica regularly processes Personal Data on behalf of Aker Solutions' Business Units. In the course of receiving such services from Frontica, Personal Data will be transferred back and forth between each Business Unit and Frontica on a regular basis.

As a general rule each Business Unit will be the Controller deciding the means and purposes for the Processing, while Frontica will be the Processor which processes data on behalf of the Business Units.

As a Controller each Business Unit in Aker Solutions has an obligation to sign a data processing agreement with Frontica. For this purpose the parent company, Aker Solutions ASA, has entered into a Main Data Processing Agreement with Frontica. The Main Data Processing Agreement is entered into by accession letters by each Aker Solutions Business Unit as Controllers.

The Main Data Processing Agreement is made available as a template on the Data Protection Site (shared services portal).

During the performance of its tasks as Processor for Aker Solutions' Business Units, Frontica is obliged to treat each Business Unit as independent entities and to keep the respective Personal Data adequately and securely separated. Being a wholly owned subsidiary of Akastor ASA, Frontica is also obligated to comply with Akastor ASA's Data Protection Standard (BCR).

To the extent Frontica uses subcontractors to fulfil the obligations according to the Main Data Processing Agreement; Frontica shall ensure that the subcontractor undertakes corresponding responsibilities. This is accomplished by Frontica signing agreements with its suppliers on terms equivalent to the Main Data Processing Agreement.

See template "Example Data Processing Agreement with Subcontractor" available on the Data Protection Site (shared services portal).

The performance and quality of each service offered by Frontica is regulated in separate Service Level Agreements (SLAs) which is entered into between Aker Solutions' Business Units and Frontica. The SLAs have an important function with regard to describing the Processing of Personal Data by detailing the following key elements of the Processing:

- The categories of Personal Data being processed
- The categories of Sensitive Data being processed
- The purpose of the Processing
- Whether security graded information is being processed

The SLAs shall be electronically available in a database (ARCA) which gives an overview of the Processing of Personal Data by Aker Solutions' Business Units as controllers, and Frontica as a Processor. The database effectively supports the overview of the Processing by providing the possibility of sorting the SLAs based on the four elements mentioned above.

In a situation where Frontica uses a subcontractor in a third party country involving transfer to this subcontractor of information exported from an EEA country, Aker Solutions is responsible for ensuring that the legal grounds for the transfer of the personal data is in place. This may be accomplished by giving Frontica a clear mandate to sign the Model Clauses 2010/87/EU with the non-EEA-based subcontractor in the name and on behalf of Aker Solutions.

2.4 Aker Solutions' use of other data Processors than Frontica

When Aker Solutions contracts with external service providers other than Frontica for the delivery of services involving Processing of Personal Data on behalf of Aker Solutions, a data Processing agreement adapted for the conditions shall be signed.

See template "Example Data Processing Agreement – External Service Provider" available on the Data Protection Site (shared services portal).

3 Key principles of the Data Protection Standard

3.1 The duty to respect the Data Protection Standard

Aker Solutions ASA's and its subsidiaries' commitment to comply with the Data Protection Standard and related Tools is established by their signing of Agreement regarding bindingness of Aker Solutions' Data Protection Standard (Binding Corporate Rules). Se Agreement regarding bindingness available on the Data Protection Site (shared services portal).

Aker Solutions' employees are bound by the rules in this standard. This is achieved by way of specific obligations contained in a contract of employment as well as in the personnel handbook and by linking observance of the standard with disciplinary procedures and sanctions, cf. Section 3.3.

3.2 Data Subjects' rights

3.2.1 Beneficiary rights

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

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

- Fair and lawful Processing
- Purpose limitation

- Data quality and proportionality
- Criteria for making the Processing legitimate
- Transparency and easy access to the Data Protection Standard
- Rights of access, rectification, erasure and blocking of data
- Right to object to the Processing
- Security and confidentiality
- Restrictions on onward transfers outside of the group of companies
- National legislation preventing respect of the Data Protection Standard
- Right to complain through the internal complaint mechanisms of the companies
- Cooperation duties with Data Protection Authority
- Liability and jurisdiction provisions

Data Subjects' queries and complaints shall be handled in a timely manner by the relevant Local or Global Data Protection Officer in accordance with internal procedures, as set out in the Data Protection Standard Complaint Mechanism, cf. Section 3.5.

If a Data Subject has suffered harm due to a breach of his or her rights under the Data Protection Standard and the complaint has not been handled by Aker Solutions in a sufficient manner, the Data Subject may take its case either to

- the Competent Authority or the court where the EEA subsidiary that originated the transfer is based, or
- the Competent Authority or the court of Aker Solutions AS (the EU Headquarters) in Norway

3.2.2 Information about Data Subjects' rights

All Data Subjects who benefit from the Data Protection Standard shall have easy access to information describing the rights. Information shall be provided in the following documents:

- Code of Conduct:
  A public available and practical guidance on how to protect Personal Data when conducting business for Aker Solutions will be published on the website of Aker Solutions as part of the Code of Conduct. The statement "Caring about Privacy-document" will contain the main elements of the Data Protect Standard.
- Aker Solutions' Privacy Statement:
  The Privacy Statement is available at akersolutions.com and apply to the online activities of the company. A link is provided from the Privacy Statement to the Public Version of the Data Protection Standard.
- The Public Version of the Data Protection Standard:
  A public version of this Data Protection Standard shall be available online. It explains Aker Solutions Binding Corporate Rules (BCR) for Processing Personal Data, the legal basis for transferring Personal Data to third countries and affected Data Subjects' rights pursuant to these rules.

3.2.3 Liability

Any Data Subject shall benefit from the remedies and liability provided for in Articles 22 and 23 of the EU Directive and under Norwegian law.

Aker Solutions ASA has appointed Aker Solutions AS to take on the responsibility for any damages resulting from the violation of the Data Protection Standard made by the Business Units. Further, it takes on the responsibility of taking necessary action in order to remedy the acts of a Business Unit, and, where

appropriate to pay compensation for any damages resulting from the violation of the Data Protection Standard by any Business Unit bound by the rules herein. Head of Corporate Legal shall be contacted in case of a potential legal action.

The burden of proof lies with Aker Solutions and not the Data Subject. Hence, for the benefit of the Data Subject, Aker Solutions ASA takes on the responsibility of demonstrating that the Business Unit situated outside the EU 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 Data Protection Standard resulting in the damage claimed by the Data Subject, it may discharge itself from any responsibility.

3.3 Training and awareness program

The training and awareness program within Aker Solutions sets up a system which guarantees implementation and a good level of compliance with the Data Protection Standard in Business Units both inside and outside the European Union. The aim of appropriate training is to make the Data Protection Standard known, understood and effectively applied throughout the group of companies.

3.3.1 Data Protection Standard:

The issuing of this Data Protection Standard as part of the corporate governance structure of Aker Solutions is an important measure in the process of achieving sufficient data privacy safeguards amongst all employees.

3.3.2 Contracts of employment/personnel handbook:

Employees are bound by the rules in this Data Protection Standard. This is achieved by way of specific obligations contained in a contract of employment as well as in the Personnel Handbook and by linking observance of the Data Protection Standard with disciplinary procedures.

- Contracts for all new personnel contain the following text:

  "The Employee's Personal Data shall be processed in a fair and lawful way. Personal Data considered as relevant contact information will be visible to other employees within the Group when necessary for the purpose of common it-systems etc.

  Any Processing of Personal Data must be in accordance with Aker Solutions People Policy and the Data Protection Standard. Failure to comply with the data privacy rules may cause disciplinary actions."

- The Personnel Handbook contains a separate chapter providing a general overview of the principles in the Data Protection Standard and the related tools. In the Handbook it is stated that all personnel are required take the outmost account to ensure that Personal Data is processed only for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Personal data must be dealt with in a fair and lawful way and in accordance with the Data Protection Standard and the related tools.

3.3.3 Introduction courses:

Awareness for new employees is accomplished through a mandatory introduction program. The program is conducted on an Internet-based platform which covers several corporate matters, including information and training regarding data protection in Aker Solutions.

3.3.4 Awareness through eLearning and Arena:

A special training program is mandatory for personnel who have permanent or regular access to Personal Data as well as for personnel who are involved in the collection of Personal Data or in the development of tools used to process data. The special training program involves basis courses based on eLearning explaining the principles set out in the Data Protection Standard and involving guidelines for Prosessing of Personal Data. The special training course will be combined with ”reaccuring” information sessions.

Further, all employees have at all times the relevant information available online via Arena combined with information presented via relevant communication channels to create awareness among all employees (office and non-office workers) of individual rights and duties considering Processing of Personal Data.

3.3.5 HR Network:

Information and general overview of obligations and duties according to the Data Protection Standard will be provided to the People Policy Owner and to the Global and each Local Data Protection Officers through relevant and targeted training programs facilitated by HR Network.

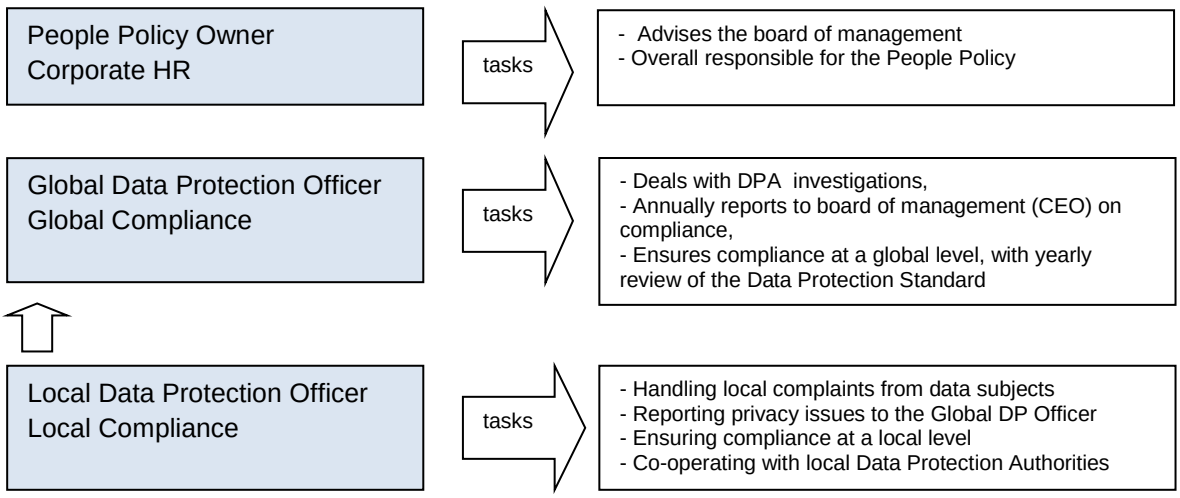
3.4 Compliance and supervision of compliance

The Data Protection Standard has several measures to ensure compliance and supervision of compliance. This includes:

- The appointment of one Global Data Protection officer
- The appointment of one Local Data Protection Officer for each Business Unit or Region
- Establishment of internal control mechanisms - ongoing monitoring
- Review program

3.4.1 HR and Data Protection Officers

Aker Solutions has appointed the following positions to oversee and ensure compliance with the rules of this Data Protection Standard:



The Global Data Protection Officer is granted an appropriate level of independency in the exercise of his functions. The Global and/or Local Data Protection Officers shall be the contact persons for most matters arising under this Data Protection Standard. Please see further description of these positions' responsibilities in the Guidelines for the Data Protection Officers.

3.4.2 Ongoing monitoring

Business Units in Aker Solutions shall structure their internal control systems to monitor themselves on an ongoing basis. The monitoring procedures for this Data Protection Standard shall be built into the normal, recurring operating activities for each Business Unit, as stated in Aker Solutions Governance Policy.

All Business Units shall once a year conduct a Control Self-Assessment (CSA) process in order to certify compliance with all Aker Solutions' policies. Compliance with this Data Protection Standard shall be included in the yearly CSA procedure for each Business Unit/Region.

3.4.3 Review program

To ensure the enforcement of the Data Protection Standard, Aker Solutions shall make sure that a review of the rules herein shall take place each year, in accordance with Internal Control and Compliance Policy in Aker Solutions, namely the Compliance Review Process.

Each review is initiated by the Global Data Protection Officer, who also selects the venue for such review. The review program covers all aspects of the Data Protection Standard including methods of ensuring that corrective actions will take place.

The reviews shall be carried out by an internal Compliance Review team which will be at the Business Unit's premises to review the internal control structure and the implementation of the Data Protection Standard. The review will refer to the Business Unit's responses to the most recent Control Self-Assessment questionnaire.

All findings and the results of each review shall be communicated by issuing a Compliance Review Report, in which the Business Unit has certain control issues to respond to. Such report shall be communicated in accordance with the Compliance Review Process, as well as to both the Global and Local Data Protection Officers.

Upon request, the relevant Data Protection Authorities may receive a copy of the results of such review. The relevant Data Protection Authority may also conduct data protection reviews themselves.

3.5 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 Standard by making a complaint about this.

If the Data Subject is an employee, he or she may choose to bring the complaint to the local HR representative or to his or her manager, or he or she may choose to contact the Local Data Protection Officer or the Global Data Protection Officer. If the Data Subject is a third party beneficiary, the Data Subject may take its case to the Global Data Protection Officer.

Please see Data Protection Standard Complaint Mechanism Tool published on the Data Protection Site (Shared Services Portal), for processes and further information.

In the case the Data Subject does not receive a reply and a solution in a sufficient manner, the Data Subject may take its case either to

- the Competent Authority or the court where the EEA subsidiary that originated the transfer is based, or
- the Competent Authority or the court of Aker Solutions AS (the EU Headquarters) in Norway.

Please see Data Protection Standard Complaint Mechanism for further details.

3.6 Mutual assistance and cooperation with Data Protection Authorities

Aker Solutions undertakes to cooperate with the Data Protection Authorities, particularly by applying recommendations and advice from the authorities, and also by responding to requests from the authority regarding the Data Protection Standard.

The Data Protection Authorities may conduct audits in order to ascertain compliance with the Data Protection Standard.

The Global Data Protection Officer and the Local Data Protection Officers shall be the main contact point between relevant Data Protection Authorities and Aker Solutions on any matter arising out of the Data Protection Standard or Processing of Personal Data in general. If such Data Protections Offices is not appointed locally, the main contact person locally shall be the CEO of the relevant company together with the Global Data Protection Officer.

3.7 Relationship between national laws and the Data Protection Standard

The Data Protection Standard is based on the EU Data Protection Directive 95/46/EC and the Norwegian Personal Data Act. The purpose of the Data Protection Standard is to ensure compliance with this legislation, and to ensure adequate safeguards for the transfers of Personal Data. However, the Data Protection Standard should not be considered as an instrument to replace EEA data protection laws.

If anything in the Data Protection Standard is in conflict with relevant local mandatory laws or regulations, the latter shall prevail.

Where an employee or a Business Unit in Aker Solutions has reasons to believe that the applicable legislation prevent the fulfilling of obligations under the rules of this Data Protection Standard, there is an obligation to promptly inform the Global Data Protection Officer or the Local Data Protection Officer (who will inform the Global Data Protection Officer). Necessary steps will be taken in order to assess whether changes need to be made to the Data Protection Standard. When in doubt, the Global Data Protection Officer shall consult Corporate Legal.

3.8 Procedure for updating the Data Protection Standard

Aker Solutions may make amendments to the Data Protection Standard, e.g. due to modifications of relevant legislation or changes to Aker Solutions Legal Structure..

Updates of the Data Protection Standard are possible without having to re-apply for authorization by the Data Protection Authorities, provided that:

- The Global Data Protection Officer keeps a fully updated list of members and keep track of and record of any updates to the rules and provide the necessary information to the Data Subjects or Data Protection Authorities upon request
- No Transfer of Personal Data is made to a new member until the exporter of the data has made sure that the new member is effectively bound by this Data Protection Standard, and can demonstrate compliance
- Any substantial changes to the Data Protection Standard or to the list of members are reported once a year to the Data Protection Authorities granting the authorizations with a brief explanation of the reason justifying the update

The current version of the Data Protection Standard shall always be available for all Business Units and employees.

Aker Solutions shall communicate any substantial modifications to the rules to the Data Subjects by making the necessary changes to all relevant documents including the Code of Conduct, the Privacy Statement and the Public version of the Data Protection Standard, cf. 3.2.2.

4 General privacy principles observed by Aker Solutions

The following general principles are in accordance with the principles of the EU Data Protection Directive 95/46/EC. Aker Solutions has by implementing this Data Protection Standard established a basis for internal control and procedures that ensures compliance with these principles when Processing Personal Data. It is the responsibility of each Business Unit as a Controller to apply such internal control and procedures.

Any inquiries concerning the general principles should be addressed to the Global or Local Data Protection Officer.

4.1 Fair and lawful Processing

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

4.2 Purpose specification

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

4.3 Data quality and proportionality

Personal Data shall be:

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

4.4 Criteria for making data Processing legitimate

4.4.1 Processing of Personal Data

Personal Data may be processed only if:

- the Data Subject has given his Consent; or
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract; or
- Processing is necessary for compliance with a legal obligation to which the controller is subject; or
- Processing is necessary in order to protect the vital interests of the Data Subject; or
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the Data Subject which require protection under Article 1 (1) of the European Data Protection Directive.

4.4.2 Processing of special categories of data (Sensitive Data)

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

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

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

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

4.4.3 National identification numbers

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

4.5 Information to be given to the Data Subject

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

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

- the identity of the Controller and of his representative, if any;
- the purposes of the Processing for which the data are intended;
- any further information such as
  - the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply
  - the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair Processing in respect of the Data Subject.

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

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

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

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

4.6 The Data Subject's right of access to data

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

- without constraint at reasonable intervals and without excessive delay or expense:

  - confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the Processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
  - confirmation to him in an intelligible form of the data undergoing Processing and of any available information as to their source,
  - knowledge of the logic involved in any automatic Processing of data concerning him at least in the case of automated decisions referred to in the Data Protection Standard Section 4.7.2;
- as appropriate the rectification, erasure or blocking of data the Processing of which does not comply with the provisions of this Data Protection Standard, in particular because of the incomplete or inaccurate nature of the data;
- notifications to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with b), unless this proves impossible or involves a disproportionate effort.

4.7 The Data Subject's right to object

4.7.1 The Data Subject's right to object to processing

The Data Subject has the right:

- at least in the cases referred to in Section 4.4.1 e) and f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the Controller may no longer involve those data;
- to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

4.7.2 Automated individual decisions

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

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

- is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the Data Subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or
- is authorized by a law which also lays down measures to safeguard the Data Subject's legitimate interests.

4.8 Confidentiality of Processing

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

4.9 Security of Processing

4.9.1 Appropriate technical and organizational security measures

The Controller must implement appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.

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

4.9.2 Use of Data Processor

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

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

- the Processor shall act only on instructions from the Controller,
- the obligations set out in 4.9.1 shall also be incumbent on the Processor.

See Section 2.3 and 2.4 regarding Aker Solutions' use of data Processors.

4.9.3 Documentation

For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in Section 4.9.1 and 4.9.2 shall be in writing or in another equivalent form.

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

4.10.1 Transfer from Controller to Controller

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

- it is not incompatible with the purpose for which the Personal Data were collected, cf. 4.2;
- it is in accordance with the principle of data quality and proportionality, cf. 4.3;
- the criteria for making Data Processing legitimate is fulfilled, cf. 4.4;
- if applicable, information is given to the Data Subject in accordance with 4.5.2;
- appropriate security measures protect the data during transfer and further Processing by the receiving Controller, cf. 4.9.

4.10.2 Transfer from Controller to Processor

Transfer of Personal Data from a Controller to a Processor, both bound by the Data Protection Standard, 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. 4.9.1;
- the carrying out of Processing by way of a Processor is governed by a contract or legal act binding the Processor to the Controller and stipulating in particular that:
  - the Processor shall act only on instructions from the Controller,
  - the obligations set out in 4.9.1 shall also be incumbent on the Processor.

See Sections 2.3 and 2.4 regarding Aker Solutions' use of data Processors.

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

4.11.1 Transfer to external Controllers established within the EEA

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

- it is not incompatible with the purpose for which the Personal Data were collected, cf. 4.2;
- it is in accordance with the principle of data quality and proportionality, cf. 4.3;
- the criteria for making data Processing legitimate is fulfilled, cf. 4.4;
- if applicable, information is given to the Data Subject in accordance with 4.5.2;
- appropriate security measures protect the data during transfer and further Processing by the receiving Controller, cf. 4.9.

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

4.11.2 Transfer to external Controller established outside the EEA

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

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

4.12 Transfer of Personal Data to external Processors

4.12.1 Transfer to external Processors established within the EEA

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

- the Processor provides sufficient guarantees in respect of the technical security measures and organizational measures governing the Processing to be carried out, cf. 4.9.2;

- the carrying out of Processing by way of a Processor is governed by a contract or legal act binding the Processor to the Controller and stipulating in particular that:
  - the Processor shall act only on instructions from the Controller,
  - the obligations set out in 4.9.1, cf. the Data protection directive art 17, shall also be incumbent on the Processor.

See Sections 2.3 and 2.4 regarding Aker Solutions' use of Data Processors.

4.12.2 Transfer to external Processor established outside the EEA

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

- the receiving 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; or
- the Processor is established in the US and has endorsed the Safe Harbour Principles; or
- one of the derogations in the Data Protection Directive article 26 applies;

and;

- the Processor provides sufficient guarantees in respect of the technical security measures and organizational measures governing the Processing to be carried out, cf. 4.9.2;
- the carrying out of Processing by way of a Processor is governed by a contract or legal act binding the Processor to the Controller and stipulating in particular that:
- the Processor shall act only on instructions from the Controller,
- the obligations set out in 4.9.1, cf. the Data protection directive art 17, shall also be incumbent on the Processor.

or

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

5 References

Policies: People Policy
Information Security Policy
Governance Policy

Standards: Standard 1 Information Security Standard
Standard 2 IT Acceptable Use Standards

Tools: Guidelines for Data Protection Officers
Processing and transfer of personal
CCTV Guidance

6 Revision Summary