Data Protection Procedure

Processing and Transfer of Personal Data in Aker Solutions

(Binding Corporate Rules)

© Aker Solutions

Table of contents

© 2018 Aker Solutions

© 2018 Aker Solutions

1 Introduction

1.1 Scope

This Data Protection Procedure 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 Procedure applies to all Processing of Personal Data in Aker Solutions.

The Data Protection Procedure 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 Procedure, the term “Aker Solutions” refers to the whole company group or each of the companies as the case may be.

The Data Protection Procedure is linked to Aker Solutions’ Information Security and Data Protection Policy, and applies to all personnel employed in Aker Solutions. In addition, third parties such as customers, contractors and others shall benefit from the rights granted to them herein.

The Data Protection Procedure has two main purposes:

- Establishing a legal basis for authorization of transfer of Personal Data from Business Units established within the European Economic Area (EEA) to Business Units established outside the EEA (Third Countries).
- Ensure effective compliance (internal control) with the EU General Data Protection Regulation 2016/679 (GDPR) regarding Processing of all Personal Data in Aker Solutions.

© 2018 Aker Solutions

1.2 Data Protection

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

This Data Protection Procedure is based on the Norwegian Personal Data Act and the GDPR. 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, contractors, business contacts and others.

The GDPR 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 Procedure is to ensure that the Processing of Personal Data has such adequate level of protection.

The Data Protection Procedure provides a legal basis (Binding Corporate Rules) for transfer of Personal Data from Business Units within the EEA to Business Units in Third Countries.

Aker Solutions' Data Protection Procedure is based on the following data protection principles:

- The Processing of Personal Data shall take place in a lawful, fair and transparent way.
- The collecting of Personal Data shall only be made for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- The collecting of Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which the Personal Data are processed.
- The Personal Data shall be kept accurate and where necessary, up to date. Every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed.
- All Personal Data shall be kept confidential and processed in a manner that ensures appropriate security of the Personal Data, inducing protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- Data Subjects shall have the right of objection, access to, rectification, erasure, restriction of processing and portability of own Personal Data.
- The Controller shall be responsible for, and be able to demonstrate compliance with, the data protection principles set out herein.

1.3 Responsibility

This Data Protection Procedure is linked to the Aker Solutions Information Security and Data Protection Policy, and is as such under the responsibility of the IT Function. The IT Function is responsible for ensuring that the Data Protection Procedure is applied in all Business Units. The Data Protection Organization, as described herein, is responsible for the implementation of the Data Protection Procedure. All employees are responsible for adhering to this Procedure.

Aker Solutions ASA and every Business Unit acting as Controller shall be responsible for and be able to demonstrate compliance with this Data Protection Procedure.

© 2018 Aker Solutions

1.4 Definitions

The following definitions shall have the same meaning as the relevant definitions set out in the GDPR.

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 procedure, 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 means Personal Data protection policies which are adhered to by Aker Solutions Business Units established on the territory of the EEA for transfers or a set of transfers of Personal Data to any (Aker Solutions) Business Unit located in one or more Third Countries. Aker Solutions' BCR is set out in this Data Protection Procedure.

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, 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.

1.4.5 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.

1.4.6 Data Privacy Officer

A position within Aker Solutions, implemented to oversee and ensure compliance and supervision of compliance of the Data Protection Procedure. There is one Group Privacy Officer and several Local Privacy Officers, in addition to appointed Privacy Champions, as the case may be. See roles and responsibilities in Section 3.3.

1.4.7 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.

1.4.8 EEA

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

© 2018 Aker Solutions

1.4.9 GDPR

The GDPR shall mean the EU General Data Protection Regulation 2016/679.

1.4.10 Joint Controllers

Joint Controllers shall mean the situation where two or more Controllers jointly determine the purposes and means of the Processing.

1.4.11 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 may include:

- Names, dates of birth, SAP ID, passport details
- Contact details such as addresses, e-mail addresses, telephone numbers, instant message identification and social media profiles
- Indirect information such as IP address and laptop name
- Expressions of opinions on living individuals
- Location data
- Information concerning salary and payment information
- Client and supplier 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.

1.4.12 Processing

Any operation or set of operations which is performed upon Personal Data or on sets of Personal Data, whether or not by automatic means, such as use, collection, recording, organisation, structuring, alignment or combination, adaptation or alternation, retrieval, consultation, dissemination, storage and disclosure by transmission or otherwise making available, restriction, erasure or destruction.

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.

1.4.13 Personal Data Breach

Personal Data Breach shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

© 2018 Aker Solutions

1.4.14 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.

1.4.15 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

1.4.16 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).

1.4.17 Transfer

For the purpose of this Data Protection Procedure, Transfer shall mean any Personal Data disclosure, copy or move via a network, access from a system or web application or any Personal Data disclosure, copy or move from one medium to another irrespective of type of medium from the EEA to a recipient outside the EEA. The Business Unit who transfers or discloses the Personal Data will be the data exporter.

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

2.1 Material and geographical scope

The Data Protection Procedure applies to Aker Solutions ASA and its subsidiaries worldwide (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 the Legal and Compliance function. To get a copy of the current version, please contact the said function.

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

2.2 Description of Processing regulated by the Data Protection Procedure

Aker Solutions processes the following main categories of Personal Data, concerning employees and their next of kin, clients, suppliers, contractors, newsletter subscribers, tenants, relatives, visitors, joint ventures and partners for the following main purposes:

© 2018 Aker Solutions

Data category	Purpose of Processing
HR management data such as general contact information, salary information, picture, social security number, passport number, organizational connections, pension and compensation information, project assignments, international assignments, offshore work and business travels, role, title, CV, education, competencies and skills, career and work experiences).This also includes data relating to development, performance objectives and reviews, talent and key resource information, recruitment information including background checking, union membership, bank account number, information related to ethics and code of conduct such as gifts received and conflict of interest, grievances, warnings, consents, agreements and confidentiality undertakings, organizational structuring, rightsizing and termination, participation in internal networking, knowledge sharing, IP registrations, details of next of kin, etc.	Recruitment, staffing, development of employees, talent management, succession planning, performance management and work force administration, including but not limited to internal work sharing, enabling collaboration for internal projects and organizational teams and activities (e.g. document and content management), tendering for work and project operation internally, authentication and authorization. Administer and manage all aspects of the employee relationship (including job applicants, former employees, temporary employees, employees, apprentices, students, contractors, consultants, next of kin and dependants.
Business-related data (for example business relations, business interest and security data, organizational connections, general contact information, picture etc.)	Support, administer and manage all aspects of the customer, supplier, joint venture or partner relationships (internal/external), processing of personal data as part of provision of products and services to third parties, tendering for work and project operation externally, business operation and protection of business interests and security (e.g. information security, logging, conduction of audits and controls, surveys, analysis, reports and managing of daily operations and transactions/possible transactions involving Aker Solutions).
IT-administration data (for example electronic logs regarding a person's use of IT-resources, user profile/account and application information etc.)	Support and manage information technology (IT) and information system (IS) administration and information security.
Audio and video recordings and related data	Internal communications, training and documentation through audio and video recordings.
HSE-related data (for example data relating to HSE incidents and safety certificates, incidents, issues, work environment, security, access control etc.)	Support and manage occupational health services and physical security, and the registration, managing and reporting of health, service and environment (HSE) related information (incidents, issues etc.).
Planning, control data and HR reports (for example registration of hours worked, absences and leaves, holiday, overtime, employment history within Aker Solutions, e.g. start date, Aker Solutions corporate seniority, job grade, position, organizational unit (department), immediate superior, contract details, employee type, job location, leaving date and records of compulsory and work-related training, e-learning and certificates, gender, nationality, age, height,	Internal control and planning, work force administration, scheduling time tables, recording time, conducting surveys and questionnaires, controls and internal audits, statistics, analysis, provide input to analytics and decision making related to the operations and the organization as such, organizational development, structure and rightsizing, and administer cost and finances related to staffing such as IT costs per employee, social costs, rates, office cost,

© 2018 Aker Solutions

weight and financial information such as rates and cost information etc.)	equipment cost, cost allocation, billing financial reporting.
Data relating to employees' participation or use of Aker Solutions' social activities, events or services.	Administer and manage social activities or events through internal arrangement or participation in organized activities such as cabin rental, equipment rental, Aker Extra, sport or social arrangements.
Background check and Integrity Due Diligence data (for example name, gender, age, roles in companies, information available in public available sources)	Due diligence investigations against anti-corruption laws and export controls, Integrity Due Diligence of business partners (including self-assessment and background check) and process requests for visits (visitors).
Video surveillance / activity logs (for example CCTV recordings, visiting registrations and access logs)	Support and manage safeguarding against illegal or unauthorized entry into areas, buildings or rooms or to support the control of equipment and/or production processes.
Complaints (for example name and contact information of complainant, audio recording of the complaint and contents of complaint)	Follow-up on complaints and concerns reported by employees to their supervisor or the Head of Compliance.
Whistleblowing, complaints and investigation information (for example the identity of notifying person, details on potential misconduct, information on alleged person(s) involved and information revealed as part of the investigation)	Whistleblowing hotline (available for employees and third parties) for raising concerns, managing internal investigations of incidents and concerns (e.g. related to employee's potential violation of terms of employment or incidents or concerns that may have an adverse effect on the business).
Data necessary to comply with legal obligations (for example tax and accounting information and information relating to legal proceedings)	Comply with legal obligations to which Aker Solutions is subject and/or protect a legal position of Aker Solutions.

2.3 Records of processing activities

Aker Solutions ASA and every Business Unit acting as Controller shall maintain a record of processing activities under its responsibility carried in accordance with GDPR Article 30(1).

The record shall be available to the Data Protection Authority on request.

3 Key principles of the Data Protection Procedure

3.1 Data Subjects' rights

3.1.1 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 minimisation, accuracy and storage limitation
- Criteria for making the Processing legitimate
- Transparency and easy access to the Data Protection Procedure

© 2018 Aker Solutions

- Rights of access, rectification, erasure, restriction of processing and blocking of data
- Right to data portability
- Right to object to the Processing
- Security and confidentiality
- Right to basic information related to Personal Data processing
- Restrictions on onward transfers outside of the group of companies
- National legislation preventing respect of the Data Protection Procedure
- Right to complain through the internal complaint mechanisms of the companies
- Cooperation duties with Data Protection Authority
- Rights in relation to automated decision making and profiling
- Liability and jurisdiction provisions

Data Subjects' queries and complaints shall be handled in a timely manner by the relevant Local or Group Privacy Officer in accordance with internal procedures, as set out in the Data Protection Procedure Complaint Mechanism, cf. Section 3.4.

3.1.2 Information about Data Subjects' rights

All Data Subjects who benefit from the Data Protection Procedure shall have easy access to information describing the rights. A public version of the Data Protection Procedure shall be available online on the Aker Solutions public internet site, providing information related to i.a. transfer of personal data and data subjects' rights.

The list of members of the BCR will be made available upon request to the Group Privacy Officer.

3.1.3 Liability

Aker Solutions ASA has appointed Aker Solutions AS to take on the responsibility for any damages resulting from the violation of the Data Protection Procedure 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 damages resulting from the violation of the Data Protection Procedure by any Business Unit bound by the rules herein. Head of the Legal and Compliance function shall be contacted in case of a potential legal action.

The burden of proof lies with Aker Solutions AS and not the Data Subject. Hence, for the benefit of the Data Subject, Aker Solutions AS 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 Procedure resulting in the damage claimed by the Data Subject, it may discharge itself from any responsibility.

3.2 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 Procedure in Business Units both inside and outside the EEA. The aim of appropriate training is to make the Data Protection Procedure known, understood and effectively applied throughout the group of companies.

© 2018 Aker Solutions

3.2.1 Introduction courses

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

3.2.2 Awareness through eLearning and applicable communications channel

A special training program is available 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 basic courses based on eLearning explaining the principles set out in the Data Protection Procedure 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 the Aker Solutions Intranet or applicable internal communications tools 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.

3.2.3 Targeted Training

Information and general overview of obligations and duties according to the Data Protection Procedure will be provided to the owners of the Information Security and Data Protection Policy and the People Policy and to the Group and each Local Privacy Officers through relevant and targeted training programs.

3.3 Compliance and supervision of compliance

3.3.1 Measures to ensure compliance and supervision of compliance

The Data Protection Procedure have several measures to ensure compliance and supervision of compliance, including:

- The appointment of one Group Privacy Officer overseeing and supervising the Group's compliance;
- The appointment of Local Privacy Officers for Business Units and regions, as appropriate, responsible for supervision and overview of local compliance;
- The appointment of appointed Privacy Champions responsible for overseeing and supervising compliance within the agreed scope of work.
- Establishment of internal control mechanisms and ongoing monitoring; and
- Review program.

The Group Privacy Officer shall be involved, properly and in a timely manner in all issues which relate to the protection of Personal Data, and is granted an appropriate level of independency in the exercise of his/her functions. The Group and/or Local Privacy Officers shall be the contact persons for most matters arising under this Data Protection Procedure. Please see further description of these positions’ responsibilities in the Guidelines for the Data Privacy Officers.

3.3.2 Owner of the Information Security and Data Protection Policy

The Owner of the Information Security and Data Protection Policy has the following tasks:

- Advises the board of management; and
- Overall responsible for the Information Security and Data Protection Policy.

© 2018 Aker Solutions

3.3.3 Group Privacy Officer *(Global Compliance)*

The Group Privacy Officer shall have the following tasks:

- Responsible for informing and advising the Group and its employees of their obligations pursuant to this Data Protection Procedure;
- Prepare annual compliance program for monitoring compliance
- Monitoring compliance with the Data Protection Procedure and the relevant sub-policies;
- Overall responsible for ensuring awareness-training and training of staff involved in processing operations and related audits;
- Coordinate and participate in Data Protection Impact Assessments and group risk assessments, provide advice where requested and follow up on actions from assessments;
- Co-operating with and being key contact point for the competent DPA and dealing with DPA investigations;
- Operates the Data Protection Organization;
- Deals with Personal Data Breach in cooperation with the Chief Information Security Officer;
- Regularly report to Executive Management Team and Audit Committee on compliance;
- Conduct yearly review and update of the Data Protection Procedure and BCR related documents;
- Coordinate global communication related to information to data subjects; and
- Deal with global issues or as escalated by the Local Privacy Officers.

3.3.4 Local Privacy Officer *(Local Compliance)*

The Local Privacy Officer shall have the following tasks:

- Handling local complaints from data subjects, access requests and other requests from data subjects related to the exercise of their individual rights;
- General reporting and reporting privacy issues to the Group Privacy Officer;
- Ensure local communication to data subjects and others;
- Follow-up and monitor changes in local laws and regulations and inform Group Privacy Officer when necessary;
- Plan and arrange necessary training for target groups and employees;
- Ensuring compliance at a local level; and
- Co-operating with local Data Protection Authorities.

3.3.5 Privacy Champions

If special Privacy Champions are appointed, these are additional to the Group Privacy Officer and Local Privacy Officers and shall be appointed for a limited scope or area such as a project, a process, a department etc.

The Privacy Champion shall be tasked with assisting Group or Local Privacy Officers whitin their scope of work according to instructions or mandate provided.

3.3.6 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 Procedure shall be build into the normal, recurring operating activities for each Business Unit, as stated in Aker Solutions Governance Policy and other applicable policies and procedures.

© 2018 Aker Solutions

Regular monitoring of compliance to the Data Protection Procedure shall be included in the Company's annual audit program and in the functional and organizational specific auditing programs. Risks related to data protection shall be included in the company's regular risk assessment.

3.3.7 Review program

To ensure the enforcement of the Data Protection Procedure, Aker Solutions shall make sure that a specific data privacy review, in addition to the annual Company audit program, of the rules herein, shall take place each year, in accordance with Company applicable policies and procedures related to governance, risk and internal control.

Each review is initiated by the Group Privacy Officer, who shall also select the venue for such review. The review program covers all aspects of the Data Protection Procedure 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 and compliance with the Data Protection Procedure.

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 Group and Local Privacy Officers and to the board of Aker Solutions ASA.

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.

3.4 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 complaint about this.

Employees may file a complaint to the local HR representative, to his or her manager, the Local Privacy Officer or the Group Privacy Officer. If the Data Subject is a third party beneficiary, the Data Subject may complain to the Group Privacy Officer.

Data Subjects' queries and complaints shall be handled in a timely manner by the relevant Local or Group Privacy Officer in accordance with internal procedures, as set out in the Data Protection Procedure Complaint Mechanism. Please see Data Protection Procedure Complaint Mechanism Tool published on the Aker Solutions' intranet 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.

In case of violation of this Data Protection Procedure or in the case the Data Subject does not receive a reply and 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 or the courts:

- in the EEA country at the origin of the Personal Data transfer, against the Business Unit in such country of origin responsible for the relevant transfer;

© 2018 Aker Solutions

- in Norway, against Aker Solutions AS or
- in the EEA country where the Data Subject resides or has its place of work, against the Business Unit being the Controller of the relevant Personal Data.

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.

Please see Data Protection Procedure Complaint Mechanism for further details.

3.5 Mutual assistance and cooperation with Data Protection Authorities

Aker Solutions undertakes to cooperate with the competent 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 Procedure. Further, Aker Solutions undertakes to conduct prior consultation as per legal requirements.

Except when a Data Protection Authority in one of the EEA countries has jurisdiction under its applicable data protection law, compliance with these rules shall be exclusively supervised by the Norwegian Data Protection Authority.

To the extent the Norwegian Data Protection Authority has discretionary powers for enforcement of applicable data protection law, it shall have similar discretionary powers for enforcement of this Procedure.

The Group Privacy Officer and the Local Privacy Officers shall be the main contact point between relevant Data Protection Supervisory Authorities and Aker Solutions on any matter arising out of the Data Protection Procedure or Processing of Personal Data in general. If such Data Privacy Officers are not appointed locally, the main contact person locally shall be the CEO of the relevant Business Unit together with the Group Privacy Officer.

3.6 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 local law. This Data Protection Procedure provides supplemental rights and remedies to Data Subjects only.

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

The Group Privacy Officer shall inform the competent Data Protection Authority of the legal requirements of such legislation if they are likely to have a substantial adverse effect on the guarantees provided by the Data Protection Procedure.

© 2018 Aker Solutions

3.7 Procedure for updating the Data Protection Procedure

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

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

a) The Group Privacy Officer keeps a fully updated list of members and keeps track of and records of any updates to the rules and provides the necessary information to the Data Subjects or Data Protection Authorities upon request;
b) 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 Procedure, and can demonstrate compliance; and
c) Any substantial changes to the Data Protection Procedure 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 Procedure shall always be available for all Business Units and employees.

Aker Solutions shall communicate any substantial modifications to the rules to the Data Subjects and to the Business Units by making the necessary changes to all relevant documents.

4 General privacy principles observed by Aker Solutions

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.

Any inquiries concerning the general principles should be addressed to the Group or Local Privacy Officer.

4.1 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 should be taken into account when Processing Personal Data.

4.2 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.

4.3 Data minimisation, 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/or further processed ("data minimisation");

© 2018 Aker Solutions

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").

4.4 Criteria for making data Processing lawful

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

4.4.2 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 local law or a collective agreement pursuant to local law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject;
c) Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving Consent;
d) the Processing relates to data which are manifestly made public by the Data Subject;
e) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
f) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of local law or pursuant to a contract with a health professional that is subject to the obligation of professional secrecy or another person subject to an equivalent obligation of secrecy; or
g) allowed according to other national rules than a)-e) above that have been established in accordance with the GDPR.

© 2018 Aker Solutions

4.4.3 Processing of Personal Data relating to criminal convictions and offences

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

4.4.4 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 should 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.

4.4.5 National identification numbers

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

4.4.6 Processing which does not require identification

To the extent that the Controller can demonstrate that it is not in a position to identify the Data Subject, the Controller shall be exempted from the application of the rights mentioned in Section 4.6.1 to 4.6.6. The Controller is also not obliged to obtain further Personal Data in order to link data in its possession to a Data Subject.

Where the Controller is not in a position to identify the Data Subject, the Controller shall inform the Data Subject accordingly, if possible. Unless the Data Subject provides additional information enabling his or her identification, the Controller is exempted from the obligation to meet requests for exercising the rights set out in Section 4.6.1 to 4.6.6.

4.5 Information to be provided to the Data Subject

4.5.1 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;

© 2018 Aker Solutions

b) the contact details of the Group or Local Privacy Officer;
c) the purposes of the Processing for which the Personal Data are intended as well as the legal basis for the Processing;
d) where the Processing is based on point f) set out in 4.4.1 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 organisation, 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 organisation 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/her already has it.

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

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

a) the identity and the contact details of the Controller and of his representative, if any;
b) the contact details of the Group or Local Privacy Officer;
c) the purposes of the Processing for which the Personal Data are intended as well as the legal basis for the processing;
d) the categories of Personal Data concerned;
e) the recipients or categories of recipients of the Personal Data, if any;
f) where applicable, the fact that the Controller intends to transfer such Personal Data to a Third Country or an international organization, with a reference to the appropriate safeguards cf. Section 4.14.2 and 4.15.2 and the means by which to obtain a copy of such safeguards or where they are

© 2018 Aker Solutions

made available if the Third Country or organisation in question is not recognised 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.

4.6 The Data Subject’s rights

4.6.1 Data Subject's right of access

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

a) confirmation as to whether or not data relating to him are being processed and where that is the case, access to the Personal Data processed by the Controller;
b) information about the purposes of the Processing, the categories of 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 recognised 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) 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.

4.6.2 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.

4.6.3 Right of erasure

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

a) the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise Processed;
b) the Data Subject withdraws his or her Consent to the Processing and where there is no other legal basis for the Processing;
c) the Data Subject objects to the Processing pursuant to Section 4.6.7 (a) and there are no overriding legitimate grounds for the Processing, or the Data Subject objects to the Processing pursuant to Section 4.6.7 (b);
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) the establishment, exercise or defence of legal claims.

4.6.4 Right of restriction of Processing

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

© 2018 Aker Solutions

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 defence of legal claims;
d) the Data Subject has objected to the Processing under Section 4.6.7 pending the verification whether the legitimate grounds of the Controller override those of the Data Subject.

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

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

Where required by applicable law, the Controller shall communicate any rectification or erasure of Personal Data or restriction of Processing carried out in accordance with Section 4.6.2 to 4.6.4 above to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort.

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

4.6.6 Right of data portability

Where required by applicable law, 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.

4.6.7 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 Section 4.4.1 e) and f), save where otherwise provided by applicable law. 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 defence 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.

© 2018 Aker Solutions

4.6.8 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 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 4.6.8 shall not be based on the Processing of Sensitive Personal Data unless point a) of Section 4.4.2 applies and suitable measures to safeguard the Data Subject's rights, freedoms and legitimate interests are in place.

4.7 Procedure for handling Data Subject's requests

Requests in accordance with Section 4.6.1 to 4.6.8 should be filed in writing to the relevant Data Privacy Officer. Prior to fulfilling the Data Subject's request, the Controller may, where appropriate, request the Data Subject to:

a) specify the IT system in which the Personal Data are likely to be stored;
b) specify the circumstances in which the Controller obtained the Personal Data; and
c) show proof of his or her identity.

Further, in the case of an access request, the Controller may, where appropriate, request the Data Subject to specify the categories of Personal Data to which he or she requests access.

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.

© 2018 Aker Solutions

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.

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 Joint Controllers

In situations where two or more Controllers jointly determine the purposes and means of the Processing, they shall be considered Joint Controllers. Such situations may arise when two Business Units together determine the purposes and means of the Processing, which may be the case e.g. in joint research projects.

Whether two or more Controllers are Joint Controllers must be assessed on a case-by-case basis and depends on whether there is any joint determination in relation to the purposes and means of the Processing. In the cases of Joint Controllers, they shall in a transparent manner determine their respective responsibilities for compliance with applicable EU/EEA data protection law, in particular as regards the information requirements and the Data Subjects rights referred to in Sections 4.5 to 4.6.

The parties' respective responsibilities shall be described in an arrangement between the parties, in particular as regards the exercising of the rights of the Data Subject and their respective duties to provide the information referred to in Sections 4.5.1 and 4.5.2. In addition, the arrangement shall typically include:

i. description of the processing and data flow map;
ii. the parties responsibilities with regard to data protection compliance;
iii. disclosure of data and confidentiality;
iv. technological and organisational security measures and conduction of risk assessment;
v. use of subcontractors;
vi. data transfers outside the EU/EEA;
vii. deletion and return of data;
viii. applicability of internal procedures;
ix. liability.

The essence of the arrangement shall be made available to the Data Subject and shall duly reflect the parties' respective roles and the relationships of the joint controllers towards the Data Subjects.

4.10 Use of data Processors

When Aker Solutions contracts with service providers for the delivery of services involving Processing of Personal Data on behalf of Aker Solutions, only Processors providing sufficient guarantees to implement technical and organizational measures in such a manner that the processing will meet the requirements of applicable EU/EEA data protection law shall be chosen.

The Processing by a Processor shall be governed by a contract that, as a minimum, sets out the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data

© 2018 Aker Solutions

and categories of the Data Subjects and the obligations and rights of the controller (a data processing agreement). The contract shall stipulate, in particular that the Processor:

(a) processes the personal data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a Third Country or an international organisation, unless required to do so by national law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;
(b) ensures that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
(c) takes all measures required by law related to the security of Processing;
(d) respects the conditions referred to below related to engagement of another Processor;
(e) taking into account the nature of the Processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights under applicable EU/EEA data protection law;
(f) assists the Controller in ensuring compliance with the legal obligations related to security of Processing and consultation with the Supervisory Authorities taking into account the nature of processing and the information available to the Processor;
(g) at the choice of the Controller, deletes or returns all the Personal Data to the Controller after the end of the provision of services relating to processing, and deletes existing copies unless applicable law requires storage of the Personal Data;
(h) makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Data Protection Procedure and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller

The processor shall not engage another processor without prior specific or general written authorisation of the Controller. In the case of general written authorisation, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

4.11 Data protection by design and by default

The Controller shall, both when determining the means for Processing and at the time of the Processing, implement appropriate technical and organisational measures, which are designed to implement data protection principles, such as data minimisation, in an effective manner, in order to integrate the necessary safeguards into the Processing for protecting Data Subjects' rights.

The Controller shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are Processed. This obligation applies to the amount of Personal Data collected, the extent of their Processing, the period of their storage and their accessibility. These measures shall particularly ensure that by default, Personal Data are not made accessible without intervention to an indefinite number of persons. Please refer to the applicable Aker Solutions procedure for applying these principles.

4.12 Data protection impact assessment and prior consultation

The Controller shall, when required by applicable law, carry out data protection impact assessments for processing operations that are likely to result in a high risk to the rights and freedoms of Data Subjects.

© 2018 Aker Solutions

Where a data protection impact assessment indicates that the Processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk, the competent Data Protection Authority shall be consulted, prior to the Processing.

Aker Solutions has established a procedure for Controlling and Processing Personal Data. Please refer to this procedure for details regarding data protection impact assessments.

4.13 Security of Processing

4.13.1 Appropriate technical and organizational security measures

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

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

4.13.2 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 Local Privacy Officer who shall forward the notification to the Group Privacy Officer.

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 unauthorised personnel can access the data, data theft and other kinds of data leaks.

Aker Solutions has established a procedure for Controlling and Processing of Personal Data which shall be followed when 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.

Aker Solutions shall document and 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.

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

4.14.1 Transfer from Controller to Controller

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

a) it is not incompatible with the purpose for which the Personal Data were collected, cf. 4.2;
b) it is in accordance with the principle of minimisation, accuracy and storage limitation, cf. 4.3;
c) the criteria for making Data Processing lawful is fulfilled, cf. 4.4;
d) if applicable, information is given to the Data Subject, cf. 4.5; and

© 2018 Aker Solutions

e) appropriate security measures protect the data during transfer and further Processing by the receiving Controller, cf. 4.13.1.

4.14.2 Transfer from Controller to Processor

Transfer of Personal Data from a Controller to a Processor, both bound by the Data Protection Procedure, may take place, provided that Section 4.10 is complied with.

4.15 Transfer of Personal Data to external Controllers not bound by the Data Protection Procedure

4.15.1 Transfer to external Controllers established within the EEA

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

a) it is not incompatible with the purpose for which the Personal Data were collected, cf. 4.2;
b) it is in accordance with the principle of minimisation, accuracy and storage limitation, cf. 4.3;
c) the criteria for making data Processing legitimate is fulfilled, cf. 4.4;
d) if applicable, information is given to the Data Subject, cf. 4.5;
e) appropriate security measures protect the data during transfer and further Processing by the receiving Controller, cf. 4.10.

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

4.15.2 Transfer to external Controllers 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 the conditions in Section 4.15.1 are fulfilled and one of the conditions in Section 4.16.2 are met.

4.16 Transfer of Personal Data to external Processors

4.16.1 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 Section 4.10 is complied with.

4.16.2 Transfer to external Processors established outside the EEA

Transfer of Personal Data from a Controller established within the EEA to a Processor established outside the EEA is prohibited, except when the conditions in Section 4.13.1 are fulfilled and one of the legal basis in Articles 45, 46, 47 or 49 of the GDPR are met, including:

a) the receiving Processor is established in a country which the EU Commission has considered having an adequate level of protection, cf. the Commission's decisions on the adequacy of the protection of Personal Data in third countries provided at: http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm;
b) the Processor is established in the US and has been certified under the EU-US Privacy Shield or any other similar program that is recognised by the EU Commission as ensuring an adequate level of protection;

© 2018 Aker Solutions

c) the Processor has implemented Binding Corporate Rules or a similar transfer mechanism that provides appropriate safeguards under applicable law;
d) the Controller and the Processor have provided appropriate safeguards by entering into EU Standard Contractual Clauses (model contract);
e) the Controller and the Processor have provided appropriate safeguards by entering into Standard Data Protection Clauses adopted by the EU Commission or a Data Protection Authority; or
f) an approved code of conduct or an approved certification mechanism pursuant to Article 46(1)(e) and (f) of the GDPR are provided for.

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

a) the transfer is necessary for the performance of a contract between the Controller and the Data Subject or for taking necessary steps at the request of the Data Subject prior to entering into a contract;
b) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural and legal person;
c) the transfer is necessary for important reasons of public interest;
d) the transfer is necessary for the establishment, exercise or defence of a legal claim;
e) the transfer is necessary to protect a vital interest of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent; or
f) the transfer is required by any law to which the relevant Controller is subject.

4.16.3 Transfers based on paragraph 2 litra b) and e) above require the prior approval of the Local Privacy Officer. Data Subject's Consent for Transfer

If none of the conditions listed in Section 4.16.2 are met or Consent is allowed or required under applicable law, Aker Solutions shall (also) seek an explicit Consent from the Data Subject for the relevant transfer. The Consent must be requested prior to participation of the Data Subject in specific projects, assignments or tasks that require the transfer of Personal Data.

A transfer can only be based on a Data Subject's Consent if it is likely to be a valid legal basis for the transfer. This means that Consent should not be used as a legal basis for transfers of employees' Personal Data, unless it is clear that it is freely given and all the other conditions set out in this Section are otherwise complied with, Consent will therefore as a main rule not be a valid legal basis for transfers of employees' Personal Data.

Prior to requesting Consent, the Data Subject shall be informed of the possible risks of the transfer due to the absence of appropriate safeguards and the fact that the EU Commission has not recognised the country in question as ensuring an adequate level of protection. When requesting Consent, the conditions in Section 4.4.4 apply.

4.16.4 Transfers from Business Units in Third Countries to third parties in Third Countries

Transfer of Personal Data collected in connection with the activities of a Business Unit established in a Third Country that is not recognised by the EU Commission as ensuring an adequate level of protection, to a third party also established in such Third Country, is permitted if one of the grounds in Section 4.16.2 applies or if the transfers are:

© 2018 Aker Solutions

a) necessary for compliance with a legal obligation to which the relevant Business Unit is subject;
b) necessary to serve the public interest; or
c) necessary to satisfy a legitimate purpose of the Business Unit.

© 2018 Aker Solutions

5 References

Policies:	Information Security and Data Protection Policy People Policy
Procedures:	Asset Management and Information Classification Procedure Information Security Procedure Control and Processing Procedure Data Subjects Rights Procedure Transfer of Personal Data procedure General Provisions and Principles Procedure Information Security and Incident management and Notification Procedure QM-00012 Enterprise Change Management QM-00010 Nonconformity Handling
Work Instructions:	Complaint mechanisms CCTV Guidelines for Data Privacy Officers

6 Revision Summary

Version	Description	Approved by	Date issued
00	Data Protection Standard	Chief HR Officer	September 2015
01	Data Protection Procedure	Chief IT Officer	March 2018

© 2018 Aker Solutions