Data Protection

Processing and Transfer of Personal Data in Kvaerner

Binding Corporate Rules
Public Document

Table of contents

1 Introduction

1.1 Scope

This Data Protection Standard contains a set of legally binding rules within Kvaerner which provide principles for **Processing** of **Personal Data** within the company group. The Data Protection Standard also includes the Binding Corporate Rules (see definition in Section 1.2.1) for Kvaerner, and shall apply for all Processing of Personal Data in Kvaerner.

The Data Protection Standard applies to Kværner ASA and its subsidiaries. For the purpose of this standard, the term "Kvaerner" refers to the whole company group or each of the Legal Entities as the case may be, see Section 1.2 below.

The Data Protection Standard is part of Kvaerner People Policy, and applies to all Kvaerner personnel. 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 Legal Entities established within the EEA to Legal Entities established outside the EEA (Third Countries, as defined below).

- Establishing consistent and uniform principles and procedures for the processing of all Personal Data in Kvaerner in accordance with the EU Data Protection Directive and the Norwegian Personal Data Act.

This document contains a summary of the rules in the BCR adopted by Kværner.

1.2 Definitions

1.2.1 Binding Corporate Rules (BCR)

BCR is a set of rules which provides an acceptable 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 Kvaerner Legal Entities situated in countries which are not members of the European Economic Area (EEA), so-called third countries (see definition below), in order to allow the Transfer of Personal Data from Legal Entities in the EEA to any (Kvaerner) Legal Entity located in a Third Country.

1.2.2 Consent

Consent means any freely given specific and informed indication of a Data Subject's wishes by which the Data Subject signifies his or her agreement to Personal Data relating to him or her being processed.

1.2.3 Controller

The Controller means the natural or legal person, e.g. Kværner ASA and/or a Legal Entity, which alone or jointly with others determines the purpose and means of the Processing of Personal Data.

1.2.4 Data Protection Officer

A Data Protection Officer holds a position within Kvaerner, 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.

1.2.5 Data Subject

A Data Subject is an individual to whom the Personal Data being processed relates to, for example an employee of Kvaerner, a person applying for a job at Kvaerner by entering information on Kvaerner's web site or a representative of a Kvaerner business partner.

1.2.6 EEA

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

1.2.7 Kvaerner

For the purpose of this Standard Kvaerner shall mean Kværner ASA and its subsidiaries (including partly owned subsidiaries where Kværner ASA directly or indirectly owns at least 50% and which is governed by Kvaerner's Corporate Governance Policies). Further, for the purpose of this standard, the term "Kvaerner" refers to the whole company group or each of the subsidiaries as the case may be.

1.2.8 Legal Entity

A Legal Entity shall mean a subsidiary in which Kværner ASA directly or indirectly owns at least 50 % of the voting interest and which is governed by Kvaerner's Corporate Governance Policies.

1.2.9 Personal data

Personal Data includes all types of information that directly or indirectly may be related or 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 linked to an identifiable individual.

1.2.10 Processing

Processing means 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.

1.2.11 Processor

A Processor is 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 Legal Entity. Aker Business Services is a Processor for Kvaerner, cf. Section **Error! Reference source not found.**.

1.2.12 Sensitive Data

Sensitive Data is defined as Personal Data revealing:

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

1.2.13 Third Countries

Third Country or 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).

1.2.14 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 Legal Entity who transfers the Personal Data will be the data exporter, and the receiving party will be the data importer.

1.3 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 Kvaerner 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. Kvaerner has Legal Entities placed in several 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 Legal Entities within the EEA to Legal Entities in third countries. As a general rule each Legal Entity 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 Legal Entity established in a Third Country receiving the Personal Data from the data exporter, will be the data importer.

Kvaerner's 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 collection of Personal Data shall only be made for explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
- The collection of Personal Data shall be relevant and not excessive in relation to the purpose of the intended processing.
- Personal Data shall be kept accurate and where necessary, up to date.
- Personal Data shall not be stored longer than is necessary for the purposes for which the data were collected or for which they are further processed.
- 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.

1.4 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 Legal Entities. Each Local Data Protection Officer is responsible for the implementation of the Data Protection Standard in its Legal Entity/region. All employees are responsible for adhering to this standard.

2 Description of Processing regulated by the Data Protection Standard

2.1 Material and geographical scope

The Data Protection Standard applies to all Processing of Personal Data in Kvaerner, and shall apply to Legal Entities as described in Section 1.1.

2.2 Categories of Personal Data and purpose of the data Processing

Kvaerner processes the following main categories of Personal Data, 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 Kvaerner: 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)

3 Key principles of the Data Protection Standard

3.1 The duty to respect the Data Protection Standard

Both Kværner ASA's and the Legal Entities' commitment to comply with the Data Protection Standard and related Tools are established by their signing of an Agreement Regarding Bindingness of Kvaerner' Data Protection Standard (Binding Corporate Rules).

Each Kvaerner employee is bound by the rules in this standard.

3.2 Data Subjects' rights

3.2.1 Beneficiary rights

All Data Subjects 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 appointed by Aker Solutions in accordance with internal procedures.

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 Kvaerner 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 Kværner 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 their rights. Information shall be provided for in the following documents:

Code of Conduct:
A public available and practical guidance on how to protect Personal Data when conducting business for Kvaerner will be published on the website of Kvaerner as part of the Code of Conduct. The statement "Caring about Privacy-document" will contain the main elements of the Data Protect Standard.

Kvaerner' Privacy Statement:
A Privacy Statement is available at kvaerner.com and applies 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 (this document). This Public Version explains Kvaerner 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.

Kværner ASA has appointed Kværner AS to take on the responsibility for any damages resulting from the violation of the Data Protection Standard made by the Legal Entities. Further, it takes on the responsibility of taking necessary action in order to remedy the acts of a Legal Entity, and, where appropriate, to pay compensation for any damages resulting from the violation of the Data Protection Standard by any Legal Entity bound by the rules herein. The Senior Vice President - Corporate Legal shall be contacted in case of a potential legal action.

The burden of proof lies with Kvaerner and not the Data Subject. Hence, for the benefit of the Data Subject, Kværner AS takes on the responsibility of demonstrating that the Legal Entity situated outside the EU is not liable for the violation resulting in the damage claimed by the Data Subject.

Where Kværner AS can prove that the Legal Entity 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 Kvaerner sets up a system which guarantees implementation and a good level of compliance with the Data Protection Standard in Legal Entities both inside and outside the EEA. The aim of appropriate training is to make the Data Protection Standard known, understood and effectively applied throughout the group of companies.

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 Legal Entity or Region
- Establishment of internal control mechanisms - ongoing monitoring
- Review program

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.

3.5 Internal complaint mechanisms

All Data Subjects, i.e. employees and third party beneficiaries, shall have the right to claim that any of Kvaerner's Legal Entities is not compliant 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.

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 Kværner AS (the EU Headquarters) in Norway.

3.6 Mutual assistance and cooperation with Data Protection Authorities

Kvaerner 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 Kvaerner on any matter arising out of the Data Protection Standard or Processing of Personal Data in general. If such Data Protection Officer is not appointed locally, the main contact person locally shall be the CEO of the relevant subsidiary 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 relevant data protection laws.

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

3.8 Procedure for updating the Data Protection Standard

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

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 Kvaerner

The following general principles are in accordance with the principles of the EU Data Protection Directive 95/46/EC. Kvaerner 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 Legal Entity 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 fairly, lawfully and pursuant to the principles stipulated in the Data Protection Standard. This means that the 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:

a) adequate, relevant and not excessive in relation to the purposes for which they are collected and /or further processed;
b) 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;

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.

4.4 Criteria for making data Processing legitimate

4.4.1 Processing of Personal Data

Personal Data may be processed only if:

a) the Data Subject has given his Consent; or
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; or
c) Processing is necessary for compliance with a legal obligation to which the controller is subject; or
d) Processing is necessary in order to protect the vital interests of the Data Subject; or
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 in a third party to whom the data are disclosed; or
f) 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:

a) the Data Subject has given his explicit Consent to the Processing of those data, except where the local laws applicable to the Legal Entity provide that the prohibition above may not be lifted by the Data Subject's giving his Consent; or
b) 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
c) 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
d) 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.
e) 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 legislation 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

In cases of collection of Personal Data from the Data Subject the Controller must provide the Data Subject with at least the following information:

a) the identity of the Controller and of his representative, if any;
b) the purposes of the Processing;
c) any further information such as
   - the 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,
   - his or her right of access to and the right to rectify the data concerning him/her 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.

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

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

Where the Personal Data have been collected from persons other than the Data Subject, the Controller shall provide the Data Subject with the information mentioned in Section 4.5.1 as soon as the data have been obtained. If the purpose of collecting the data is to collect them to other persons, the Controller may wait to notify the Data Subject until such disclosure takes place.

This provision shall not apply where 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:

a) 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,
b) confirmation to him in an intelligible form of the data undergoing Processing and of any available information as to their source,
   a. 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;

c) 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;

d) 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 the Processing

The Data Subject has the right:

a) at least in the cases referred to in Section 4.4.1 e) and f), to object at any time to the processing of data relating to him or her, save where otherwise provided by national legislation. Where there is a justified objection, the Processing made by the Controller may no longer involve those data;

b) to object, on request and free of charge, to the Processing of Personal Data relating to him or her 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 her, or significantly affects him or her and which is based solely on automated Processing of data intended to evaluate certain personal aspects relating to the Data Subject, such as performance at work, creditworthiness, reliability, conduct, etc.

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

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

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

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 particular kind 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:

a) the Processor shall act only on instructions from the Controller,
b) the obligations set out in 4.9.1 shall also apply to the Processor.

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.

4.10 Transfer to Controllers and Processors bound by the Data Protection Standard (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:

a) it is not incompatible with the purpose for which the Personal Data were collected, cf. Section 4.2;
b) it is in accordance with the principle of data quality and proportionality, 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 in accordance with 4.5.2;
e) 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:

a) 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;
b) the carrying out of Processing by way of a Processor is governed by a contract or legal act binding the Processor to the Controller and stipulating in particular 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.

4.11 Transfer 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:

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 data quality and proportionality, 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 in accordance with 4.5.2;
e) 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 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 one of the following requirements is fulfilled:

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

4.12 Transfer to external Processors not bound by the Data Protection Standard

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:

a) 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;
b) the carrying out of Processing by way of a Processor is governed by a contract or legal act binding the Processor to the Controller and stipulating in particular 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.

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:

a) the receiving Controller is established in a country which the EU Commission has considered having an adequate level of protection, cf. the Commission's decisions on the adequacy of the protection of Personal Data in third countries provided at: http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm; or

b) the Processor is established in the US and has endorsed the Safe Harbour Principles; or

c) one of the derogation in the Data Protection Directive article 26 applies; or

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

and all conditions in litra e) - h) is fulfilled;

e) 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;

f) 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:

g) the Processor shall act only on instructions from the Controller,

h) the obligations set out in 4.9.1, cf. the Data protection directive art 17, shall also apply to the Processor.