Binding Corporate Rules (BCR)

This document contains the provisions of the "Binding Corporate Rules (BCR) for Elanders AB and its affiliated group companies for the protection of *Personal Data*" which are binding towards *Data Subject*s, by virtue of third-party beneficiary rights. The information on these BCR is provided to the *Data Subject*s via our website.

1. Purpose of the BCR

Protecting the security and privacy of *Personal Data* is important to Elanders. Therefore, Elanders conducts its business in compliance with applicable laws on data privacy protection and data security.

BCR are internal *Personal Data* protection rules which Elanders as a multinational company has adopted in order to regulate the processing of *Personal Data* among Elanders Group companies world-wide under consideration of the EU General Data Protection Regulation EC 2016/679 (EU-GDPR), being effective as of May 25th 2018, which allow a transfer of *Personal Data* from the EU/ European Economic Area (EEA) to third countries only, if there are adequate safeguards for the protection of individuals' rights in place.

The main objectives of these BCR are to adduce adequate safeguards for the protection of the privacy and fundamental rights and freedoms of individuals within the meaning of applicable data protection law, especially the data protection laws of the member states of the EEA.

All employees of Elanders Group companies are obligated to respect these BCR and to observe the regulations laid down in this document.

Furthermore, the purpose of these BCR is to clearly define the rules applicable to all Elanders Group entities for processing *Personal Data* in order to ensure a consistent and adequate protection of *Personal Data* throughout the entire Elanders Group. This is to ensure that, when accessing or transferring *Personal Data* from the EEA to third, the Elanders Group entity in the third country will have an adequate level of data privacy protections in place.

Where the local legislation, for instance EU legislation, requires a higher level of protection for personal data it will take precedence over these BCR.

2. Mechanisms for reporting and recording changes

Individual Elanders Group companies are not entitled to adopt regulations that deviate from these BCR. Additional data protection policies can only be created in agreement with Elanders' Chief Corporate Data Protection Officer, if required by applicable national laws. Elanders' Chief Corporate Data Protection Officer keeps together with the Corporate Communication Department a fully updated list of the BCR members and keeps track of and record any updates to the rules and provide the necessary information to the *Data Subjects* or *Supervisory Authorities* upon request.

The Management of the Elanders Group and Elanders' Chief Corporate Data Protection Officer ensure that no data transfer is made to a new BCR member until the new BCR member is effectively bound by the BCR and can deliver compliance.

Any changes to these BCR or to the list of BCR members will be reported by Elanders' Chief Corporate Data Protection Officer once a year to the relevant *Supervisory Authorities* with a brief explanation of the reasons justifying the update and to all Elanders Group companies.

Where a modification would possibly affect the level of the protection offered by the BCR or significantly affect the BCR (i.e. changes to the binding character), the relevant *Supervisory Authorities* will be informed immediately by Elanders' Chief Corporate Data Protection Officer.

3. Scope of the BCR

The BCR apply to the processing of all *Personal Data* relating to *Data Subject*s by all Elanders companies and those who are obligated to these BCR by contract having their headquarter

- outside an EEA country to the extent that this *Personal Data* has been transferred from a participating company established in an EEA country or established in a country with an adequate level of data protection as acknowledged by a decision of the EU Commission to a participating company established outside the EEA; and

- in an EEA country or in a country with an adequate level of data protection as acknowledged by a decision of the EU Commission.

The contact details of all Elanders companies are listed in Annex 1 to these BCR.

Within the business scope of the Elanders Group, Sweden, Germany, Hungary, Italy, Poland, Netherlands, England, Czech Republic, USA, Russia, Asia are the countries and continents where the most data flow to and from.

The nature of the data covered by the BCRs are:

- Employee master data
- Communication data (e.g. email address, telephone number)
- Contract master data (contractual relationship, interest in the service, product or the contract)
- Client history
- Contract invoicing and payment data
- Planning and control data
- Information disclosed (by third parties, such as credit agencies or public records)

The main categories of persons affected by the processing include in particular:

- Customers
- Interested parties
- Subscribers

- Employees
- Vendors
- Consultants
- Suppliers
- Commercial agents
- Contact partners

The purposes of data transfers within the Elanders Group are to ensure competent and efficient administration of the following:

- Data necessary to administrate employment and external workforce (to fulfill obligations under labor law and other legal obligations as well as to administrate employee benefits and access rights).
- Shareholder's data necessary for shareholdings records and shareholder's meetings.
- Visitor data, for example to allow access rights and handle cookie consents for webpages.
- Customer and third-party workforce data such as business contact details and data relating to certification of performed training by such workforce processed for administrating contracts and other business relations.
- Performance of existing contractual relationships, conducting business initiations and handling of business activities.
- Job applicant data for recruitment activities.

4. Definitions and explanations

Terms written in italics and capital letters are defined in Annex 4 'Definitions' attached hereto and are based on the respective definitions of the European General Data Protection Regulation EC 2016/679.

Elanders AB and its affiliated group companies are *Controllers* as defined in the EU-GDPR seen in Annex 2.

5. Substantive principles for the processing of *Personal Data*

The following principles which derive specifically from the EU-GDPR apply to the processing of *Personal Data* by participating companies within the scope of these BCR.

5.1 Legitimacy & legality of data processing

Elanders will ensure that the processing of *Personal Data* will be done lawfully and fairly in compliance with the relevant statutory provisions and with due regard for the principles laid down in these BCR.

Elanders will only process data if and to the extent that at least one of the following prerequisites is fulfilled:

- The *Data Subject* has given consent to the processing of his or her personal data for one or more specific purposes.

- 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.
- Processing is necessary for compliance with a legal obligation to which Elanders is subject.
- Processing is necessary in order to protect the vital interests of the *Data Subject* or of another natural person.
- 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 Elanders Group.
- Processing is necessary for the purposes of the legitimate interests pursued by Elanders 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*, in particular where the *Data Subject* is a child.

Elanders will ensure that *Data Subject*s are able to withdraw his/her consent at any time in a simple, fast and efficient way.

Elanders will only process *Personal Data* of a child that is at least 16 years old. Elanders will, only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child, process *Personal Data* where the child is below the age of 16 years.

5.2 Purpose

Elanders will process *Personal Data* exclusively for specified, explicit and legitimate purposes. Under no circumstances, will Elanders process *Personal Data* in a way incompatible with the legitimate purposes for which the *Personal Data* was collected. Elanders companies are obligated to adhere to these original purposes when storing and further processing or using data transferred to them by another Elanders company; the purpose of *Data Processing* may only be changed with the consent of the *Data Subject* or to the extent permitted by the national law to which the Elanders company transferring the data is subject.

5.3 Transparency

All Elanders companies will process *Personal Data* in a transparent manner.

a. Where *Personal Data* are collected from *Data Subjects*, Elanders will provide *Data Subjects* with the following information at the time when *Personal Data* are obtained (in consultation with the transferring company, if applicable):

- identity and contact details of Elanders and of the transferring company and, where applicable, of the C*ontroller's* representative;
- contact details of the data protection officer, where applicable;

- categories of recipients or identity of the receiving entity, if any;
- purposes of *Processing* for which the *Personal Data* are intended as well as the legal basis for the processing;
- where the *Processing* is based on point (f) of Art. 6 (1) EU-GDPR, the legitimate interests pursued by the *Controller* or by a third party;
- where applicable, the fact that the *Controller* intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Art. 46 or 47 EU-GDPR, or the second subparagraph of Art. 49 (1) EU-GDPR, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
- period for which the *Personal Data* will be stored, or if that is not possible, the criteria used to determine that period;
- existence of the right to request access to and rectification or erasure of *Personal Data* or restriction of *Processing* concerning the *Data Subject* from Elanders and to object to *Processing* as well as the right to data portability;
- where the *Processing* is based on point (a) of Art. 6 (1) EU-GDPR or point (a) of Art. 9 (2) EU-GDPR, the existence of the right to withdraw consent at any time, without affecting the lawfulness of *Processing* based on consent before its withdrawal;
- right to lodge a complaint with a *Supervisory Authority*;
- 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;
- existence of automated decision-making including profiling, and 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*.

b. Where *Personal Data* have not been obtained from the *Data Subject*, Elanders will provide the *Data Subject* with the following information (in consultation with the transferring company, if applicable):

- identity and contact details of Elanders and of the transferring company and, where applicable, of the C*ontroller's* representative;
- contact details of the data protection officer, where applicable;
- purposes of processing for which the *Personal Data* are intended as well as the legal basis for the processing;
- categories of *Personal Data* concerned;

- recipients or categories of recipients of the *Personal Data*, if any;

- where applicable, the fact that the *Controller* intends to transfer *Personal Data* to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Art. 46 or 47 EU-GDPR, or the second subparagraph of Art. 49 (1) GDPR, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;

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

- where the *Processing* is based on point (f) of Art. 6 (1) EU-GDPR, the legitimate interests pursued by the *Controller* or by a third party;

- 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 processing as well as the right to data portability;

- where the *Processing* is based on point (a) of Art. 6 (1) or point (a) of Art. 9 (2) EU-GDPR, the existence of the right to withdraw consent at any time, without affecting the lawfulness of *Processing* based on consent before its withdrawal;

- right to lodge a complaint with a *Supervisory Authority*;

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

- the existence of automated decision-making, including profiling, referred to in Art. 22 (1) and (4) EU-GDPR 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*.

Elanders will provide the information referred to within the subsection b):

- within a reasonable period after obtaining the *Personal Data*, but at the latest within one month, having regard to the specific circumstances in which the *Personal Data* are processed;
- if the *Personal Data* are to be used for communication with the *Data Subject*, at the latest at the time of the first communication to that *Data Subject*; or
- if a disclosure to another recipient is envisaged, at the latest when the *Personal Data* are first disclosed.

Where Elanders intends to further process the *Personal Data* for a purpose other than that for which the *Personal Data* were collected, Elanders will provide the *Data Subject* prior to that further

processing with information on that other purpose and with any relevant further information as referred to within the points above.

This shall not apply where and insofar as:

- the *Data Subject* already has the information;
- the provision of such information proves impossible or would involve a disproportionate effort.
- obtaining or disclosure is expressly laid down by Union or Member State law to which Elanders is subject and which provides appropriate measures to protect the *Data Subject*'s legitimate interests; or
- where the *Personal Data* must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

5.4 Data quality and data economy

Elanders will ensure that appropriate measures are taken to guarantee that inaccurate or incomplete data is corrected or erased and that *Personal Data* is kept up to date.

Therefore, *Personal Data* will be:

- only collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);
- accurate and, where necessary, kept 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 (accuracy);
- kept in a form which permits identification of *Data Subject*s for no longer than is necessary for the purposes for which the *Personal Data* are processed (storage limitation);
- processed in a manner that ensures appropriate security of the *Personal Data*, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).
- processed only if it is required, i.e. as little *Personal Data* as possible. In particular, use is to be made of the possibility of anonymous or pseudonymous data, provided that the cost and effort involved is commensurate with the desired purpose (data economy).

Personal Data which is no longer required for the business purposes, for which it was originally collected and stored, will be erased by Elanders. In the event that statutory retention periods apply, the data shall be blocked rather than erased.

5.5 Onward transfer of data

Any transfers of *Personal Data* from Elanders companies which are undergoing processing or are intended for processing after the transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of these BCR, the conditions laid down in the EU-GDPR are complied with by Elanders and the *Processor*. All provisions in these BCR shall be applied in order to ensure that the level of protection of natural persons guaranteed by the EU-GDPR is not undermined.

A transfer of *Personal Data* to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

Without assessing the adequacy of the protection level by the Commission, Elanders or a *Processor* will transfer *Personal Data* to a third country or an international organisation only if appropriate safeguards are in place, and the rights and effective legal remedies for *Data Subjects* are available.

The appropriate safeguards may be provided for, without requiring any specific authorization from a S*upervisory Authority*, by:

- standard data protection clauses adopted by the EU-Commission in accordance with the examination procedure referred to in Art. 93 (2) EU-GDPR;
- an approved code of conduct together with binding and enforceable commitments of Elanders or the *Processor* in the third country to apply the appropriate safeguards, including as regards *Data Subject*s' rights; or
- an approved certification mechanism together with binding and enforceable commitments of Elanders or the *Processor* in the third country to apply the appropriate safeguards, including as regards *Data Subject*s' rights.

Subject to the authorisation from the competent *Supervisory Authority*, the appropriate safeguards may also be provided for, in particular, by:

- contractual clauses between Elanders or the *Processor* and Elanders, the *Processor* or the recipient of the *Personal Data* in the third country or international organisation.

5.6 Special Categories of *Personal Data*

Elanders will not process any *Special Categories of Personal Data* revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of

genetic data, *Biometric Data* for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The exceptions mentioned in Art. 9 (2) EU-GDPR will remain unaffected. These exceptions are as follows:

a) The *Data Subject* has given explicit consent to the processing of *Special Categories of Personal Data* for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in Art. 9 (1) EU-GDPR may not be lifted by the *Data Subject*.

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 Union or Member State law or a collective agreement pursuant to Member State 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) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the *Personal Data* are not disclosed outside that body without the consent of the *Data Subjects*.

e) Processing relates to *Personal Data* which are manifestly made public by the *Data Subject*.

f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

g) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the *Data Subject*.

h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in Art. 9 (3) EU-GDPR.

i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State

law which provides for suitable and specific measures to safeguard the rights and freedoms of the *Data Subject*, in particular professional secrecy.

j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Art. 89 (1) EU-GDPR based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the *Data Subject*.

5.7 Automated individual decisions

If *Personal Data* is processed for the purpose of making automated individual decisions, the legitimate interests of the *Data Subject* must be ensured through appropriate measures. Decisions which have negative legal consequences for the *Data Subject* or substantially prejudice the *Data Subject*, may not be reached exclusively on the basis of an automated individual procedure designed to evaluate an individual's personal characteristics, i.e. decisions may not be exclusively based on the use of information technology. An exception applies only if the decision

- is necessary for entering into, or performance of, a contract between the *Data Subject* and a *Data Controller*;
- is authorized by Union or Member State law to which Elanders is subject and which also lays down suitable measures to safeguard the *Data Subject*'s rights and freedoms and legitimate interests; or
- is based on the *Data Subject*'s explicit consent.

In case of one of these three exceptions Elanders implements suitable measures to safeguard *the Data Subject's* rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of Elanders, to express his or her point of view and to contest the decision.

5.8 Data security

Elanders will take appropriate technical and organizational measures to ensure the requisite data security, which protects *Personal Data* against accidental or unlawful erasure, unauthorized use, alteration, against loss, destruction as well as against unauthorized disclosure or unauthorized access. With regard to the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, Elanders will ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

The security measures provided by Elanders relate in particular to computers (servers and workplace computers), networks, communication links and applications. To ensure an adequate level of technical and organizational measures for data protection, Elanders introduced the Corporate Information Security Guide with binding effect for the entire Elanders Group.

Elanders will use specific measures ensure adequate protection of *Personal Data* include admission controls, system access controls, data access controls, transmission controls, input controls, job controls, availability controls and segregation controls.

Elanders will implement appropriate technical and organizational measures for ensuring that, by default, only *Personal Data* which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of *Personal Data* collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures will ensure that by default *Personal Data* are not made accessible without the individual's intervention to an indefinite number of natural persons.

All workplace computers – including mobile devices (e.g. laptops) – are password-protected. The Elanders intranet has a firewall system to protect internal company content from unauthorized external access. Transmission of *Personal Data* within the company's own network is typically encrypted – to the extent that the nature and intended purpose of the *Personal Data* requires this.

If a *Personal Data Breach* occurs despite appropriate technical and organizational measures taken, Elanders is obligated to notify the *Personal Data Breach* to the *Supervisory Authority* competent in accordance with Art. 33 (1) EU-GDPR not later than seventy-two (72) hours after having become aware of the *Personal Data Breach*, unless it is unlikely to result in a risk to the rights and freedoms of *Data Subjects*.

Elanders shall also notify the *Data Subject* without undue delay where the *Personal Data Breach* is likely to result in a high risk to the rights and freedoms of the *Data Subject* in order to allow him or her to take the necessary precautions.

5.9 Confidentiality of *Data Processing*

Elanders will process *Personal Data* in a manner that ensures appropriate security of the *Personal Data*, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

Only personnel, who are authorized and have been specifically instructed in compliance with data privacy protection requirements, may collect, process or use *Personal Data*. Access authorization of the individual employee will be restricted according to the nature and scope of his/her particular field of activity. Elanders' employees are prohibited from using *Personal Data* for private purposes, from transferring or from otherwise making available *Personal Data* to unauthorized persons. Unauthorized persons in this context include, for example, other employees, to the extent that they do not require the *Personal Data* to complete their specialist tasks. The confidentiality obligation continues beyond the end of the employment relationship of the employee in question.

5.10 Commissioned *Data Processing*

If a participating company commissions another company to process *Personal Data* under the terms of these BCR, the following requirements must be observed:

- The *Processor* is carefully selected by Elanders and is selected after the criteria as to who is able to ensure the necessary technical and organizational security measures required to perform *Data Processing* in compliance with data privacy protection regulations;
- Elanders will ensure and regularly verify that the *Processor* remains fully compliant with the agreed technical and organizational security measures;
- The performance of commissioned *Data Processing* must be regulated in a written or otherwise documented contract, in which the rights and obligations of the *Processor* are unambiguously defined;
- The *Processor* will be bound to process the received data by contract from Elanders within the contractual framework and in accordance to the instructions issued by Elanders. The processing of data for the *Processor*'s own purposes or for the purposes of a third party are prohibited by contract;
- Elanders takes responsibility for the legitimacy of processing and continues to be the point of contact for the *Data Subject*.

The data processing agreement of Elanders with a commissioned *Data Processor* stipulates 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 organization, unless required to do so by Union or Member State law to which the *Processor* is subject; in such a case, the *Processor* shall inform the *Controller* of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

b) ensures that persons authorized to process the *Personal Data* have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c) takes all measures required pursuant to Art. 32 EU-GDPR;

d) respects the conditions referred to in Art. 28 (2) and (4) EU-GDPR for engaging another *Processor*;

e) taking into account the nature of the processing, assists the *Controller* by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the *Controller*'s obligation to respond to requests for exercising the *Data Subject*'s rights laid down in Art. 12 to 22 EU-GDPR;

f) assists the *Controller* in ensuring compliance with the obligations pursuant to Art. 32 to 36 EU-GDPR 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 Union or Member State 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 Art. 28 EU-GDPR and allow for and contribute to audits, including inspections, conducted by the *Controller* or another auditor mandated by the *Controller*.

With regard to point (h), the *Processor* shall immediately inform the *Controller* if, in its opinion, an instruction infringes EU-GDPR or other Union or Member State data protection provisions.

5.11 Accountability and other tools

Every Elanders Group entity acting as controller is responsible for and able to demonstrate compliance with the BCR. In order to demonstrate GDPR compliance, every Elanders Group entity will maintain a record of all categories of processing activities according to Art. 30 (1) GDPR. This record will be maintained in writing including in electronic form and will be made available to the *Supervisory Authority* upon request.

In order to enhance compliance and when required, data protection impact assessments according to Art. 35 GDPR shall be carried out for processing operations that are likely to result in a high risk to the rights and freedoms of natural persons. 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 respective *Supervisory Authority*, prior to processing, shall be consulted.

Within the Elanders Group appropriate technical and organizational measures are in place which are designed to implement data protection and IT security principles and to facilitate compliance with the GDPR requirements.

5.12 Processing of *Personal Data* relating to criminal convictions and offences

Processing of *Personal Data* relating to criminal convictions and offences or related security measures based on Article 6 (1) GDPR shall be carried out by Elanders Group companies only under the control of official EU authorities or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of *Data Subjects*. Any comprehensive register of criminal convictions shall be kept by Elanders Group companies only under the control of official EU authorities.

6. Substantive rights of the *Data Subject*

Elanders ensures the inalienable rights of *Data Subjects* as listed below in respect to their *Personal Data* processed by an Elanders company within the scope of these BCR.

- The *Data Subject* has the right to demand communication in an intelligible form of the *Personal Data* processed in relation to him/her, of any available information as to its source, and the purpose of the processing.

- The *Data Subject* also has the right to information about the identity of Elanders and, in the event of the transfer of *Personal Data*, the *Data Subject* also has the right to information about the recipients or categories of recipients. The right to information also covers the logical structure of automated processing operations, to the extent that automated decisions are affected. The *Data Subject* does not have a right to informationwhere the *Personal Data* must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy. . Local legal regulations may restrict the *Data Subject*'s right to information if this right is exercised repeatedly within a short period of time, unless the *Data Subject* can show a legitimate reason for the repeated assertion of claims for information. According to Art. 15 (3) EU-GDPR, Elanders shall provide a copy of the *Personal Data* undergoing *Processing*. For any further copies requested by the *Data Subject*, the *Controller* may charge a reasonable fee based on administrative costs. Where the *Data Subject* makes the request by electronic means, and unless otherwise requested by the *Data Subject*, the information shall be provided in a commonly used electronic form.

- The *Data Subject* has the right to demand rectification if his/her *Personal Data* is found to be incorrect or incomplete.

- The *Data Subject* has the right to demand that his/her *Personal Data* be blocked off if it is not possible to establish whether the data is correct or incorrect.

- The *Data Subject* has the right to demand that his/her *Personal Data* be erased if the *Data Processing* was unlawful or has become unlawful in the interim or as soon as the data is no longer required for the purpose of the processing. Justified claims by the *Data Subject* for erasure will be acted on within a reasonable period by Elanders, to the extent that statutory retention periods or contractual obligations do not prevent erasure. In the event of statutory retention periods, the *Data Subject* may demand that his/her data be blocked rather than erased. The same applies if it would be impossible to erase the data.

- The *Data Subject* has the right to object to the processing of his/her *Personal Data* for advertising purposes or for purposes of market research and/or opinion polling purposes. The *Data Subject* will be informed of his/her right to object free of charge.

- The *Data Subject* also has a general right of objection to the processing of his/her *Personal Data*, if because of the *Data Subject*'s special personal situation, the legitimate interest of the *Data Subject* outweighs the legitimate interest of the controller in processing the *Personal Data*.

The *Data Subject* has the right not to be subject to decisions based on automated individual procedures designed to evaluate an individual's personal characteristics. This means for the *Controller* that decisions may not be exclusively based on the use of information technology.The *Data Subject* has the right to obtain confirmation from Elanders as to whether or not *Personal Data* concerning him or her are being processed, and, where that is the case, access to the *Personal Data* and the following information:

- the purposes of the processing;
- the categories of *Personal Data* concerned;
- the recipients or categories of recipient to whom the *Personal Data* have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the *Personal Data* will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request rectification or erasure of *Personal Data* or restriction of processing of *Personal Data* concerning the *Data Subject* from Elanders or to object to such processing;
- the right to lodge a complaint with a *Supervisory Authority*;
- where the *Personal Data* are not collected from the *Data Subject*, any available information as to their source;
- the existence of automated decision-making, including profiling, 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 *Personal Data* are transferred to a third country or to an international organisation, the *Data Subject* will have the right to be informed of the appropriate safeguards relating to the transfer.

The *Data Subject* can assert the above mentioned rights in writing towards the respective participating company, the competent Data Protection Officer (DPO) of such participating company or the Global Data Protection function of Elanders AB. The request of the *Data Subject* will receive a response from the contacted entity within a reasonable period. The response by Elanders will be in written form (e-mail is sufficient).

7. Third-party beneficiary rights

The BCR confer rights on *Data Subjects* to enforce the rules as third-party beneficiaries. Beside the third-party beneficiary rights specified within this section, the *Data Subjects* are also entitled to enforce the following elements of the BCR:

- Transparency (please see section 5.3)
- Data quality and data economy (please see section 5.4)
- Onward transfer of data (please see section 5.5)
- Special Categories of Personal Data (please see section 5.6)
- Data security (please see section 5.8)
- Confidentiality of Data Processing (please see section 5.9)
- Substantive rights of the Data Subject (please see section 6)
- Mutual assistance and cooperation with the data protection authorities (please see section 12)

- Right to lodge a complaint at a supervisory authority or before a competent court (please see section 13)
- Complaint process (please see section 14)

- Transparency requirements where national legislation prevents from complying with the BCR (please see section 16)

All *Data Subjects* benefitting from the third-party beneficiary rights will be provided with the information by Articles 13 and 14 GDPR.

The *Data Subject* shall have a right to judicial remedy for any breach of the rights guaranteed him by this BCR and the national law applicable to the processing in question.

Any *Data Subject* who has suffered damage as a result of an unlawful data processing operation or of any act incompatible with the national provisions for the protection of Personal Information or a breach of this BCR is entitled to receive compensation for the damage suffered.

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority in the EEA, in particular in the Member State of his/her habitual residence, place of work or place of the alleged infringement, in any case of non-compliance with the BCR carried out by a non-EEA BCR member, each *Data Subject* shall have the right to an effective judicial remedy where he or she considers that his or her rights under these BCR have been infringed as a result of the processing of his or her *Personal Data* in non-compliance with these BCR.

Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

The right to lodge a complaint is described in more detail in section 13 of these BCR.

8. Liability and handling of *Personal Data Breaches*

Elanders AB assumes liability for non-compliance with the BCR by BCR members established outside the EEA. Elanders AB undertakes to monitor BCR compliance by BCR members established outside the EEA and to ensure that BCR members established outside the EEA take the necessary corrective actions to remedy breaches of the BCR.

Elanders AB further undertakes to pay compensation for material or immaterial damages in the event of a violation of the BCR by a Group member. Such compensations could be enforced in national courts within the EEA.

If a BCR member outside the EU violates the BCR, the courts or other competent authorities within the EU will have jurisdiction and the *Data Subject* will have the rights and remedies against Elanders AB as

if the violation had been caused by Elanders AB in the Member State in which Elanders AB is based instead of the BCR member outside the EU.

The burden of proof lies within Elanders AB. Elanders AB will furthermore demonstrate that no breach of the BCR has taken place or that the BCR member established outside the EEA is not responsible for the breach of the BCR on which the *Data Subject*'s claim for damages is based.

Every Elanders Group company has the duty to notify without undue delay any *Personal Data Breaches* to the Management of the Elanders Group in Sweden and Elanders' Chief Corporate Data Protection Officer. Elanders' Chief Corporate Data Protection Officer will inform the *Data Subjects* without undue delay where the *Personal Data Breach* is likely to result in a high risk to their rights and freedoms in order to allow him or her to take the necessary precautions.

Furthermore, every Elanders Group company has the duty to document any *Personal Data Breach* (including the facts relating to the *Personal Data Breach*, its effects and the remedial action taken) and the documentation shall be made available to the respective *Supervisory Authority* upon request.

9. Tasks of any Data Protection Officer (DPO)

Our Data Protection Officers, who are listed in Annex 3,

- inform and advise Elanders or the *Processor* and the employees who carry out processing of their obligations pursuant to these BCR and to other Union or Member State data protection provisions;
- monitor compliance with these BCR and other Union or Member State data protection provisions and with the policies of Elanders or the *Processor* in relation to the protection of *Personal Data*, including the assignment of responsibilities, awareness-raising and training of staff having permanent or regular access to *Personal Data* and working on *Data Processing* activities;
- conduct data protection audits and methods for ensuring corrective actions to protect the rights of the *Data Subject*;
- provide advice where requested as regards the data protection impact assessment and monitor its performance;
- cooperate with the *Supervisory Authority*;
- record changes to these BCR and report those changes to the *Supervisory Authority*;
- report to the competent *Supervisory Authority* any legal requirements to which a member of the Elanders group is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by these BCR;
- act as the contact point for the *Supervisory Authority* on issues relating to processing, including the prior consultation, and consult, where appropriate, with regard to any other matter.

The duties of the Corporate Data Protection Officer (CDPO) include in particular:

- In consultation with the CEO and CFO of the Elanders AB (publ), the CDPO has to define data protection objectives and monitor their achievement. In particular an Elanders Group wide data protection strategy shall be defined incl. respective measures.

- Once a year the CDPO will submit a written Data Privacy report to Elanders Group management on the performance of his duties, reflecting also the measure to which the Elanders Group members comply to EU-GDPR.

  Independently of this, the CDPO is entitled and obliged to inform the highest management level immediately if any questions or problems arise during the performance of his duties within the Elanders Group.

- The CDPO will ensure that the transfer and/or exchange of employee and customer data between the group companies and/or third parties is handled uniformly and in accordance with Elanders BCR. Also attention must be paid to uniform processes.

- If it is appropriate to draw up agreements with works councils to secure the task in accordance with the above mentioned bullet point, the CDPO must draw up these in accordance with local rules and procedures. If negotiations with works councils are necessary, the CDPO are commissioned to start these negotiations.

- To ensure that EU-GDPR rules are also observed in the event of business relationships and data exchanges with partners in non-European Countries, the CDPO will provide respective trainings and guidelines.

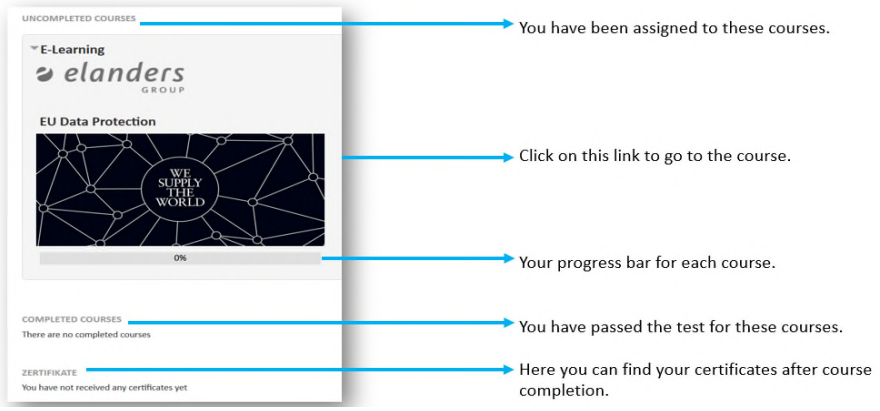
- The CDPO plans and coordinates training, data protection controls and audits relating to data protection. These must be coordinated and harmonized throughout the Elanders Group.

- The CDPO is responsible for advising, training and monitoring local data protection officers or data protection coordinators.

10. Training and awareness raising

Elanders has an online e-learning tool in place for training the employees having permanent or regular access to *Personal Data*, working on *Data Processing* activities or developing tools used to process *Personal Data*. The e-learning tool reminds the employees weekly about courses that have not yet been completed and enables the administrators (e.g. the CDPO) monitoring the trainings.

The starting page of the e-learning tool looks as follows:



The course „Data Protection“ is provided on an ongoing basis and has to be passed yearly by the respective employees. The course contains the following sections:

- ✓ Legal basis/EU-GDPR
- ✓ Data protection regulations in practice
- ✓ Binding Corporate Rules of the Elanders Group
- ✓ Knowledge test (Employees pass the test and receive a certificate if 80% of the 10 questions are answered correctly.)

Within the EU-GDPR tutorial the employees processing personal data will learn the basics of the EU-GDPR.

In the course of the training, they will receive answers to the following questions:

- ✓ What are data protection and BCR and what are their objectives?
- ✓ Why is data protection so important in this day and age?
- ✓ What are the main legal foundations for protecting data?
- ✓ What is personal data?
- ✓ Which data protection rules (incl. BCR) must employees comply with?
- ✓ What role does data and information security play in data protection?

In addition, classroom trainings are provided by the DPOs, if necessary.

11. Audit programme

To ensure verification of compliance with the regulations of the BCR, external auditors conduct audits on a yearly basis. The CDPO of the Elanders Group is in charge with monitoring BCR compliance on a day-by-day basis.

The audit programme covers all aspects of the BCR including methods of ensuring that corrective actions will take place. The result of the internal audit will be communicated to the respective managing directors, the CDPO and the Data Privacy Officer of the audited legal entity. Where appropriate, the result shall be communicated to the ultimate board of Elanders AB (parent board).

Supervisory Authorities will be provided access to the audit results upon request and Elanders authorises them to carry out own data protection audits of any BCR member if required in their own discretion.

12. Mutual assistance and cooperation with the data protection authorities

Elanders and the participating companies will trustfully cooperate and support one another in the event of inquiries and complaints from *Data Subject*s with regard to non-compliance with the BCR.

Elanders and the participating companies further undertake to trustfully cooperate with the Data Protection Authorities in the context of implementation of the BCR. Elanders will answer BCR-related requests from the Data Protection Authorities within an appropriate timeframe and in an appropriate fashion and will follow the advice and decisions of the Data Protection Authorities with regard to implementation of the BCR.

13. Right to lodge a complaint at a supervisory authority or before a competent court

Without prejudice to any other administrative or judicial remedy, every *Data Subject* has the right to lodge a complaint with a *Supervisory Authority*, in particular in the Member State of his/her habitual residence, place of work or place of the alleged infringement if the *Data Subject* considers that the processing of *Personal Data* relating to him or her infringes these BCR as of section 7.

In addition, *Data Subject*s have the right to enforce compliance with one of the above mentioned third party beneficiary rights by a BCR member, by lodging a complaint before the competent data protection authority or by seeking other legal remedies in the competent courts. Data subjects may claim compensation for damages.

Data subjects can choose to lodge such a complaint or claim compensation

- at a supervisory authority in the EU/EEA member state where the Data Subject has his/her habitual residence, place of work or the place where the alleged infringement took place; or
- before the competent court where the Controller or Processor has an establishment or where the Data Subject has his/her habitual residence.

This means that in the event of a breach of the BCR regulations by a BCR member established outside the EEA, courts and authorities within the EEA are also competent.

The *Data Subject* holds the same rights towards the BCR member that has accepted liability, as if the breach had been committed by a BCR member established in an EEA country.

The competence of courts and authorities in the EEA as described above does not apply however, if the data recipient is established in a country outside the EAA but that country does have an adequate level of data protection as acknowledged by a decision of the EU Commission.

In order to ensure that *Data Subject*s enjoy legally enforceable third party beneficiary rights also in those countries where the granting of third party beneficiary rights in the BCR document might not be sufficient, Elanders will – to the extent necessary – draw up additional contractual agreements with the relevant BCR members allowing for this. A third party beneficiary clause granting the necessary rights to *Data Subject*s is included in the Intra-Group Agreement for Compliance with the BCR which group companies have signed to signify their acceptance and implementation of the BCR. The same applies for the Adoption agreement which the other adopting companies conclude with Elanders.

14. Complaint process

Data Subjects are able to contact the competent complaint handling department in Elanders (please see contact details in section 17) or the participating company's competent local point of contact for data protection (generally the Data Protection Officer) by using the complaint handling form provided on the homepages of Elanders AB and its affiliated group companies, at any time, with complaints about a breach of these BCR by a participating company or with any questions.

Elanders will provide information on action taken on a request to the *Data Subject* without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. Elanders will inform the *Data Subject* of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the *Data Subject* makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the *Data Subject*.

If Elanders does not take action on the request of the *Data Subject*, Elanders will inform the *Data Subject* without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a *Supervisory Authority* and seeking a judicial remedy.

In addition, the *Data Subject* will be informed about the consequences if it is not satisfied by the reply or the actions taken.

Furthermore, the *Data Subject* can also lodge a claim before the Court and a complaint before the *Supervisory Authority* in the event he or she is not satisfied by the replies.

The *Data Subject* is not obliged to first follow the amicable dispute resolution process before lodging a complaint before the Courts and/or the Data Protection Authorities.

15. Whistle-blowing Process and Reporting

Elanders practices zero tolerance towards any form of malpractice, impropriety, statutory non-compliance or wrongdoing by our employees during the course of our work.

The whistle-blowing Policy allows for reporting by employees of such matters directly to Elanders without the need to copy the direct managers/supervisors as well as without fear of reprisal, discrimination or adverse consequences.

Elanders encourages employees to put their names to their allegations whenever possible. All concerns or irregularities raised will be treated with confidence and every effort will be made to ensure that confidentiality is maintained throughout the process.

Concerns may be raised verbally or in writing. As it is essential for Elanders to have all critical information in order to be able to effectively evaluate and investigate a complaint, the report made should provide as much detail and be as specific as possible. The complaint should include:

a) Details of the person/persons involved in the incident

b) Dates and time of incident

c) Type of incident

d) Evidence supporting the complaint, where possible

e) Contact details of the whistleblower, in case further information is required

All matters reported will be reviewed within a reasonable timeframe, and after due consideration and internal inquiry, a decision will be taken on whether to proceed with a detailed investigation. Direction may be sought from the CEO. While all complaints received by the Receiving Officer will be reported to the CEO, whistle-blowing complaints alleging fraud and breaches of corporate governance may be escalated to the Chairman of the Board of Directors subject to the recommendation of the CEO.

Elanders prohibits discrimination, retaliation or harassment of any kind against a whistleblower who submits a complaint or report in good faith. Employees shall be protected against retaliatory actions resulting from reporting unethical conduct to their superior. If a whistleblower believes that he/she is being subjected to discrimination, retaliation or harassment for having made a report under this Policy who feel that adverse action has been taken toward him/her due to a report of improper activity, the Receiving Officer should be similarly notified immediately. Reporting should be done to facilitate investigation and the taking of necessary action, if any.

At the appropriate time, the party making the report may need to come forward as a witness. If an employee makes an allegation in good faith but it is not confirmed by the investigation, no action will be taken against him or her. If, however, an employee has made an allegation frivolously, maliciously or for personal gain, disciplinary action may be taken against him or her.

Elanders will not retaliate against employees who in good faith, have reported suspected illegal activity or conduct of another entity that Elanders has a business relationship with, if the employee has a reasonable belief that the activity or conduct is in violation of law.

16. Transparency requirements where national legislation prevents from complying with the BCR

Where an Elanders Group company has reasons to believe that applicable local legislation prevents the company from fulfilling its obligations under the BCR or has substantial effect on the guarantees provided, the company will promptly inform the Management of the Elanders Group in Sweden and Elanders' Chief Corporate Data Protection Officer (except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

In addition, where any legal requirement Elanders Group company is subject to in a third country, is likely to have a substantial adverse effect on the guarantees provided by the BCR, the problem shall be reported to the respective *Supervisory Authority*. This includes any legally binding request for disclosure of the *Personal Data* by a law enforcement authority or state security body. In such a case, the respective *Supervisory Authority* shall be clearly informed about the request, including information

about the data requested, the requesting body, and the legal basis for the disclosure (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

If in specific cases the suspension and/or notification are prohibited, the affected Elanders Group company will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.

If, in the above cases, despite having used its best efforts, the affected Elanders Group company is not in a position to notify the respective *Supervisory Authority*, it will annually provide general information on the requests it received to the respective *Supervisory Authority* (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.). Transfers of *Personal Data* by an Elanders Group company to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

17. Contact

Data subjects can raise any concerns with the Data Protection Officer (DPO) of the relevant participating company or with the global Data Protection function of Elanders AB:

Elanders AB (Head office)
Flöjelbergsgatan 1C
431 35 Mölndal, Sweden
Internet: https://www.elanders.com/
Email: dataprotection@elanders.com

18. Final clause / IT security

To support data protection, IT security has an important role within the Elanders Group. Elanders´ wide range of business activities is based on data which is required for the provision of services.

Therefore, data are adequately protected at Elanders, in terms of their confidentiality, availability and integrity:

- Protection of **confidentiality** means that all relevant information is only made available to an entitled, authorised group of persons.
- Protection of **integrity** means that all relevant information is at all times available in full and in an unadulterated form, and that changes to this information can only be made by the group of persons authorised in this regard.
- Protection of **availability** means that all relevant information and resources are always available when required.

To achieve this protection and to fulfil legal requirements there is a very close cooperation between various departments within the Elanders Group.

Annex 1

The following Elanders Group entities are bound by the BCR that apply to all processing of personal data within the whole group

Elanders AB (publ)
Flöjelbergsgatan 1C
431 35 Mölndal
Sweden
Registration number: 556058-0622
Tel.: +46 31 750 00 00
Mail: info@elanders.com

Elanders Sverige AB
Box 137
435 23 Mölnlycke
Sweden
Registration number: 556262-1689
Phone: +46 31 750 00 00
Mail: info.sweden@elanders.com

Elanders Infologistics AB
Box 137
435 23 Mölnlycke
Sweden
Registration number: 556121-8891
Phone: +46 31 750 00 00
Mail: info.sweden@elanders.com

Elanders GmbH
Anton-Schmidt-Straße 15
71332 Waiblingen
Registration number: HRB722349
Tel.: +49 7151 9563-0
Fax.: +49 7151 9563-109
Mail: info.GERMANY@elanders.com

Elanders Holding GmbH
Hewlett-Packard-Straße 1/1
71083 Herrenberg
Registration number: HRB105591
Tel.: +49 7032 22910
Fax: +49 7032 2291 111

Elanders USA LLC
4525 Acworth Industrial Drive
Acworth, USA - Georgia 30101
Registration number: 58-1448183
Phone: +1 770 917 70 00
Fax: +1 770 917 70 20

Midland Information Resources
5440 Corporate Park Drive
USA - Davenport, IA 52807
Registration number: 42-1468885
Phone: +1 563 359 3696
Fax: +1 563 823 7651

Elanders Ltd.
Merlin Way, New York Business Park
North Tyneside
England - NE27 0QG
Registration number: GB 3788582
Phone: +44 1912-80 04 00
Fax: +44 1912-80 04 01

Elanders McNaugthan's Ltd.
Unit 4, 21 James Street
Righead Industrial Estate
ML4 3LU - Bellshill
Registration number: SC 135425
Phone: +44 1236 733 833

Spreckley Ltd.
79 Arnold Road
NG6 0ED, Nottingham
Registration number: 4179929
Phone: +44 115 978 3786
Fax: +44 115 978 3784

Elanders Polska Sp. z o.o.
Płońsk
Ul. Mazowiecka 2
Poland, 09-100 Płońsk
Registration number: KRS 0000101815
Phone: +48 23-662 23 16
Fax: +48 23-662 31 46

Elanders Hungary Kft.
Újmajor u. 2
Hungary, 8999 Zalalövő
Registration number: 20-09-065122
Phone: +36 92-57 25 00
Fax: +36 92-57 10 78
Mail: info@elanders-hungary.com

Elanders Italy S.r.l.
Via Delle Industrie 8
Italy, 31050 Ponzano Veneto (TV)
Registration number: 5686620963
Phone: +39 (0) 422 44 22 53
Fax: +39 (0) 422 44 22 53

Mentor Media Ltd.
No. 1, Bukit Batok Street 22,
#07-01 Singapur 659592
Registration number: 199302450H
Tel.: +65 6631 3333
Fax: +65 6896 3826
Mail: sales@mentormedia.com

LGI Logistics Group International GmbH
Hewlett-Packard-Straße 1/1
71083 Herrenberg
Registration number: HRB243806
Tel.: +49 7032 2291 0
Fax: +49 7032 2291 111
Mail: info@lgi.de

LGI Deutschland GmbH
Hewlett-Packard-Straße 1/1
71083 Herrenberg
Registration number: HRB354685
Tel.: +49 7032 2291 0
Fax: +49 7032 2291 111
Mail: info@lgi.de

LGI FreightLog GmbH
Murrer Straße 1
71691 Freiberg am Neckar
Registration number: HRB761526
Tel.: +49 7032 2291 0
Fax: +49 7032 2291 111
Mail: info@lgi.de

LGI TechLog GmbH
Joseph-Meyer- Straße 3
99195 Erfurt
Registration number: HRB513968
Tel.: +49 7032 2291 0
Fax: +49 7032 2291 111
Mail: info@lgi.de

LGI Logistics Solution GmbH
Werner-Heisenberg-Str. 1
46569 Hünxe
Registration number: HRB32410
Tel.: +49 7032 2291 0
Fax: +49 7032 2291 111
Mail: info@lgi.de

LGI Austria GmbH
Frankstahlstraße 1
2361 Laxenburg
Registration number: FN 349601 w
Tel.: +43 2236 860 936 333
Fax: +43 2236 860936111
Mail: info-at@lgi.de

LGI Polska Sp. z o.o.
ul. Magazynowa 2, Bielany Wroclawskie
PL 55-075 Kobierzyce
Registration number: KRS 0000246814
Tel.: +48 71 3858 253
Mail: info-pl@lgi.de

Logistics Worksolution Sp. z o.o.
Ul. Spoldzielcza 23
27-200 Strarachowice
Registration number: KRS 0000735255
Tel: +48 41 202 04 40
Mail: info-pl@lgi.de

LGI Logistics Group International AB
Lommavägen 39
S 232 35 Arlöv
Registration number: 556727-7990
Tel.: +46 40 430 610
Mail: info-se@lgi.de

LGI Czechia s. r. o.
Nádražní 295
471 23 Zákupy
Registration number: CZ25204581
Tel.: +420 487 828 012
Mail: info-cz-Zakupy@lgi.de

LGI Netherlands B.V.
Van Weerden Poelmanweg 10
3088 EB Rotterdam
Registration number: 34083373
Phone: +31 10 8511 600
Fax: +31 10 8511 601

LGI Logistics Group International UK Ltd.
4 Clarendon Drive, Wymbush
UK Milton Keynes MK8 8DA
Registration number: GB 07251732
Tel.: +44 1908 635 024
Fax: +44 1908569373
Mail: info-uk@lgi.de

LGI Hungária Logisztikai Kft.
M1 Üzleti Park B/6 épület
H 2071 Páty
Registration number: Cg.13-09-140503
Tel.: +36 23 312 978
Mail: info-hu@lgi.de

HELIX Software + Support GmbH
Hewlett-Packard-Straße 1/1
D-71083 Herrenberg
Registration number: HRB226056
Tel.: +49 7032 2292 100
Fax: +49 7032 2292130
Mail: info@helix.de

ITG GmbH Internationale Spedition + Logistik
Eichenstr. 2
D-85445 Schwaig
Registration number: HRB66157
Tel.: +49 8122 567 0
Fax: +49 8122 567 1101
Mail: info@itg.de

ITG Air & Sea GmbH
Eichenstr. 2
D-85445 Schwaig
Registration number: HRB250422
Tel.: +49 8122 567 0
Fax: +49 8122 567 1101
Mail: info@itg.de

ITG International Transports Inc.
6 Kimball Lane, Suite 230
USA-Lynnfield, MA 01940
Registration number: 43240627
Phone: +1 617 455 60 20
Fax: +1 617 455 60 15

OOO ITG International Transports + Logistics
Ostrovnaya Ulitsa 2
RUS-121552 Moskva
Registration number: OGRN 1127746350720
Phone: +7 495 234 69 84
Fax: +7 495 234 69 84

Logistik Lernzentrum GmbH
Schickardstraße 25
D-71034 Böblingen
Registration number: HRB246072

Tel.: +49 7031 3060 131
Fax: +49 7031 3060 249
Mail: info@logistiklernzentrum.de

d|o|m Deutsche Online Medien GmbH
Anton-Schmidt-Straße 5
D-71332 Waiblingen
Registration number: HRB265124
Tel.: +49 (0)71 51 / 165 17-0
Fax: +49 (0)71 51 / 165 17-99
Mail: info@d-o-m.org

myphotobook GmbH
Oranienstr. 183
D-10999 Berlin
Registration number: HRB94377
Mail: kundenservice@myphotobook.de

fotokasten GmbH
Anton-Schmidt-Str. 5 - 15
D-71332 Waiblingen
Registration number: HRB24050
Mail: info@fotokasten.de

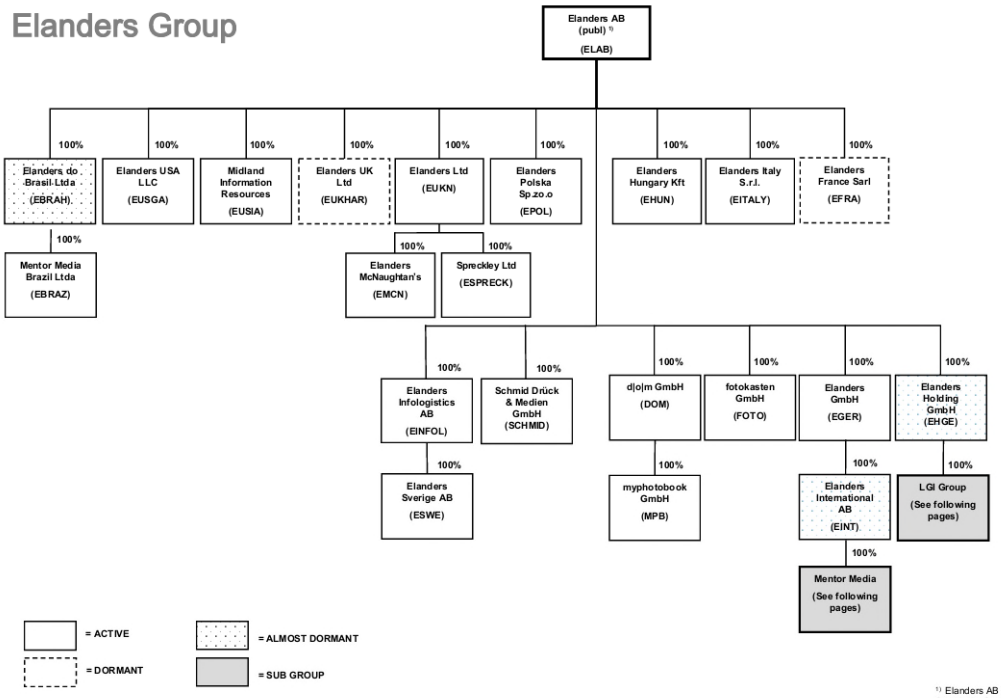
Schmid Druck und Medien GmbH
Gewerbepark 5
86687 Kaisheim
Registration number: HRB18350
Tel.: (+49) 0 90 99 / 96 95 – 0
Fax: (+49) 0 90 99 / 96 95 – 30
E-Mail: info@druckerei-schmid.de

elanders GROUP

Annex 2

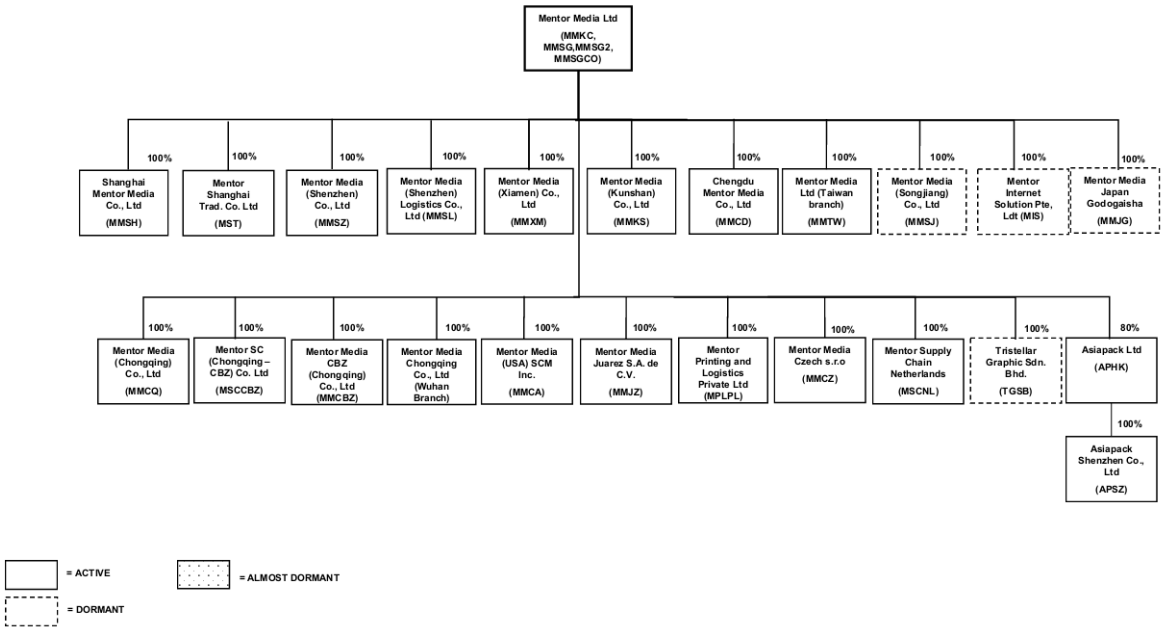
LEGAL STRUCTURE

Elanders Group

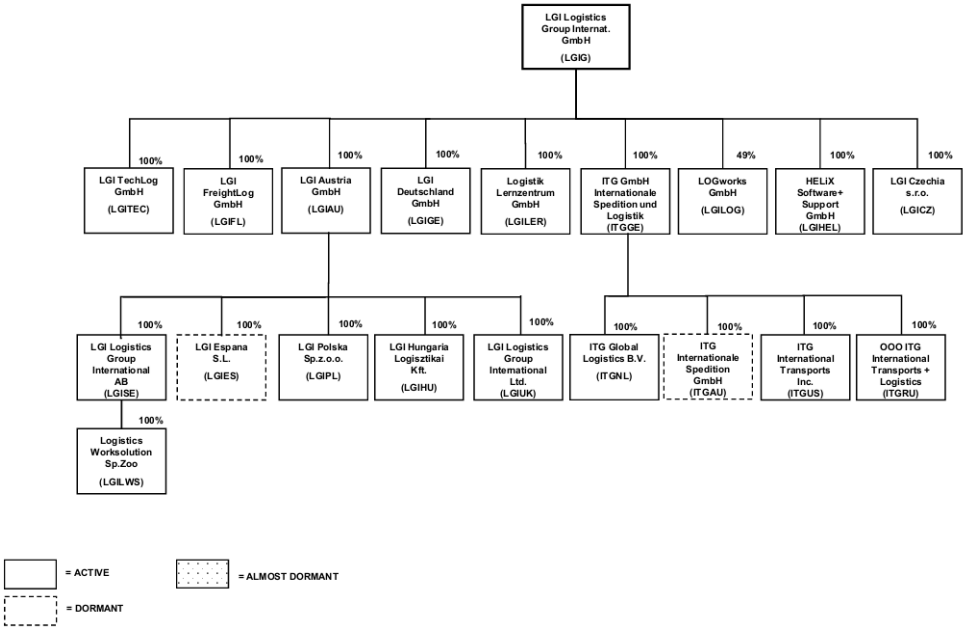


1) Elanders AB is a public company listed on the Nasdaq Stockholm Stock Exchange. Carl Bennet AB controls 50% of the capital and 66% of the votes in the company.

LEGAL STRUCTURE



LEGAL STRUCTURE



Annex 3

List of Data Protection Officers

Balázs Venter
E-Mail: balazs_venter@lgi.de, balazs.venter@elanders.com, dataprotection@elanders.com

Elanders Group
LGI Logistics Group International GmbH
LGI Deutschland GmbH
LGI FreightLog GmbH
LGI TechLog GmbH
LGI Logistics Solution GmbH
Logistik Lernzentrum GmbH
Helix Software + Support GmbH
ITG GmbH Internationale Spedition + Logistik
ITG Air & Sea GmbH

Annex 4

Definitions

- ***Biometric Data*** **means**

Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Biometric Data is increasingly used as a method of authentication, and often in conjunction with other data that should be protected (such as passwords, and, by extension, whatever information can be accessed as a result of gaining access to this). Member States are permitted to introduce further restrictions or conditions regarding the processing of *Biometric Data*.

- ***Controller*** **means**

the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of *Personal Data*.

- ***Consent*** **is**

any freely given, specific, informed and unambiguous indication of the *Data Subject*'s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of *Personal Data* relating to him or her.

- ***Cross-Border Processing*** **is**

  - processing of *Personal Data* which takes place in the context of the activities of establishments in more than one Member State of a controller or *Processor* in the Union where the controller or *Processor* is established in more than one Member State; or

  - processing of *Personal Data* which takes place in the context of the activities of a single establishment of a controller or *Processor* in the Union but which substantially affects or is likely to substantially affect *Data Subject*s in more than one Member State.

This refers to data transfers within the European Union; where this occurs, the EU-GDPR has stipulations as to which *Supervisory Authority* is to be involved.

- ***Data Concerning Health* is**

Personal Data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

- ***Data Controllers* are**

natural or legal persons, public authorities, agencies or other bodies which, alone or jointly with others, determines the purposes and means of the processing of *Personal Data*; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

These will usually be the public-facing entities that *Data Subject*s supply their information to. For instance, a hospital might have an online form for entering health information; even if the online form is provided by a third party, the hospital (which will determine what the data is processed for) will be the data controller.

- ***Data Processors* are**

natural or legal persons, public authorities, agencies or other bodies which processes *Personal Data* on behalf of the controller.

- ***Data Subject* is**

an identified or identifiable natural person. There is no restriction on their nationality or place of residence, so a *Data Subject* can be from anywhere around the world — the Regulation does not distinguish. Equally, however, a *Data Subject* has to be a *person;* a corporation or other entity cannot be a *Data Subject*, and information on those subjects has no protection under these BCR.

- ***Filing System* is**

any structured set of *Personal Data* which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis. This is used as a generic term to cover all methods by which *Personal Data* can be collected, stored, transmitted and processed.

- ***Genetic Data* are**

Personal Data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

With the increasing interest in genetics and genetic engineering, and public concerns over the legal status of genetic data, the EU-GDPR includes genetic data as part of *Personal Data*, thereby providing it with protections at least equal to other *Personal Data*. Member States are permitted to introduce further restrictions or conditions regarding the processing of genetic data.

- ***Group of Undertakings*** **means**

a controlling undertaking and its controlled undertakings.

- ***Main Establishment*** **means**

- as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of *Personal Data* are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

- as regards a *Processor* with establishments in more than one Member State, the place of its central administration in the Union, or, if the *Processor* has no central administration in the Union, the establishment of the *Processor* in the Union where the main processing activities in the context of the activities of an establishment of the *Processor* take place to the extent that the *Processor* is subject to specific obligations under this Regulation.

Determining the main establishment for organisations with a presence in multiple Member States will be important, as this defines which *Supervisory Authority* is to be involved, and may have some impact on various restrictions and conditions on processing certain types of *Personal Data* (such as biometric, genetic and health data).

- ***Personal Data*** **means**

any information relating to an identified or identifiable natural person (*Data Subject*); an identifiable natural person is one 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.

On specific note, the set of characteristics above is not exhaustive: any information that could be used to identify the *Data Subject* is *Personal Data*, and this information can be in any format. This can encompass photographs, correspondence, physical media and so on.

- ***Personal Data Breach* is**

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.

The majority of data breaches that the EU-GDPR is concerned with are *Personal Data* breaches. More general data breaches will be of concern if the data that is lost could lead to a *Personal Data Breach*.

- ***Processing* means**

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

- ***Processor* means**

a natural or legal person, public authority, agency or other body which processes *Personal Data* on behalf of the controller.

- ***Profiling* is**

any form of automated processing of *Personal Data* consisting of the use of *Personal Data* to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

- ***Pseudonymisation* is**

the processing of *Personal Data* in such a manner that the *Personal Data* can no longer be attributed to a specific *Data Subject* without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the *Personal Data* are not attributed to an identified or identifiable natural person.

- ***Recipient* means**

a natural or legal person, public authority, agency or another body, to which the *Personal Data* are disclosed, whether a third party or not.

- ***Representative* is**

a natural or legal person established in the Union who, designated by the controller or *Processor* in writing represents the controller or *Processor* with regard to their respective obligations under these BCR.

- ***Restriction of Processing* means**

the marking of stored *Personal Data* with the aim of limiting their processing in the future.

- ***Special Categories of Personal Data* are**

information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, biometric and genetic data.

- ***Supervisory Authority* means**

an independent public authority which is established by a Member State. In most cases, the *Supervisory Authority* will be the authority currently responsible for data protection measures.

Elanders AB

Case number:
DI-2019-11551

Date:
2021-01-28

Decision approving the Binding Corporate Rules of Elanders Group

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection finds that the Controller Binding Corporate Rules (Controller BCRs) of Elanders Group (Elanders) provide appropriate safeguards for the transfer of personal data in accordance with Articles 46.1, 46.2 b, 47.1 and 47.2 of the GDPR[1] and hereby approves the Controller BCRs of Elanders.

However, before making use of the BCR it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country of destination, including onward transfer situations. This assessment has to be conducted in order to determine if the guarantees provided by BCRs can be complied with in practice, in light of the circumstances of the possible impingement created by the third country legislation with the fundamental rights and the circumstances surrounding the transfer. If this is not the case, the data exporter in a Member State, if needed with the help of the data importer, should assess whether it can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

Where the data exporter in a Member State is not able to take supplementary measures necessary to ensure an essentially equivalent level of protection as provided in the EU, personal data cannot be lawfully transferred to a third country under this BCR. Therefore the data exporter is required to suspend or end the transfer of personal data. In such case if a Group Company envisages to transfer personal data to a third country nevertheless, it must notify the competent supervisory authority beforehand to enable that SA to ascertain whether the proposed transfer should be suspended or prohibited in order to ensure an adequate level of protection.

The approved Controller BCRs will not require any specific authorization from the concerned EU/EEA Data Protection Authorities.

The Swedish Authority for Privacy Protection presupposes that Elanders notifies changes to the Controller BCRs to the Swedish Authority for Privacy Protection, which

Postadress:
Box 8114
104 20 Stockholm
Webbplats:
www.imy.se
E-post:
imy@imy.se
Telefon:
08-657 61 00

[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

shall in turn forward the information to all concerned EU/EEA Data Protection Authorities.

The decision can be revoked if Elanders processes personal data contrary to the Controller BCRs or to the other provisions of the GDPR.

In accordance with Article 58.2 j of the GDPR, each concerned EU/EEA Data Protection Authority maintains the power to order the suspension of data flows to a recipient in a third country or to an international organization whenever the appropriate safeguards envisaged by the Controller BCRs of Elanders are not respected.

Application

Elanders has applied for approval by the Swedish Authority for Privacy Protection (IMY) of their Controller BCRs for the transfer of personal data to third countries within the Elanders Group.

In accordance with the cooperation procedure as set out in the Working Document WP263 rev.01[2], the Controller BCRs application of Elanders were reviewed by IMY, as the competent Authority for the BCRs (BCR Lead) and by one Supervisory Authority acting as co-reviewer. The application was also circulated to every EU/EEA Data Protection Authority for further review and comments.

Grounds for the decision

Having regard to Article 47 of the GDPR, IMY shall approve BCRs provided that they meet the requirements set out under this Article.

The review mentioned above concluded that the Controller BCRs of Elanders comply with the requirements set out by Article 47 of the GDPR, as well as the Working Document WP256 rev.01[3].

The EDPB provided its opinion 02/2021 in accordance with Article 64.1 f regarding the Controller BCRs of Elanders and IMY took utmost account of this opinion.

The decision has been taken by the Director General Lena Lindgren Schelin after presentation by the legal advisor Albin Brunskog. In addition, the Head of Unit Catharina Fernquist has participated in the final management of this matter.

Lena Lindgren Schelin

[2] Working Document Setting Forth a Co-Operation Procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR; adopted by the Article 29 Data Protection Working Party on 11 April 2018; endorsed by the European Data Protection Board (EDPB) on the first plenary meeting 25 May 2018. The Working Party was set up under Article 29 of Directive 95/46/EC. It was an independent European advisory body on data protection and privacy.
[3] Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules; Adopted by the Article 29 Data Protection Working Party on 28 November 2017; Last Revised and Adopted on 6 February 2018; endorsed by the European Data Protection Board (EDPB) on the first plenary meeting 25 May 2018.

How to appeal the decision

If you wish to appeal the decision, you shall write to IMY. You shall indicate in your letter which decision you wish to appeal and the requested change to the decision. The letter shall have reached IMY within three weeks of receipt of the decision, otherwise the appeal is not admissible. IMY will forward the appeal to the Administrative Court in Stockholm (Sw. Förvaltningsrätten i Stockholm) for examination, unless IMY chooses to change the decision in line with your request.

Provided that the appeal does not entail any privacy sensitive personal data or information that could be covered by the obligation of professional secrecy, you can e-mail the appeal to IMY. The contact details can be found on the first page of the decision.

Annexes to the decision

Annex 1: BCR-C, which includes

Sub-Annex 1 – List of BCR members,

Sub-Annex 2 – Legal Structure,

Sub-Annex 3 – List of Data Protection Officers, and

Sub-Annex 4 – Definitions.

Annex 2: Application

Annex 3: WP256 rev.01 referential

Annex 4: Declaration of Commitment

Annex 5: General Declaration of Commitment

Annex 6: Intra-Group Agreement

Annex 7: Complaint handling form

Annex 8: Rights of affected parties

Annex 9: Legal structure