D-Link

Intra-Group Data Processing Framework Agreement

This D-Link Intra-Group Data Processing Framework Agreement (hereinafter the "**Agreement**") is entered in by and between Affiliate Companies of

- D-Link Corporation, Xinhu 3rd Road, Neihu District, Taipei City, Taiwan (hereinafter "**D-Link Corporation**")
- who have joined the Agreement by signing the Letter of Accession (Annex 1 of this Agreement)

(hereinafter each a "**Party**" or a "**D-Link Company**" or collectively the "**Parties**" or the "**D-Link Companies**").

Table of Content

PREAMBLE

Whereas, The D-Link Companies are committed to the protection of privacy and personal data;

Whereas, This Agreement with its annexes is intended to regulate data transfer and data processing by the D-Link Companies;

Whereas, The Agreement is intended to ensure an adequate level of security in accordance with data protection regulations when personal data are processed and, in particular, transferred with regards to business activities of the Parties;

Whereas, In executing and supplementing the provisions of this Agreement, the Parties will agree or have already mutually agreed upon Individual Data Processing Contracts (hereinafter referred to as "**Individual Contract**"), which determine the details of the respective data processing and/or data transfers.

NOW, THEREFORE, the Parties have agreed as follows:

1 DEFINITIONS

The definitions of the EU General Data Protection Regulation (GDPR), especially of Art. 4 GDPR, apply to this Agreement.

In addition, the following definitions shall be applicable:

- "Affiliate Company" of D-Link Corporation means, D-Link Corporation itself and any company that, directly or indirectly, is controlled by or is under common control with D-Link Corporation. Control means, in relation to a company, the direct or indirect ownership of more than 50 per cent of the voting capital or similar right of ownership of that person or the legal power to direct or cause the direction of the general management and policies of that company whether through the ownership of voting capital, by contract or otherwise.
- "Contractual Documents" are this Agreement and the documents mentioned in Article 2.2 of the Agreement.
- "Text Form" describes a readable declaration, in which the person making the declaration is named, must be made on a durable medium. A durable medium is any medium that, (i) enables the recipient to retain or store a declaration included on the medium that is addressed to him personally such that it is accessible to him for a period of time adequate to its purpose, and (ii) that allows the unchanged reproduction of such declaration.

- “Third Party” or “Third Parties” are all individuals, corporate bodies and all other organizations that are not a Party to this Agreement.

- “Written Form”, “Written” or “in Writing” means the form by signing the original document by hand.

2 SCOPE, INTEGRAL PARTS OF THE AGREEMENT, ORDER OF PRECEDENCE, ACCESSION, BINDING CHARACTER

2.1 Scope of the Agreement

2.1.1 All D-Link Companies fall within the scope of this Agreement as far as they have acceded to the Agreement in accordance with the provisions of Article 2.3 of the Agreement. In particular, all D-Link Companies located in the EU/EEA shall enter into the Agreement pursuant to Article 2.3 of the Agreement.

2.1.2 The Agreement applies to the processing and transfer of all personal data

- in the context of the activities of a Party in the EU/EEA,

- where the processing is related to the offering of goods or services in the EU/EEA and

- to the monitoring of behavior of persons in the EU/EEA

to which the EU General Data Protection Regulation 2016/679 ("GDPR") applies.

2.2 Contractual Documents

2.2.1 In addition and subordinate to the terms of the Agreement, exclusively the following Contractual Documents shall be applicable in the following order of precedence (descending order):

- Annex 1:
  - Appendix 1 – Template Letter of Accession, attached to the Agreement
  - Appendix 2 – signed Letters of Accession, stored and managed by D-Link Corporation
- Annex 2, consisting of:
  - Appendix 1 – Individual Data Processing Contracts as agreed pursuant to Article 2.3 of the Agreement
- Annex 3 – Data Processing Agreement, attached to the Agreement

    - Appendix1 – Technical and Organizational Security Measures

- Annex 4 – Standard Contractual Clauses Controller to Processor, attached to the Agreement
- Annex 5 – Standard Contractual Clauses Controller to Controller, attached to the Agreement

2.2.2 The Contractual Documents shall, in their respective applicable version, become applicable under this Agreement. New versions of the Contractual Documents listed above will be applicable under this Agreement and replace the corresponding previous versions.

2.2.3 In the event of uncertainties or discrepancies between the Contractual Documents and this Agreement, the provisions of this Agreement shall prevail unless this Agreement expressly stipulates another order of precedence. The Parties may explicitly agree in Writing upon another order of precedence in the subordinate Contractual Document referencing to the provision of this Agreement from which it is intended to deviate.

2.2.4 Notwithstanding, the provisions of Annex 4 (Standard Contractual Clauses Controller to Processor) and Annex 5 (Standard Contractual Clauses Controller to Controller) shall prevail over the provisions of this Agreement and the other Contractual Documents.

2.3 Accession to the Agreement and Individual Contracts

2.3.1 The Parties hereby agree that any Affiliate Company of D-Link Corporation may, at the request of any other Party, become a Party to this Agreement by signing the Letter of Accession (Annex 1, Appendix 1 – Template Letter of Accession).

2.3.2 D-Link Companies accede to the Agreement by signing the letter of accession (Annex 1, Appendix 1). The signed Letters of Accession must be sent to D-Link Corporation and will be included to the Agreement in Annex 1, Appendix 2.

2.3.3 D-Link Companies accede to Individual Data Processing Contracts by signing the letter of accession in Annex 1 of this Agreement with reference to the Individual Contract agreed on the basis of Annex 2 – Individual Data Processing Contract. The signed Letters of Accession must be sent to D-Link Corporation and will be included to the Agreement in Annex 1, Appendix 2.

2.3.4 A Party shall fall out of the scope of the Agreement as soon as it ceases to be an Affiliate Company of D-Link Corporation or by declaring their withdrawal in writing to all other Parties.

2.3.5 D-Link Corporation shall from time to time inform all Parties about any changes to the Parties by making a copy of the current versions of Annex 1, Appendix 2 (signed Letters of Accession), and Annex 2 available for download.

2.4 Changes to the Contractual Documents

2.4.1 D-Link Companies reserve the right to change and/or update the Contractual Documents at any time. Such updating of the Contractual Documents may be necessary in particular due to changed legal requirements, significant changes in the group structure of D-Link Corporation and its Affiliate Companies, conditions imposed by the competent data protection supervisory authorities, new data transfers and data processing or changes to existing data transfers and data processing.

2.4.2 D-Link Corporation shall keep an overview of all changes and updates to the Contractual Documents made since they came into force and make copies of the current versions of the Contractual Documents available to the Parties for download. It also maintains a regularly updated list of all participating D-Link Companies that are effectively bound by the Agreement.

2.5 Binding Character of the Agreement

2.5.1 The Agreement shall be observed by all D-Link Companies under the scope of this Agreement. Upon submission of the letter of accession, the provisions of the Agreement are individually binding for the respective D-Link Company.

2.5.2 The employees of the D-Link Companies shall also be bound by the provisions of the Agreement. The management of each D-Link Company is obliged to ensure that the Agreement is legally binding for all employees in an appropriate manner. The text of the provisions of the framework agreement shall be available to the employees of the D-Link Companies at all times. The D-Link Companies shall inform their employees that non-compliance with the Agreement may lead to disciplinary or labor law measures (e.g. warning, termination).

3 PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

3.1 General principles for the processing of personal data

Personal data shall be

- processed lawfully, fairly and in a transparent manner in relation to the data subject (“**lawfulness, fairness and transparency**”);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (“**purpose limitation**”);

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“**data minimization**”);

- 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 subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject (“**storage limitation**”);

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (“**integrity and confidentiality**”).

Each Party is responsible for compliance with these principles and must be able to demonstrate such compliance ("**accountability**").

3.2 Privacy by design

Taking into account the state of the art, the implementation costs and the nature, extent, circumstances and purposes of the processing, as well as the different likelihood and severity of the risks to the rights and freedoms of natural persons associated with the processing, the Parties shall take appropriate technical and organizational measures (such as, but not limited to pseudonymization) both at the time the resources for the processing are determined and at the time the processing itself takes place, which are designed to effectively implement data protection principles, such as data minimization, and to implement the necessary safeguards to comply with data protection requirements and to protect the rights of data subjects.

3.3 Privacy by default

The D-Link Companies shall take appropriate technical and organizational measures to ensure that by default only personal data required for the specific purpose of processing is processed. This obligation applies to the amount of personal data collected, the scope of its processing, its storage period and its accessibility. In particular, such measures must ensure that personal data is not made accessible to an undetermined number of natural persons without the intervention of the person concerned.

3.4 Information obligations

Each Party fulfills all legal information obligations towards the data subject and, in particular, provides all information necessary to ensure fair and transparent processing in a precise, transparent, comprehensible and easily accessible form in clear and simple language. If a D-Link Company intends to further process the personal data for a purpose other than that for which the personal data was collected, it shall provide the data subject with information about this other purpose and all other relevant information prior to such further processing.

4 PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

4.1 General Prohibition

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or 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 shall be prohibited.

4.2 Exemptions

Exemptions shall apply in the following scenarios:

- The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where under the applicable data protection law, the prohibition of processing cannot be lifted by the data subject.

- The processing is necessary to enable the D-Link Company or data subject to carry out the obligations and exercise specific rights in the field of employment and social security and social protection law, insofar as Union law or the law of the Member States or a works council agreement under the law of the Member States provides for appropriate safeguards of the fundamental rights and interests of the data subject.

- The processing is necessary to protect the vital interests of the data subject or of another natural person and the data subject is physically or legally incapable of giving consent.

- The processing relates to personal data which are manifestly made public by the data subject.

- The processing is necessary for the establishment, exercise or defence of legal claims.

- The processing is necessary for reasons of substantial public interest on the basis of applicable data protection law.

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

- The 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 applicable data protection law.

- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on applicable data protection law.

5 DATA PROCESSING AND DATA TRANSFERS

5.1 Data Processing on behalf of another D-Link Company

5.1.1 Where a D-Link Company processes personal data on behalf of another D-Link Company (according to Art. 4 no. 8, Art. 28 GDPR), both Parties will comply with the regulations in Annex 3 (Data Processing Agreement) regarding such processing. For the purposes of Annex 3 (Data Processing Agreement), the Party that processes personal data on behalf of the other Party will be the “Processor”, while the other Party is the “Controller”.

5.1.2 The respective Individual Contract (see Annex 2) determines, whether a Party processes personal data on behalf of another Party.

5.1.3 In data processing scenarios, the provisions of Annex 2, Appendix 1 shall take precedence over the provisions of this Agreement, except from Annex 5 (Standard Contractual Clauses Controller to Processor) which shall prevail.

5.2 Data Transfers

5.2.1 The respective Individual Contract (see Annex 2) determines, whether a Party receives personal data as independent data controller.

5.2.2 Any transfer of personal data from one Party to another Party must be permitted based on one of the provisions of the GDPR (in particular Articles 6 to 10 GDPR).

5.3 Transfer of Personal Data to Countries outside of the EU/EEA

5.3.1 Where a D-Link Company based inside of the EU/EEA transfers personal data to a D-Link Company based in a country outside of the EU/EEA that is not subject to an adequacy decision of the EU commission, both Parties will comply with the EU Standard Contractual Clauses. In scenarios, where the receiving Party processes personal data on behalf of the other Party, the Parties will comply with the Controller to Processor

Clauses in Annex 4. Where all Parties are controllers of personal data, the Parties will comply with the Controller to Controller Clauses in Annex 5.

5.3.2 In such scenarios, the provisions of Annex 4 (Standard Contractual Clauses Controller to Processor) respectively Annex 5 (Standard Contractual Clauses Controller to Controller) shall take precedence over the provisions of this Agreement.

5.3.3 The respective Individual Contract (see Annex 2) determines whether personal data are transferred from a Controller to a Processor that is based outside of the EU or the EEA, or whether personal data are transferred from a Controller to a Controller that is based outside of the EU or the EEA.

6 TECHNICAL AND ORGANIZATIONAL MEASURES (TOMS)

6.1 Appropriate TOMS

The Parties take the appropriate technical and organizational measures to ensure a level of data protection appropriate to the risk, taking into account the state of the art, the implementation costs and the type, extent, circumstances and purposes of the processing as well as the risks to the rights and freedoms of data subjects. Every Party that processes personal data of another party must at least implement TOMS that provide a level of protection comparable to that shown in the Appendix 1 to Annex 3.

6.2 Risk assessment

In assessing the adequate level of protection, the Parties take the risks associated with the processing, including destruction, loss or alteration, whether unintentional or unlawful, or unauthorized disclosure of, or access to, personal data which have been transmitted, stored or otherwise processed into account.

6.3 Need to know

The D-Link Companies take appropriate measures to ensure that their employees and other natural persons under their control who have access to personal data only process such personal data in accordance with instructions of the respective D-Link Company, unless they are obliged to do so under applicable data protection law.

7 EMPLOYEES

7.1 Data Protection at the Workplace

7.1.1 This Agreement creates a D-Link Group-wide data protection concept that lays down uniform standards for guaranteeing and enforcing the data protection rights of the affected employees of D-Link Companies.

7.1.2 The D-Link Companies in the EU or EEA shall inform their employees about the data transfers and the data processing that affects them according to Art. 13 and 14 GDPR, if the GDPR is applicable.

7.1.3 In addition to the D-Link Companies to which the data was transferred according to this Agreement, the respective D-Link Company remains contact point for its employees (i.e. also for fulfilling their rights under the GDPR).

7.2 Sanctions to Employees

All D-Link Companies will inform their employees that non-compliance with this Agreement may lead to disciplinary or labor law measures (e.g. warning, termination).

8 TERM

8.1 Termination

Without prejudice to the provisions of Annex 4 (Standard Contractual Clauses Controller to Processor) respectively Annex 5 (Standard Contractual Clauses Controller to Controller), the Agreement and/or any Individual Contract may be terminated with respect to a particular Party by any other Party immediately by written notice to the particular Party if that particular Party ceases to be a D-Link Company.

8.2 Survival

Any termination or expiry of the Agreement and of any Individual Contract shall not affect any accrued rights or liabilities of any party nor shall it affect the coming into force or the continuation in force of any provisions of the Agreement and the respective Individual Contract (including any provisions of other Contractual Documents), which are expressly or by implication intended to come into force or continue in force on or after termination or expiry of the Agreement and the respective Individual Contract.

9 MISCELLANEOUS

9.1 Cooperation between D-Link Companies

All D-Link Companies will cooperate and support each other in a spirit of trust in the event of inquiries and complaints from affected parties regarding non-compliance with data protection regulations and/or this Agreement.

9.2 Complete Agreement

The Contractual Documents contain all agreements between the Parties relating to the subject of the Agreement and replaces all previous agreements, arrangements, declarations, negotiations or offers, regardless whether they were in Writing, in Text Form or oral.

9.3 Severability Clause

If provisions in this Agreement are or become completely or partially legally invalid or unenforceable, this does not affect the validity of the remaining part of this Agreement. In this event the Parties will negotiate a reasonable provision in good faith which comes as close as possible in terms of intent and purpose as well as economically to the legally invalid or unenforceable provision.

9.4 Applicable Law, Jurisdiction

9.4.1 The Agreement and the other Contractual Documents are subject to the law of the country where the data transferring Affiliate Company has its registered office.

9.4.2 Exclusive jurisdiction for all disputes under or in connection with the Contractual Documents shall belong to the court in whose area the registered office of the respective data transferring Affiliate Company is situated.

9.4.3 The provisions of provisions of Annex 4 (Standard Contractual Clauses Controller to Processor) respectively Annex 5 (Standard Contractual Clauses Controller to Controller) with respect to applicable law and jurisdiction remain unaffected by this Article 9.4.

List of Annexes attached to the Agreement:

- Annex 1, Appendix 1 – Template Letter of Accession, attached to the Agreement
- Annex 2, Appendix 1 Individual Data Processing Contracts
- Annex 3 – Data Processing Agreement, attached to the Agreement (with the Appendix 1 Technical and Organizational Measures)
- Annex 4 – Standard Contractual Clauses Controller to Processor, attached to the Agreement
- Annex 5 – Standard Contractual Clauses Controller to Controller, attached to the Agreement

List of Annexes stored and managed by D-Link Corporation:

- Annex 1, Appendix 2 – signed Letters of Accession

Annex 1

Appendix 1 – Template Letter of Accession

[Letterhead of entity]

[date and place]

I hereby declare that, on behalf of [name of entity], in accordance with Article 2 of the D-Link Intra-Group Data Processing Framework Agreement (“**Agreement**”), the accession to the Agreement and the Contractual Documents as specified in the Agreement, in particular to the Individual Contracts with effect to [date].

The current, applicable versions of the Agreement and the other Contractual Documents are available for download under [such as: inserting a hyperlink to Intranet].

This Letter of Accession is supplemental to the Agreement (as amended from time to time) made between the D-Link Companies (as defined in the Agreement) and attached at Annex 1, Appendix 2 of the Agreement, under which the Parties thereto have agreed to transfer personal data according to the terms contained therein.

The [name of entity] wishes to become a Party to the Agreement as a D-Link Company.

On behalf of [name of entity]

____

[name and position]

Annex 2

Appendix 1 –Individual Data Processing Contracts

This Individual Data Processing Contract (hereinafter the “**Individual Contract**”) is entered into by and between Affiliate Companies of

> D-Link Corporation, Xinhu 3rd Road, Neihu District, TaipeiCity, Taiwan (hereinafter “**D-Link Corporation**“) who have joined the D-Link Intra-Group Data Processing Framework Agreement (hereinafter the “**Agreement**”) by signing the Letter of Accession (Annex 1 of the Agreement)

(hereinafter each a “**Party**” or a “**D-Link Company**“ or collectively the “**Parties**” or the “**D-Link Companies**“).

The Parties have concluded the following Individual Data Processing Contracts:

Individual Data Processing Contract 1 – Employee Data

I. General Description of the Data Transfer

D-Link Affiliates based in the EU transfer personal data of employees to D-Link Corporation based in Taiwan.

II. Specific Description of the Data Transfer and Processing

Purpose of the Data Transfer and Processing	**Categories of Personal Data**	**Data subjects**
1. Group-wide human resources management and talent development.	E-mail address (work), Phone number (work), Name (First Name Last Name), Departments up to three levels, Employee Type (permanent or part-time), Join Date (YYYY/MM/DD), Seniority, Gender, Office (Country and State/City), Job Grade, Job Title, Education Degree/Graduated School/Major, Date of Birth / Age, Currency of Salary, Monthly Salary, 13th/14th Salary, Installment, Transportation Allowance, Telephone Allowance, Bonus Type, Payment Period, On-Target Bonus Base, Paytime per Year, Whole salary package includes all allowance, benefit and KPI Scheme, CV and resume, Departments related to employee's reporting line	Employees of D-Link Affiliates
2. Performance and organization of employee transfers between group companies.	E-mail address (work), Phone number (work), Name (First Name Last Name), Departments up to three levels, Employee Type (permanent or part-time), Join Date (YYYY/MM/DD), Seniority, Gender, Office (Country and State/City), Job Grade, Job Title, Education Degree/Graduated School/Major, Date of Birth / Age, Currency of Salary, Monthly Salary, 13th/14th Salary, Installment, Transportation Allowance, Telephone Allowance, Bonus Type, Payment Period, On-Target Bonus Base, Paytime per Year, Whole salary package includes all allowance, benefit and KPI Scheme, CV and resume, Departments related to employee's reporting line	Employees of D-Link Affiliates
3. Identifying synergies between the individual group companies.	E-mail address (work), Name (First Name Last Name), Departments up to three levels, Employee Type (permanent or part-time), Join Date (YYYY/MM/DD), Seniority, Gender, Office (Country and State/City), Job Grade, Job Title, Education Degree/Graduated School/Major, Date of Birth / Age, Currency of Salary, Monthly Salary, 13th/14th Salary, Installment, Transportation Allowance, Telephone Allowance, Bonus Type, Payment Period, On-Target Bonus	Employees of D-Link Affiliates

Purpose of the Data Transfer and Processing	**Categories of Personal Data**	**Data subjects**
	Base, Paytime per Year, Whole salary package includes all allowance, benefit and KPI Scheme, CV and resume, Departments related to employee’s reporting line	
4. Comparability of employee structures and business results of the group companies to identify opportunities for improvement.	E-mail address (work), Name (First Name Last Name), Departments up to three levels, Employee Type (permanent or part-time), Join Date (YYYY/MM/DD), Seniority, Gender, Office (Country and State/City), Job Grade, Job Title, Education Degree/Graduated School/Major, Date of Birth / Age, Currency of Salary, Monthly Salary, 13th/14th Salary, Installment, Transportation Allowance, Telephone Allowance, Bonus Type, Payment Period, On-Target Bonus Base, Paytime per Year, Whole salary package includes all allowance, benefit and KPI Scheme, CV and resume, Departments related to employee’s reporting line	Employees of D-Link Affiliates

II. Roles of the Parties

All Parties (D-Link Affiliates as well as D-Link Corporation) process the personal data as individual controllers of personal data.

III. Onward Transfer

D-Link Corporation will not transfer the personal data received to third parties or have it processed by a service provider as part of processing on behalf of D-Link Corporation.

IV. Legal Justification of the Transfer and Processing

The transfer of personal data from D-Link Affiliates to D-Link Corporation as well as the processing of personal data by D-Link Corporation is based on Art. 6 (1)(f) GDPR. The legitimate interests of the Parties are derived from the purposes of the data processing as stated above.

V. Third Country Data Transfer

D-Link Corporation is based in Taiwan. The transfer therefore constitutes as a third country data transfer. The Parties agree that the EU Standard Contractual Clauses between Controllers contained in Annex 5 to this Agreement shall apply to secure this third country data transfer, whereas the respective D-Link Affiliate is the data exporter and D-Link Corporation is the data importer.

VI. Additional information

Types of data processing used by recipient of personal data	**Analysis performed by data recipient**	**Data retention period of recipient of personal data**	**Source of personal data**
• Excel • Company internal system • Big Data analysis with anonymized data	• Compensation analysis • Performance analysis • Performance analysis • Capacity analysis • Career path analysis	No longer than six month after termination of employment contract	Directly from the respective employees via application and personnel questionnaire. The data are stored by the Affiliates in the following internal systems: • Internal HR system • Excel

VII. Contract Term

Beginning of the Individual Contract	The beginning of the Agreement.
Ordinary termination	Pursuant to the Agreement.

Individual Data Processing Contract 2 – Business Partner Data

I. General Description of the Data Transfer

D-Link Affiliates based in the EU transfer personal data of business partners to D-Link Corporation based in Taiwan.

II. Specific Description of the Data Transfer and Processing

Purpose of the Data Transfer and Processing	Categories of Personal Data	Data subjects
Executing group-wide marketing campaigns.	Account data of customer and business partners (including name, phone number, e-mail, street address, Google and FB OpenID, etc.); Licensing related data of customers and business partners (data collected by D-Link Affiliates in relation to the licensing of service or software, including personally identifiable information name, e-mail, passport number, etc.)	Business partners (and customers) of D-Link Affiliates

II. Roles of the Parties

All Parties (D-Link Affiliates as well as D-Link Corporation) process the personal data as individual controllers of personal data.

III. Onward Transfer

D-Link Corporation will not transfer the personal data received to third parties or have it processed by a service provider as part of processing on behalf of D-Link Corporation.

IV. Legal Justification of the Transfer and Processing

The transfer of personal data from D-Link Affiliates to D-Link Corporation as well as the processing of personal data by D-Link Corporation is based on Art. 6 (1)(f) GDPR. The legitimate interests of the Parties are derived from the purposes of the data processing as stated above.

V. Third Country Data Transfer

D-Link Corporation is based in Taiwan. The transfer therefore constitutes as a third country data transfer. The Parties agree that the EU Standard Contractual Clauses between Controllers contained in Annex 5 to this Agreement shall apply to secure this third country data transfer, whereas the respective D-Link Affiliate is the data exporter and D-Link Corporation is the data importer.

VI. Additional information

Types of data processing used by recipient of personal data	**Analysis performed by data recipient**	**Data retention period of recipient of personal data**	**Source of personal data**
• Excel • Marketing Campaign	N/A	As long as the business cooperation exists	Directly from the respective business partners or customers. From the following external sources: • Media cooperation with publishers and address brokers • Marketing requests via D-Link website • D-Link social media channels The data are stored by the Affiliates in the following internal systems: • Salesforce CRM

VII. Contract Term

Beginning of the Individual Contract	The beginning of the Agreement
Ordinary termination	Pursuant to the Agreement

Individual Data Processing Contract 3 – Organization, Compilation and Preservation of Data

I. General Description of the Data Transfer

D-Link Affiliates based in the EU transfer personal data of employees and business partners to D-Link Corporation based in Taiwan.

II. Specific Description of the Data Transfer and Processing

Purpose of the Data Transfer and Processing	Categories of Personal Data	Data subjects
Supporting group companies with the organization, compilation and preservation of personal data. Including potential organizational restructuring, expansion or spin-off from time to time with corresponding changes in workforce arrangement.	E-mail address (work); Phone number (work); Name (First Name Last Name); Office (Country and State/City); Job Grade; Job Title; Whole salary package includes all allowance, benefit and KPI Scheme; CV and resume; Departments related to employee's reporting line.	• Employees of D-Link Affiliates • Business partners of D-Link Affiliates

II. Roles of the Parties

All Parties (D-Link Affiliates as well as D-Link Corporation) process the personal data as individual controllers of personal data.

III. Onward Transfer

D-Link Corporation will not transfer the personal data received to third parties or have it processed by a service provider as part of processing on behalf of D-Link Corporation.

IV. Legal Justification of the Transfer and Processing

The transfer of personal data from D-Link Affiliates to D-Link Corporation as well as the processing of personal data by D-Link Corporation is based on Art. 6 (1)(f) GDPR. The legitimate interests of the Parties are derived from the purposes of the data processing as stated above.

V. Third Country Data Transfer

D-Link Corporation is based in Taiwan. The transfer therefore constitutes as a third country data transfer. The Parties agree that the EU Standard Contractual Clauses between Controllers contained in Annex 5 to this Agreement shall apply to secure this third country data transfer, whereas the respective D-Link Affiliate is the data exporter and D-Link Corporation is the data importer.

VI. Additional information

Types of data processing used by recipient of personal data	**Analysis performed by data recipient**	**Data retention period of recipient of personal data**	**Source of personal data**
• Excel • On Premise • Company internal system	N/A	• No longer than six month after termination of employment contract regarding employees of Affiliates • As long as the business corporation exists for business partners	Directly from the respective employees via application and personnel questionnaire. From the following external sources: • Media cooperation with publishers and address brokers • Marketing requests via D-Link website • D-Link social media channels The data are stored by the Affiliates in the following internal systems: • Salesforce CRM

VII. Contract Term

Beginning of the Individual Contract	The beginning of the Agreement.
Ordinary termination	Pursuant to the Agreement.

Individual Data Processing Contract 4 – IT Support

I. General Description of the Data Transfer

D-Link Affiliates based in the EU transfer personal data of employees to D-Link Corporation based in Taiwan that processes such data on behalf of the D-Link Affiliates.

II. Specific Description of the Data Transfer and Processing

Purpose of the Data Transfer and Processing	Categories of Personal Data	Data subjects
Provide IT infrastructure to the group companies.	E-mail address (work); Phone number (work); Name (First Name Last Name); Departments up to three levels; Join Date (YYYY/MM/DD); Job Title; Education Degree/Graduated School/Major; Skill sets (including training and certification such as LPI-C, CCNA, MCSE, etc.)	• Employees of D-Link Affiliates

II. Roles of the Parties

D-Link Affiliates are controllers of the personal data and D-Link Corporation processes the personal data on behalf of the D-Link Affiliates. The Parties agree that the Data Processing Agreement in Annex 3 to this Agreement applies to all processing operation related to this individual data processing contract.

III. Onward Transfer

D-Link Corporation will not transfer the personal data received to third parties or have it processed by a service provider as part of processing on behalf of D-Link Corporation.

IV. Legal Justification of the Transfer and Processing

The transfer of personal data from D-Link Affiliates to D-Link Corporation is based on Art. 6 (1)(f) GDPR. The legitimate interests of the Parties are derived from the purposes of the data processing as stated above. The processing of D-Link Corporation is based on Art. 28 GDPR.

V. Third Country Data Transfer

D-Link Corporation is based in Taiwan. The transfer therefore constitutes as a third country data transfer. The Parties agree that the EU Standard Contractual Clauses between

Controllers contained in Annex 4 to this Agreement shall apply to secure this third country data transfer, whereas the respective D-Link Affiliate is the data exporter and D-Link Corporation is the data importer.

VI. Additional information

Types of data processing used by recipient of personal data	**Analysis performed by data recipient**	**Data retention period of recipient of personal data**	**Source of personal data**
• Excel	N/A	• No longer than six month after termination of employment contract	Directly from the respective employees via application and personnel questionnaire. The data are stored by the Affiliates in the following internal systems: • Internal HR system

VII. Contract Term

Beginning of the Individual Contract	The beginning of the Agreement.
Ordinary termination	Pursuant to the Agreement.

Annex 3

Data Processing Agreement

1. Content and scope of the Data Processing Agreement

Scope, nature and purpose of the processing of the personal data of the Controller are set forth in the Agreement and in the respective individual data processing contracts in Annex 2 to the Agreement. Processor and any person acting under its authority who has access to personal data of the Controller, shall only process any personal data under the scope of this Data Processing Agreement on documented instructions from Controller, unless required to do so by law. Processor will confirm oral instructions in writing or text form without undue delay.

2. Compliance with GDPR

Processor will comply with all requirements referred to in Art. 28 to 33 GDPR.

3. Technical and organizational measures

3.1 Processor must execute the technical and organizational measures described in Section 6 of the Agreement and in Appendix 1 to this Annex 3.

3.2 Processor shall periodically monitor the internal processes and the technical and organizational measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection laws and the protection of the rights of the data subjects.

4. Audit rights

Processor makes available to Controller all information necessary to demonstrate compliance with this Agreement and allow for and contribute to audits, including inspections, conducted by Controller or another auditor mandated by Controller. Processor will especially provide proof to Controller upon request about the implementation of the technical and organizational measures described in Section 3 of this Data Processing Agreement.

5. Supporting obligations

5.1 Processor cooperates at the request of Controller in creating the records of processing activities, which relate to the subject matter for the Data Processing Agreement. Processor shall especially provide Controller with information necessary for the records of processing activities.

5.2 Processor will support Controller with necessary data protection impact assessments according to Art. 35 GDPR and with regards to prior consultation of supervisory authorities.

5.3 Processor will inform Controller without undue delay if the Processor is of the opinion that an instruction on the processing of personal data might violate any applicable data protection law.

6. Rights of data subjects

6.1 Insofar as a data subjects contacts the Processor directly concerning a rectification, erasure, restriction or other data subject right, the Processor will immediately forward the data subject’s request to the Controller in text form. The Processor rectificates, erases or restricts the processing of personal data on behalf of the Controller only after the latter's documented instructions.

6.2 Processor assists Controller with regards to Controller’s obligation to provide transparent information to the data subjects concerned. Processor will provide Controller with all relevant information in this regard.

7. Confidentiality of employees and subcontractors

Processor entrusts only such employees and only such subcontractors and/or their employees with the processing of personal data of Controller who have been bound to confidentiality and have previously been familiarized with the data protection provisions and the consequences of their violations relevant to their work.

8. Notification obligations

Processor reports any personal data breach (Art. 4 no. 12 GDPR) regarding the processing of personal data under this Data Processing Agreement immediately to Controller.

9. Supervisory authorities

9.1 Processor will inform Controller immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to the Data Processing Agreement. This also applies insofar as Processor is under investigation or is party to an investigation by a competent authority in connection with infringements to any civil or criminal law, or administrative rule or regulation regarding the processing of personal data of Controller in connection with the Data Processing Agreement.

9.2 Insofar as Controller is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a data subject or by a Third Party or any other claim in connection with the Data Processing Agreement with Processor, Processor shall make every effort to support Controller.

10. **Sub-processors**

10.1 Processor is allowed to engage sub-processors as long as the same data protection obligations as set out in this Data Processing Agreement are imposed on that sub-processor by way of a contract. Such contract with the sub-processor must provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR.

10.2 Processor will inform Controller prior to engaging a new sub-processor. Controller has the right to object to such engagement of a new sub-processor in writing within two weeks of receipt of that notice.

11. **Erasure of personal data**

After the end of the processing based on the Data Processing Agreement or upon request by Controller, Processor shall hand over to Controller or destroy all documents, data carriers and equipment, processing and utilization results as well as all data sets related to the Data Processing Agreement that Processor has been provided with in a way that complies with applicable data protection law requirements. The erasure or destruction of personal data of Controller has to be confirmed to Controller in writing.

Appendix 1 to the Data Processing Agreement (Annex 3 to the Agreement)

Technical and organizational security measures

The following measures to assure the security of the processing of personal data constitute minimum requirements which must be complied with by the Processor. Further measures which lead to higher level of protection can be introduced in the discretion and at the expense of the D-Link Company. Measures which are subject to technical progress can also be introduced in the discretion and at the expense of the Parties if there is no shortfall below the required level of protection.

In addition to the measures described, the IT department of the processor is certified in accordance with ISO 27001:2013.

1. Ensurance of availability and resilience

1.1 Availability control

Data sets can be at risk as a result of damage from fire and water, lightning strike or loss of electric power or theft and sabotage. The availability control is supposed to assure that no data are lost in these situations.

Protection against accidental destruction can be primarily assured by complying with fire prevention requirements and with additional hardware for interruption-free power supply and network security. IT systems, for example, can still be operated in the case of a sudden loss of electricity by taking corresponding precautions and with additional software until a controlled shutdown is possible. This can avoid both loss of data as well as damage to hardware.

Availability control also includes, however, measures to secure data, i.e. classic backup and related solutions. The intervals in which such data backup must be carried out always depends on the type of personal data, the frequency of changes and the importance of the personal data for the controller. However, the rule for all data backup is that also the created backup must be secured against destruction and theft. Therefore, the recommendation is to either directly create the data backup on a server at another location or store data carriers with data backups at another location.

1.2 Ensurance of resilience

Sufficient computer and server capacity must be used so that the functionality is also assured in the event of heavy access or heavy load.

2. Ensurance of integrity

2.1 Transfer control

Transfer control basically focuses on securing the transmission path for personal data, regardless whether on data carriers or electronically.

Measures must be taken to prevent unauthorized parties from having access to personal data during a transmission, regardless of the type of transmission. In every instance of data transmission, corresponding security measures must be taken.

2.2 Input control

As already mentioned above, it also always makes sense to protocol who accesses which personal data and when and what is changed. The measures for input control should ensure exactly this. It should be possible to determine at any time with those measures who has generated certain personal data, what the content of these personal data was and is and when the generation or the change was made, all with system logs or e-mail record.

3. Ensurance of confidentiality

3.1 Physical access control

The physical access control requires measures which prevent unauthorized persons from having physical access to data processing systems with which personal data are processed. Unauthorized persons must accordingly be prevented from even having the probability to enter data processing facilities. The physical access control, however, should not only prevent unauthorized physical entry, but also a destruction of IT equipment.

The authorization for physical access must always be exactly determined and documented. This applies especially also for persons who do not belong to the company such as service technicians (who should always be accompanied) or the cleaning personnel. Physical access control also includes all measures which prevent entry by force.

Effective physical access control is normally only possible with a combination of various measures that interact with each other.

3.2 Equipment access control

In contrast to physical access control, measures for equipment access control must be taken to prevent the use of data processing systems by unauthorized persons. This requires identification of the users and examination of the authorizations, in order to prevent unauthorized gaining knowledge or even changing or deleting personal data.

3.3 Data access control

Employees of the Party and Third Parties with corresponding authorizations can only access personal data which are relevant and necessary for rendering the purposes of the processing. Data access control accordingly involves limiting authorized access to personal data to the extent possible and necessary for the accessing persons.

The different authorizations can regulate the access to certain parts of the network, certain programs and/or certain editing rights (read rights, print rights, change rights). Furthermore, it is advisable to protocol authorized access in order to later be able to verify who had access when to which personal data and might have changed the personal data.

4. Ensurance of unlinkability by designation of purpose

4.1 Purpose of use control / Separation control

Personal data collected and processed for different purposes must be stored and evaluated separately. The requirement of data separation reflects this need and requires organizational and technical measures for data separation.

For example, employee and customer data or also the personal data of different customers must be separated. Physical separation (different data carriers), however, cannot always be implemented or does not always make economic sense. Therefore, it is sufficient for the personal data to be stored logically separate from each other. It is sufficient if the personal data, for example, can only be accessed using different access data.

4.2 Pseudonymization

The pseudonymized processing of personal data, when required, must occur in such a manner that the personal data can no longer be attributed to a specific data subject without reference to additional information if this additional information is separately stored and is subject to corresponding technical and organizational measures.

5. Procedures for regular testing, assessment and evaluation

5.1 Data protection management

The data protection management demands organizational measures which must be taken to assure the handling of personal data in conformity with the law.

The data protection management consists primarily of the audit function (ongoing recording of status of existing data protection processes), the governance function (managing the data protection) as well as the awareness function (education / information for employees) and includes, but are not limited to, the following processes:

- internal organization prior to the beginning of new processing of personal data,
- guidelines ("data protection strategies") to assure the principles of data quality, information, security and the rights of the data subjects,
- continuous updating of records of processing activities,
- appointment of a data protection officer,
- conducting training for employees.

5.2 Incident response management

IT security concepts and emergency plans for action in the case of a failure of IT systems as well as in the event of serious data protection breaches must exist.

Furthermore, there must be a reporting duty for data protection breaches to supervisory authorities and data subjects that is based on the degree of severity, which may be done according to the criteria from ISO 27001:2013. As a general rule, every data protection breach must be reported to the competent supervisory authority unless it "probably does not lead to a risk" for the data subject. The breach of data protection must be reported to the competent supervisory authority within 72 hours. Exceeding the deadline is only possible in justified situations. The reporting must include, among other aspects, the type of data protection breach, the categories of affected personal data, the number of affected data subjects and the data sets, an assessment of the consequences for the data subject as well as the measures to eliminate the cause or mitigate the harm to the data subject.

Therefore, incident response management must be available which meet the above requirements.

5.3 Data protection by default

So-called "data protection by default settings" must be made for IT systems. The basic mode requires technical specifications which take into account above all the requirement of data minimization. The selection of the settings for the respective IT system must be limited to what is necessary for the respective purpose of the processing.

The requirement of data protection by defaults covers the

- amount of the collected personal data,
- scope of processing of these personal data,
- storage times for these personal data, and
- accessibility to these personal data (restrictions on access).

5.4 Order control

The order control is supposed to assure that a processor of personal data also complies with the instructions from the controller of personal data and that the processing of the personal data on behalf of the controller only takes place within the scope of these instructions. Only being bound by instructions has the consequence that a transmission of personal data to the controller does not constitute transmission to Third Parties which would require the data subjects' consent.

Order control accordingly requires proportionate measures in terms of type and scope which assure that the transmission, storage, use and change and deletion of personal data can only take place at the processor in accordance with the requirements of the controller. In the first place, the controller must accordingly comply with the controller's instructions.

The instructions can be issued in any form. However, it is advisable to choose a form which avoids mistakes and permits proper proof at a later time. These requirements can best be implemented in practice by using forms (in text form, in writing or electronic) when issuing the instruction. The instructions should always also include which personal data are supposed to be transmitted and how the transmission shall take place.

The taken measures must continuously be reviewed with regard to their implementation and, if necessary, improved.

Annex 4

EU Standard Contractual Clauses Controller to Processor

The EU Standard Contractual Clauses controller to processor apply in scenarios, where a controller transfers personal data to a processor that is based outside of the EU/EEA under this Agreement. Such scenarios are further defined in Annex 2 to this Agreement. The data exporter is the Controller, while the data importer is the Processor.

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The data exporter

and

The data importer

each a ‘party’; together ‘the parties’,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) ‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;[1]

(b) ‘the data exporter’ means the controller who transfers the personal data;

(c) ‘the data importer’ means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) ‘the sub-processor’ means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) ‘the applicable data protection law’ means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) ‘technical and organizational security measures’ means those measures aimed at protecting 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.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter’s behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate 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, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(1) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(2) any accidental or unauthorized access; and

(3) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognized sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses (3). Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor’s obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against

the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses (Annex 4 to the Agreement)

Please see the respective individual data processing contract in Annex 2 to the Agreement for the description of the data processing activity, including the definition of data exporter and data importer, the description of data subjects, categories of data and the processing operations.

Appendix 2 to the Standard Contractual Clauses (Annex 4 to the Agreement)

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

Please see Appendix 1 to Annex 3 to the Agreement for a description of the technical and organizational security measures implemented by the data importer.

Appendix 3 to the Standard Contractual Clauses (Annex 4 to the Agreement)

Modification to Clause 4f: The data exporter must inform the data subject pursuant to Clause 4f that the data will be transferred to a third country without an adequate level of protection within the meaning of Regulation (EU) 2016/679, not only when special categories of data are transferred, but in all data transfers.

Modification to Clause 5d (i): The data importer must only inform the data exporter but also the data subject without delay of any legally binding request for disclosure of personal data by a law enforcement authority; if this disclosure of information is otherwise prohibited, for example by a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, the data importer must contact the competent supervisory authority and clarify the further procedure.

Amendment to Clause 5: The data importer agrees and warrants to take legal action against any disclosure of personal data and to avoid the disclosure of personal data to the respective authorities until a competent court in the last instance has issued a final judgment ordering the disclosure of the personal data.

Modification to Clause 7: Clause 7 1a is deleted; the parties agree to choose clause 7 1b in such a case.

New Clause 13 Liability:

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate with the data exporter in the defense and settlement of the claim.

Annex 5

EU Standard Contractual Clauses controller to controller

The EU Standard Contractual Clauses controller to controller apply in scenarios, where a controller transfers personal data to a controller that is based outside of the EU/EEA under this Agreement. Such scenarios are further defined in the individual data processing contracts in Annex 2 to this Agreement. The data exporter and the data importer are also defined in Annex 2 to this Agreement.

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement

between

data exporter

and

data importer

each a “party”; together “the parties”.

Definitions

For the purposes of the clauses:

a) “personal data”, “special categories of data/sensitive data”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority/authority” shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established);

b) “the data exporter” shall mean the controller who transfers the personal data;

c) “the data importer” shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection;

d) “clauses” shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

h) It will process the personal data, at its option, in accordance with:

   i. the data protection laws of the country in which the data exporter is established, or

   ii. the relevant provisions[3] of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data[4], or

   iii. the data processing principles set forth in Annex A.

i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

   i. the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

   ii. the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

   iii. data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

   iv. with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of

[3] "Relevant provisions" means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses).

[4] However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected.

third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

b) In the event that:

i. the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

ii. compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

iii. the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

iv. a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

v. a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

ANNEX A (of Annex 5 to the Agreement)

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.

8. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

   a) i. such decisions are made by the data importer in entering into or performing a contract with the data subject, and

      ii. the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

   or

   b) where otherwise provided by the law of the data exporter.

ANNEX B (of Annex 5 to the Agreement)

DESCRIPTION OF THE TRANSFER

Please see the respective Annex 2 to the Agreement for the description of the data processing transfer etc.

ANNEX C (of Annex 5 to the Agreement)

Amendment to Clause I: The data exporter must inform the data subject that the data will be transferred to a third country without an adequate level of protection within the meaning of Regulation (EU) 2016/679.

Amendment to Clause II: The data importer must inform the data exporter and the data subject without delay of any legally binding request for disclosure of personal data by a law enforcement authority; if this disclosure of information is otherwise prohibited, for example by a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, the data importer must contact the competent supervisory authority and clarify the further procedure.

Amendment to Clause II (i): The data importer agrees and warrants to take legal action against any disclosure of personal data where the requirements of this Clause II (i) are not met and to avoid the disclosure of personal data to the respective authorities until a competent court in the last instance has issued a final judgment ordering the disclosure of the personal data.

Modification to Clause III (a), sentence 1: The parties will indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of these clauses. Indemnification hereunder is contingent upon (a) the party(ies) to be indemnified (the “indemnified party(ies)”) promptly notifying the other party(ies) (the “indemnifying party(ies)”) of a claim, (b) the indemnifying party(ies) having sole control of the defence and settlement of any such claim, and (c) the indemnified party(ies) providing reasonable cooperation and assistance to the indemnifying party(ies) in defence of such claim.