PERSONAL DATA PROCESSING AGREEMENT FOR REVEL SYSTEMS, INC.

1. BACKGROUND

1.1. **Purpose and Application.** This Personal Data Processing Agreement for Revel Systems, Inc. ("**DPA**") is incorporated into the Agreement and forms part of the Agreement between Revel and Customer. This DPA applies to Personal Data processed by Revel and its Subprocessors in connection with the Agreement.

1.2. **Structure.** Appendices 1, 2 and 3 are incorporated into and form part of this DPA. Among other things, they set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of data subjects and the applicable technical and organizational measures.

1.3. **GDPR.** Revel and Customer agree that it is each party's responsibility to review and adopt requirements imposed on Controllers and Processors by the General Data Protection Regulation 2016/679 ("**GDPR**"), in particular with regards to Articles 28 and 32 to 36 of the GDPR, if and to the extent applicable to Personal Data of Customer/Controller that is processed under the DPA.

1.4. **Governance.** Revel acts as a Processor and Customer acts as a Controller under this DPA. Customer acts as a single point of contact and is solely responsible for obtaining any relevant authorizations, consents and permissions for the processing of Personal Data in accordance with this DPA.

2. SECURITY OF PROCESSING

2.1. **Appropriate Technical and Organizational Measures.** Revel has implemented and will apply the technical and organizational measures set forth in Appendix 2. Customer has reviewed such measures and agrees that as to all services purchased by Customer under the Agreement the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data.

2.2. **Changes.** Revel applies the technical and organizational measures set forth in Appendix 2 to Revel's Cloud Environment. Revel may change the measures set out in Appendix 2 at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

3. REVEL OBLIGATIONS

3.1. **Instructions from Customer.** Revel will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the services purchased by Customer under the Agreement then constitutes further instructions. Revel will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the services purchased by Customer under the Agreement. If any of the before-mentioned exceptions apply, or Revel otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, Revel will notify Customer (email permitted).

3.2. **Processing on Legal Requirement.** Revel may also process Personal Data where required to do so by applicable law. In such a case, Revel shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest. Appendix 1 sets out the type of Personal Data and categories of Data Subjects Processed.

3.3. **Personnel.** To process Personal Data, Revel and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. Revel and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

3.4. **Cooperation.** At Customer's request Revel will reasonably cooperate with Customer in dealing with requests from Data Subjects or regulatory authorities regarding Revel's processing of Personal Data or any Personal Data Breach. Revel shall notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing, without itself responding to such request without Customer's further instructions, if applicable and legally permissible. Revel shall provide functionality that supports Customer's ability to correct or remove Personal Data from the services purchased by Customer under the Agreement or restrict its processing in line with Data Protection Law. Where such functionality is not provided, Revel will correct or remove any Personal Data, or restrict its processing, in accordance with the Customer's instructions and Data Protection Law.

3.5. **Personal Data Breach Notification.** Revel will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. Revel may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by Revel.

3.6. **Data Protection Impact Assessment.** If, pursuant to Data Protection Law, Customer is required to perform a data protection impact assessment, at Customer's written request, Revel will provide such documents as are generally available for the services purchased by Customer under this Agreement (for example, this DPA, the Agreement, audit reports or certifications). Any additional assistance shall be mutually agreed between the Parties.

4. DATA EXPORT AND DELETION

4.1. **Export and Retrieval by Customer.** During the Term of and subject to the terms and conditions of the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case Revel and Customer will find a reasonable method to allow Customer access to Personal Data.

4.2 Deletion. Upon termination of the Agreement and in accordance with the terms and conditions of the Agreement and this DPA, Customer may request in writing that Revel delete any Personal Data in Revel's possession within a reasonable time period in line with Data Protection Law unless applicable law requires retention.

5. CERTIFICATIONS AND AUDITS

5.1. **Customer Audit.** Customer or its independent third-party auditor reasonably acceptable to Revel (which shall not include any third-party auditors who are either a competitor of Revel or not suitably qualified or independent, as determined by Revel in its sole discretion) may audit Revel's control environment and security practices relevant to Personal Data processed by Revel only if:

a) Revel has not provided sufficient evidence of its compliance with the technical and organizational measures that protect the production systems of the services purchased by Customer under the Agreement through a certification as to compliance with ISO 27001 (as defined in the "Scope of Certification" of the ISO 27001 certificate). Upon Customer's written request, no more than one (1) time annually, the ISO 27001 certification is available through Revel;

b) A Personal Data Breach has occurred;

c) An audit is formally requested by Customer's data protection authority; or

d) Mandatory Data Protection Law provides Customer with a direct audit right and provided that Customer shall only audit Revel pursuant to this Section 5.1 once in any twelve-month period unless mandatory Data Protection Law requires more frequent audits.

5.2. **Scope of Audit.** Customer shall provide at least sixty days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency of any audit shall be as set forth in Section 5.1(d) and the scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to Revel.

5.3. **Cost of Audits.** Customer shall bear the costs of any audit unless such audit reveals a material breach by Revel of this DPA, then Revel shall bear its own expenses of an audit. If an audit determines that Revel has breached its obligations under the DPA, Revel will promptly remedy the breach at its own cost.

6. SUBPROCESSORS

6.1. **Permitted Use.** Revel is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

a) Revel on its behalf shall engage Subprocessors under a written contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. Revel shall be liable for any breaches by the Subprocessor in accordance with the terms of this DPA.

b) Revel will evaluate the security, privacy, and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and

c) Revel's list of Subprocessors in place on the effective date of the Agreement will be made available to Customer upon written request, including the name, address and role of each Subprocessor Revel uses to provide the services purchased by Customer under the Agreement.

6.2. **New Subprocessors.** Revel's use of Subprocessors is at its discretion, provided that:

a) Revel will inform Customer in advance (by email) of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor; and

b) Customer may object to such changes as set out in Section 6.3.

6.3. **Objections to New Subprocessors**

a) If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, subject to Section6.3(b) below, Customer may terminate the Agreement (limited to the service purchased by Customer under the Agreement for which the new Subprocessor is intended to be used) on written notice to Revel. Such termination shall take effect at the time determined by the Customer which shall be no later than thirty days from the date of Revel's notice to Customer of the new Subprocessor. If Customer does not terminate within this thirty-day period, Customer is deemed to have accepted the new Subprocessor.

b) Within the thirty-day period from the date of Revel's notice to Customer informing Customer of the new Subprocessor, the parties will come together in good faith to discuss a resolution to the objection. Such discussions shall not extend the period for termination and do not affect Revel's right to use the new Subprocessor(s) after the thirty-day period.

c) Any termination under this Section 6.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.

6.4. **Emergency Replacement.** Revel may replace a Subprocessor without advance notice where the reason for the change is outside of Revel's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, Revel will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 6.3 applies accordingly

7. INTERNATIONAL PROCESSING

7.1. **Conditions for International Processing.** Revel shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law.

7.2. **Standard Contractual Clauses.** Where (i) Personal Data of an EEA or Swiss based Controller is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as a safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of another Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses, then:

a) Revel and Customer will enter into the Standard Contractual Clauses; and

b) Customer will enter into the Standard Contractual Clauses with each relevant Subprocessor as follows, either (i) Customer joins the Standard Contractual Clauses entered into by Revel and the Subprocessor as an independent owner of rights and obligations ("Accession Model") or, (ii) the Subprocessor (represented by Revel) enters into the Standard Contractual Clauses with Customer ("Power of Attorney Model"). The Power of Attorney Model shall apply if and when Revel has expressly confirmed that a Subprocessor is eligible for it through the Subprocessor list provided under Section 6.1(c), or a notice to Customer.

7.3. Relation of the Standard Contractual Clauses to the Agreement. Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and Subprocessor rules in sections 5 and 6, such specifications also apply in relation to the Standard Contractual Clauses.

7.4. Governing Law of the Standard Contractual Clauses. The Standard Contractual Clauses shall be governed by the law of the country in which the Customer is incorporated.

8. DOCUMENTATION; RECORDS OF PROCESSING

Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.

9. DEFINITIONS

Capitalized terms not defined herein will have the meanings given to them in the Agreement.

9.1. "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, if Customer ever acts as processor for another controller, it shall in relation to Revel be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.

9.2. **"Cloud Environment"** means the location where the production instance of the services purchased by Customer under the Agreement is hosted for the Customer.

9.3. **"Data Protection Law"** means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement (and includes, as far as it concerns the relationship between the parties regarding the processing of Personal Data by Revel on behalf of Customer, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not).

9.4. **"Data Subject"** means an identified or identifiable natural person as defined by Data Protection Law.

9.5. **"EEA"** means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway.

9.6. **"Personal Data"** means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is (i) entered by Customer or its Authorized Users into or derived from their use of the services purchase by Customer under the Agreement, or (ii) supplied to or accessed by Revel or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data (as defined under the Agreement).

9.7. **"Personal Data Breach"** means a confirmed (1) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data or (2) a similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.

9.8. **"Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller, be it directly as processor of a Controller or indirectly as Subprocessor of a Processor which Processes Personal Data on behalf of the Controller.

9.9. **"Standard Contractual Clauses"** or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply). The Standard Contractual Clauses current as of the effective date of the Agreement are attached hereto as Appendix 3.

9.10. **"Subprocessor" m**eans third parties engaged by Revel in connection with the services purchased by Customer under the Agreement and which process Personal Data in accordance with this DPA.

Appendix 1 to the DPA and, if applicable, the Standard Contractual Clauses

Data Exporter
The Data Exporter is the Customer who purchased services under the Agreement that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data.

Data Importer
Revel and its Subprocessors provide the following support: Revel supports the services purchased by Customer under the Agreement remotely from Revel facilities in Vilnius, Lithuania and other locations where Revel employs personnel in the operations function.

Data Subjects
Unless provided otherwise by the Data Exporter, transferred Personal Data relates to the following categories of Data Subjects: Revel employees/contractors, Revel customers, or other individuals or entities having Personal Data stored in the services purchased by the Customer under the Agreement.

Data Categories
The transferred Personal Data concerns the following categories of data:

- Name
- Email
- Title
- Telephone Number
- Address
- Other Personal Data as may be needed to provide Data Subjects with the services purchased under the Agreement

Special Data Categories (if appropriate)
The transferred Personal Data concerns the following special categories of data: As set out in the Agreement (including the Order Form) if any.

Processing Operations / Purposes
The transferred Personal Data is subject to the following basic processing activities:

- Use of Personal Data to set up, operate, monitor, and provide the services purchased by Customer under the Agreement (including operational and technical support)
- Provision of consulting services
- Communication to Authorized Users
- Storage of Personal Data
- Upload any fixes or upgrades
- Back up of Personal Data
- Computer processing of Personal Data, including data transmission, data retrieval, data access
- Network access to allow Personal Data transfer
- Execution of instructions of Customer in accordance with the Agreement

Appendix 2 to the DPA and, if applicable, the Standard Contractual Clauses – Technical and Organizational Measures

1. TECHNICAL AND ORGANIZATIONAL MEASURES
The following sections define Revel's current technical and organizational measures. Revel may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1.1 Physical Access Control. Unauthorized persons are prevented from gaining physical access to premises, buildings, or rooms where data processing systems that process and/or use Personal Data are located.
Measures:

- Revel protects its assets and facilities using the appropriate means based on the Revel Information Security Policy
- In general, buildings are secured through access control systems (e.g. smart card access system)
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas, and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- Access rights are granted to authorized persons on an individual basis according to the System Access Control and Data Access Control measures (see Sections 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to Revel buildings must register their names at reception and must be met by authorized Revel personnel.

Additional measures for Cloud Environment:

- Revel and all third-party Cloud Environment providers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Cloud Environment facilities from being compromised.
- Only authorized representatives have access to systems and infrastructure within the Cloud Environment facilities.
- To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.

1.2 System Access Control. Data processing systems used to provide the services purchased by Customer under the Agreement must be prevented from being used without authorization.
Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the Revel Information Security Policy.
- All personnel access Revel systems with a unique identifier (user ID).
- Revel has procedures in place so that requested authorization changes are implemented only in accordance with the Revel Information Security Policy (for example, no rights are granted without authorization). When personnel leave the company, their access rights are revoked.
- Revel has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.
- The Revel network is protected from the public network by firewalls
- Revel uses up–to-date antivirus software at access points to the company network
- Security patch management is implemented to provide regular and periodic deployment of relevant security updates.
- Full remote access to Revel's corporate network and critical infrastructure is protected by strong authentication.

1.3 Data Access Control. Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified, or removed without authorization in the course of processing, use and storage.
Measures:

- As part of the Revel Information Security Policy, Personal Data requires at least the same protection level as "Revel Systems Confidential" information according to the Revel Data Classification Policy.
- Access to Personal Data is granted on a need-to-know basis. Revel uses authorization concepts that document grant processes and assigned roles per account (user ID). All Personal Data is protected in accordance with the Revel Information Security Policy.
- Security measures that protect applications processing Personal Data are regularly checked. To this end, Revel conducts internal and external security checks and penetration tests on its IT systems.
- Revel does not allow the installation of software that has not been approved by Revel.
- A Revel security standard governs how data is deleted or destroyed once it is no longer required.

1.4 Data Transmission Control. Except as necessary for the provision of the services purchased by Customer under the Agreement, Personal Data must not be read, copied, modified, or removed without authorization during transfer.
Measures:

- Personal Data in transfer over Revel internal networks is protected according to the Revel Information Security Policy.
- When Personal Data is transferred between Revel and its customers, the protection measures for the transferred Personal Data are mutually agreed upon. This applies to both physical and network-based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of Revel-controlled systems.

1.5 Data Input Control. It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified, or removed from Revel data processing systems.
Measures:

- Revel only allows authorized personnel to access Personal Data on a need-to-know basis.
- Revel has implemented a logging system for input, modification, and deletion, or blocking of Personal Data by Revel or its Subprocessors to the extent technically possible.

1.6 Job Control. Personal Data being processed on Customer's behalf is processed solely in accordance with this DPA, the Agreement and related instructions of the Customer.
Measures:

- Revel uses controls and processes to monitor compliance with the Agreement between Revel and the Customer, Subprocessors or other service providers.
- As part of the Revel Information Security Policy, Personal Data requires at least the same protection level as "Revel Systems Confidential" information according to the Revel Data Classification Policy.
- All Revel employees and Subprocessors or other service providers are bound to respect the confidentiality of all sensitive information.

1.7 Availability Control. Personal Data will be protected against accidental or unauthorized destruction or loss.
Measures:

- Revel and all third-party Cloud Environment providers employ regular backup processes to provide restoration of business-critical systems as and when necessary.
- Revel and all third-party Cloud Environment providers use uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Cloud Environment.
- Revel has defined business contingency and disaster recovery plans for business-critical processes.
- Emergency processes and systems are regularly tested.

1.8 Data Separation Control. Personal Data collected for different purposes can be processed separately.
Measures:

- Revel uses the technical capabilities of the deployed software to achieve data separation among Personal Data originating from multiple customers.
- Customer has access only to its own Personal Data.

- If Personal Data is required to handle a support incident from Customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

1.9 Data Integrity Control. Personal Data will remain intact, complete, and current during processing activities.

Measures:

- Revel has implemented a multi-layered defense strategy as a protection against unauthorized modifications.
- In particular, Revel uses the following to implement the control and measure sections described above:
    - Firewalls;
    - Security Monitoring software;
    - Antivirus software;
    - Backup and recovery;
    - External and internal penetration testing;
    - Regular external audits to prove security measures.

Appendix 3 to the DPA

COMMISSION IMPLEMENTING DECISION (EU) 2021/914

of 4 June 2021

on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [1], and in particular Article 28(7) and Article 46(2)(c) thereof,

Whereas:

(1) Technological developments are facilitating cross-border data flows necessary for the expansion of international cooperation and international trade. At the same time, it is necessary to ensure that the level of protection of natural persons guaranteed by Regulation (EU) 2016/679 is not undermined where personal data is transferred to third countries, including in cases of onward transfers [2]. The data transfer provisions in Chapter V of Regulation (EU) 2016/679 are intended to ensure the continuity of that high level of protection where personal data is transferred to a third country [3].

(2) Pursuant to Article 46(1) of Regulation (EU) 2016/679, in the absence of an adequacy decision by the Commission pursuant to Article 45(3), a controller or processor may transfer personal data to a third country only if it has provided appropriate safeguards, and on condition that enforceable rights and effective legal remedies for data subjects are available. Such safeguards may be provided for by standard data protection clauses adopted by the Commission pursuant to Article 46(2)(c).

(3) The role of standard contractual clauses is limited to ensuring appropriate data protection safeguards for international data transfers. Therefore, the controller or processor transferring the personal data to a third country (the 'data exporter') and the controller or processor receiving the personal data (the 'data importer') are free to include those standard contractual clauses in a wider contract and to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, the standard contractual clauses or prejudice the fundamental rights or freedoms of data subjects. Controllers and processors are encouraged to provide additional safeguards by means of contractual commitments that supplement the standard contractual clauses [4]. The use of the standard contractual clauses is without prejudice to any contractual obligations of the data exporter and/or importer to ensure respect for applicable privileges and immunities.

(4) Beyond using standard contractual clauses to provide appropriate safeguards for transfers pursuant to Article 46(1) of Regulation (EU) 2016/679, the data exporter has to fulfil its general responsibilities as controller or processor under Regulation (EU) 2016/679. Those responsibilities include an obligation of the controller to provide data subjects with information about the fact that it intends to transfer their personal data to a third country pursuant to Article 13(1)(f) and Article 14(1)(f) of Regulation (EU) 2016/679. In the case of transfers pursuant to Article 46 of Regulation (EU) 2016/679, such information must include a reference to the appropriate safeguards and the means by which to obtain a copy of them or information where they have been made available.

---

[1] OJ L 119, 4.5.2016, p. 1.
[2] Article 44 of Regulation (EU) 2016/679.
[3] See also judgment of the Court of Justice of 16 July 2020 in Case C-311/18, *Data Protection Commissioner* v *Facebook Ireland Ltd and Maximillian Schrems ('Schrems II')*, ECLI:EU:C:2020:559, paragraph 93.
[4] Recital 109 of Regulation (EU) 2016/679.

(5) Commission Decisions 2001/497/EC ([5]) and 2010/87/EU ([6]) contain standard contractual clauses to facilitate the transfer of personal data from a data controller established in the Union to a controller or processor established in a third country that does not offer an adequate level of protection. Those decisions were based on Directive 95/46/EC of the European Parliament and of the Council ([7]).

(6) Pursuant to Article 46(5) of Regulation (EU) 2016/679, Decision 2001/497/EC and Decision 2010/87/EU remain in force until amended, replaced or repealed, if necessary, by a Commission decision adopted pursuant to Article 46(2) of that Regulation. The standard contractual clauses in the decisions required updating in the light of new requirements in Regulation (EU) 2016/679. Moreover, since the decisions were adopted, the digital economy has seen significant developments, with the widespread use of new and more complex processing operations often involving multiple data importers and exporters, long and complex processing chains, and evolving business relationships. This calls for modernisation of the standard contractual clauses to reflect those realities better, by covering additional processing and transfer situations, and to allow a more flexible approach, for example with respect to the number of parties able to join the contract.

(7) A controller or processor may use the standard contractual clauses set out in the Annex to this Decision to provide appropriate safeguards within the meaning of Article 46(1) of Regulation (EU) 2016/679 for the transfer of personal data to a processor or controller established in a third country, without prejudice to the interpretation of the notion of international transfer in Regulation (EU) 2016/679. The standard contractual clauses may be used for such transfers only to the extent that the processing by the importer does not fall within the scope of Regulation (EU) 2016/679. This also includes the transfer of personal data by a controller or processor not established in the Union, to the extent that the processing is subject to Regulation (EU) 2016/679 (pursuant to Article 3(2) thereof), because it relates to the offering of goods or services to data subjects in the Union or the monitoring of their behaviour as far as it takes place within the Union.

(8) Given the general alignment of Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 of the European Parliament and of the Council ([8]), it should be possible to use the standard contractual clauses also in the context of a contract, as referred to in Article 29(4) of Regulation (EU) 2018/1725 for the transfer of personal data to a sub-processor in a third country by a processor that is not a Union institution or body, but which is subject to Regulation (EU) 2016/679 and which processes personal data on behalf of a Union institution or body in accordance with Article 29 of Regulation (EU) 2018/1725. Provided the contract reflects the same data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) Regulation (EU) 2018/1725, in particular by providing sufficient guarantees for technical and organisational measures to ensure that the processing meets the requirements of that Regulation, this will ensure compliance with Article 29(4) of Regulation (EU) 2018/1725. In particular, that will be the case where the controller and processor use the standard contractual clauses in Commission Implementing Decision on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([9]).

(9) Where the processing involves data transfers from controllers subject to Regulation (EU) 2016/679 to processors outside its territorial scope or from processors subject to Regulation (EU) 2016/679 to sub-processors outside its territorial scope, the standard contractual clauses set out in the Annex to this Decision should also allow to fulfil the requirements of Article 28(3) and (4) of Regulation (EU) 2016/679.

(10) The standard contractual clauses set out in the Annex to this Decision combine general clauses with a modular approach to cater for various transfer scenarios and the complexity of modern processing chains. In addition to the general clauses, controllers and processors should select the module applicable to their situation, so as to tailor their obligations under the standard contractual clauses to their role and responsibilities in relation to the data processing

([5]) Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (OJ L 181, 4.7.2001, p. 19).

([6]) Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010, p. 5).

([7]) 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 (OJ L 281, 23.11.1995, p. 31).

([8]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39); see recital 5.

([9]) C(2021) 3701.

Appendix 3 to the DPA

in question. It should be possible for more than two parties to adhere to the standard contractual clauses. Moreover, additional controllers and processors should be allowed to accede to the standard contractual clauses as data exporters or importers throughout the lifecycle of the contract of which they form a part.

(11) In order to provide appropriate safeguards, the standard contractual clauses should ensure that the personal data transferred on that basis is afforded a level of protection essentially equivalent to that guaranteed within the Union ([10]). With a view to ensuring transparency of processing, data subjects should be provided with a copy of the standard contractual clauses and be informed, in particular, of the categories of personal data processed, the right to obtain a copy of the standard contractual clauses, and any onward transfer. Onward transfers by the data importer to a third party in another third country should be allowed only if the third party accedes to the standard contractual clauses, if the continuity of protection is ensured otherwise, or in specific situations, such as on the basis of the explicit, informed consent of the data subject.

(12) With some exceptions, in particular as regards certain obligations that exclusively concern the relationship between the data exporter and data importer, data subjects should be able to invoke, and where necessary enforce, the standard contractual clauses as third-party beneficiaries. Therefore, while the parties should be allowed to choose the law of one of the Member States as governing the standard contractual clauses, that law must allow for third-party beneficiary rights. In order to facilitate individual redress, the standard contractual clauses should require the data importer to inform data subjects of a contact point and to deal promptly with any complaints or requests. In the event of a dispute between the data importer and a data subject who invokes his or her rights as a third-party beneficiary, the data subject should be able to lodge a complaint with the competent supervisory authority or refer the dispute to the competent courts in the EU.

(13) In order to ensure effective enforcement, the data importer should be required to submit to the jurisdiction of such authority and courts, and to commit to abide by any binding decision under the applicable Member State law. In particular, the data importer should agree to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. In addition, the data importer should have the option of offering data subjects the opportunity to seek redress before an independent dispute resolution body, at no cost. In line with Article 80(1) of Regulation (EU) 2016/679, data subjects should be allowed to be represented by associations or other bodies in disputes against the data importer if they so wish.

(14) The standard contractual clauses should provide for rules on liability between the parties and with respect to data subjects, and rules on indemnification between the parties. Where the data subject suffers material or non-material damage as a consequence of any breach of the third-party beneficiary rights under the standard contractual clauses, he or she should be entitled to compensation. This should be without prejudice to any liability under Regulation (EU) 2016/679.

(15) In the case of a transfer to a data importer acting as a processor or sub-processor, specific requirements should apply in accordance with Article 28(3) of Regulation (EU) 2016/679. The standard contractual clauses should require the data importer to make available all information necessary to demonstrate compliance with the obligations set out in the clauses and to allow for and contribute to audits of its processing activities by the data exporter. With respect to the engagement of any sub-processor by the data importer, in line with Article 28(2) and (4) of Regulation (EU) 2016/679, the standard contractual clauses should in particular set out the procedure for general or specific authorisation from the data exporter and the requirement for a written contract with the sub-processor ensuring the same level of protection as under the clauses.

(16) It is appropriate to provide different safeguards in the standard contractual clauses that cover the specific situation of a transfer of personal data by a processor in the Union to its controller in a third country and reflect the limited self-standing obligations for processors under Regulation (EU) 2016/679. In particular, the standard contractual clauses should require the processor to inform the controller if it is unable to follow its instructions, including if such instructions infringe Union data protection law, and require the controller to refrain from any actions that would prevent the processor from fulfilling its obligations under Regulation (EU) 2016/679. They should also require the parties to assist each other in responding to enquiries and requests from data subjects under the local law applicable

([10]) *Schrems II*, paragraphs 96 and 103. See also Regulation (EU) 2016/679, recitals 108 and 114.

to the data importer or, for data processing in the Union, under Regulation (EU) 2016/679. Additional requirements to address any effects of the laws of the third country of destination on the controller's compliance with the clauses, in particular how to deal with binding requests from public authorities in the third country for disclosure of the transferred personal data, should apply where the Union processor combines the personal data received from the controller in the third country with personal data collected by the processor in the Union. Conversely, no such requirements are justified where the outsourcing merely involves the processing and transfer back of personal data that has been received from the controller and in any event has been and will remain subject to the jurisdiction of the third country in question.

(17) The parties should be able to demonstrate compliance with the standard contractual clauses. In particular, the data importer should be required to keep appropriate documentation for the processing activities under its responsibility and to inform the data exporter promptly if it is unable to comply with the clauses, for whatever reason. In turn, the data exporter should suspend the transfer and, in particularly serious cases, have the right to terminate the contract, insofar as it concerns the processing of personal data under standard contractual clauses, where the data importer is in breach of the clauses or unable to comply with them. Specific rules should apply where local laws affect compliance with the clauses. Personal data that has been transferred prior to the termination of the contract, and any copies thereof, should at the choice of the data exporter be returned to the data exporter or destroyed in their entirety.

(18) The standard contractual clauses should provide for specific safeguards, in particular in the light of the case law of the Court of Justice ([11]), to address any effects of the laws of the third country of destination on the data importer's compliance with the clauses, in particular how to deal with binding requests from public authorities in that country for disclosure of the transferred personal data.

(19) The transfer and processing of personal data under standard contractual clauses should not take place if the laws and practices of the third country of destination prevent the data importer from complying with the clauses. In this context, laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679 should not be considered as being in conflict with the standard contractual clauses. The parties should warrant that, at the time of agreeing to the standard contractual clauses, they have no reason to believe that the laws and practices applicable to the data importer are not in line with these requirements.

(20) The parties should take account, in particular, of the specific circumstances of the transfer (such as the content and duration of the contract, the nature of the data to be transferred, the type of recipient, the purpose of the processing), the laws and practices of the third country of destination that are relevant in light of the circumstances of the transfer and any safeguards put in place to supplement those under the standard contractual clauses (including relevant contractual, technical and organisational measures applying to the transmission of personal data and its processing in the country of destination). As regards the impact of such laws and practices on compliance with the standard contractual clauses, different elements may be considered as part of an overall assessment, including reliable information on the application of the law in practice (such as case law and reports by independent oversight bodies), the existence or absence of requests in the same sector and, under strict conditions, the documented practical experience of the data exporter and/or data importer.

(21) The data importer should notify the data exporter if, after agreeing to the standard contractual clauses, it has reason to believe that it is not able to comply with the standard contractual clauses. If the data exporter receives such notification or otherwise becomes aware that the data importer is no longer able to comply with the standard contractual clauses, it should identify appropriate measures to address the situation, if necessary in consultation with the competent supervisory authority. Such measures may include supplementary measures adopted by the data exporter and/or data importer, such as technical or organisational measures to ensure security and confidentiality. The data exporter should be required to suspend the transfer if it considers that no appropriate safeguards can be ensured, or if so instructed by the competent supervisory authority.

([11]) *Schrems II.*

Appendix 3 to the DPA

(22) Where possible, the data importer should notify the data exporter and the data subject if it receives a legally binding request from a public (including judicial) authority under the law of the country of destination for disclosure of personal data transferred pursuant to the standard contractual clauses. Similarly, it should notify them if it becomes aware of any direct access by public authorities to such personal data, in accordance with the law of the third country of destination. If, despite its best efforts, the data importer is not in a position to notify the data exporter and/or the data subject of specific disclosure requests, it should provide the data exporter with as much relevant information as possible on the requests. In addition, the data importer should provide the data exporter with aggregate information at regular intervals. The data importer should also be required to document any request for disclosure received and the response provided, and make that information available to the data exporter or the competent supervisory authority, or both, upon request. If, following a review of the legality of such a request under the laws of the country of destination, the data importer concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the third country of destination, it should challenge it, including, where appropriate, by exhausting available possibilities of appeal. In any event, if the data importer is no longer able to comply with the standard contractual clauses, it should inform the data exporter accordingly, including where this is the consequence of a request for disclosure.

(23) As stakeholder needs, technology and processing operations may change, the Commission should evaluate the operation of the standard contractual clauses in the light of experience, as part of the periodic evaluation of Regulation (EU) 2016/679 referred to in Article 97 of that Regulation.

(24) Decision 2001/497/EC and Decision 2010/87/EU should be repealed three months after the entry into force of this Decision. During that period, data exporters and data importers should, for the purpose of Article 46(1) of Regulation (EU) 2016/679, still be able to use the standard contractual clauses set out in Decisions 2001/497/EC and 2010/87/EU. For an additional period of 15 months, data exporters and data importers should, for the purpose of Article 46(1) of Regulation (EU) 2016/679, be able to continue to rely on standard contractual clauses set out in Decisions 2001/497/EC and 2010/87/EU for the performance of contracts concluded between them before the date of repeal of those decisions, provided that the processing operations that are the subject matter of the contract remain unchanged and that reliance on the clauses ensures that the transfer of personal data is subject to appropriate safeguards within the meaning of Article 46(1) of Regulation (EU) 2016/679. In the event of relevant changes to the contract, the data exporter should be required to rely on a new ground for data transfers under the contract, in particular by replacing the existing standard contractual clauses with the standard contractual clauses set out in the Annex to this Decision. The same should apply to any sub-contracting to a (sub-)processor of processing operations covered by the contract.

(25) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(1) and (2) of Regulation (EU) 2018/1725 and delivered a joint opinion on 14 January 2021 ([12]), which has been taken into consideration in the preparation of this Decision.

(26) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 93 of Regulation (EU) 2016/679,

HAS ADOPTED THIS DECISION:

Article 1

1. The standard contractual clauses set out in the Annex are considered to provide appropriate safeguards within the meaning of Article 46(1) and (2)(c) of Regulation (EU) 2016/679 for the transfer by a controller or processor of personal data processed subject to that Regulation (data exporter) to a controller or (sub-)processor whose processing of the data is not subject to that Regulation (data importer).

2. The standard contractual clauses also set out the rights and obligations of controllers and processors with respect to the matters referred to in Article 28(3) and (4) of Regulation (EU) 2016/679, as regards the transfer of personal data from a controller to a processor, or from a processor to a sub-processor.

([12]) EDPB EDPS Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries for the matters referred to in Article 46(2)(c) of Regulation (EU) 2016/679.

Appendix 3 to the DPA

Article 2

Where the competent Member State authorities exercise corrective powers pursuant to Article 58 of Regulation (EU) 2016/679 in response to the data importer being or becoming subject to laws or practices in the third country of destination that prevent it from complying with the standard contractual clauses set out in the Annex, leading to the suspension or ban of data transfers to third countries, the Member State concerned shall, without delay, inform the Commission, which will forward the information to the other Member States.

Article 3

The Commission shall evaluate the practical application of the standard contractual clauses set out in the Annex on the basis of all available information, as part of the periodic evaluation required by Article 97 of Regulation (EU) 2016/679.

Article 4

1. This Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. Decision 2001/497/EC is repealed with effect from 27 September 2021.

3. Decision 2010/87/EU is repealed with effect from 27 September 2021.

4. Contracts concluded before 27 September 2021 on the basis of Decision 2001/497/EC or Decision 2010/87/EU shall be deemed to provide appropriate safeguards within the meaning of Article 46(1) of Regulation (EU) 2016/679 until 27 December 2022, provided the processing operations that are the subject matter of the contract remain unchanged and that reliance on those clauses ensures that the transfer of personal data is subject to appropriate safeguards.

Done at Brussels, 4 June 2021.

For the Commission
The President
Ursula VON DER LEYEN

Appendix 3 to the DPA

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

([1]) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE ONE: Transfer controller to controller

8.1 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 **Transparency**

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 **Accuracy and data minimisation**

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

Appendix 3 to the DPA

8.4 **Storage limitation**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation ([2]) of the data and all back-ups at the end of the retention period.

8.5 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

([2]) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

8.7 **Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union [3] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 **Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 **Documentation and compliance**

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 **Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 **Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

(4) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

Appendix 3 to the DPA

MODULE THREE: Transfer processor to processor

8.1 **Instructions**

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter ([5]).

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

([5]) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (6) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(6) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 **Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer processor to controller

8.1 **Instructions**

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

Appendix 3 to the DPA

8.2 **Security of processing**

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data ([7]), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 **Documentation and compliance**

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([8]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

([7]) This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

([8]) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. [9] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

[9] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

Appendix 3 to the DPA

Clause 10

Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. ([10]) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

([10]) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

Appendix 3 to the DPA

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([11]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

([11]) The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Appendix 3 to the DPA

Clause 13

Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller*(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

Appendix 3 to the DPA

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([12]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller*(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

([12]) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Appendix 3 to the DPA

15.1 **Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

Appendix 3 to the DPA

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

[OPTION 2 (for Modules Two and Three): These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

Appendix 3 to the DPA

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify country*).

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of _____ (*specify Member State*).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of _____ (*specify country*).

Appendix 3 to the DPA

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

Appendix 3 to the DPA

ANNEX I

A. **LIST OF PARTIES**

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: .....

Address: .....

Contact person's name, position and contact details: .....

Activities relevant to the data transferred under these Clauses: .....

Signature and date: .....

Role (controller/processor): .....

2. .....

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: .....

Address: .....

Contact person's name, position and contact details: .....

Activities relevant to the data transferred under these Clauses: .....

Signature and date: .....

Role (controller/processor): .....

2. .....

B. **DESCRIPTION OF TRANSFER**

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred

.....

Categories of personal data transferred

.....

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

.....

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

.....

Appendix 3 to the DPA

Nature of the processing

.....

Purpose(s) of the data transfer and further processing

.....

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

.....

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

.....

C. **COMPETENT SUPERVISORY AUTHORITY**

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

.....

Appendix 3 to the DPA

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

For transfers to (sub-) processors, alsodescribe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Appendix 3 to the DPA

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: .....

   Address: .....

   Contact person's name, position and contact details: .....

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): .....

2. .....