Data Processing Agreement

This DPA is entered into between the Controller and the Processor and is incorporated into and governed by the terms of the Agreement.

This Data Processing Addendum ("**DPA**") is incorporated by reference into, and amends, the main agreement, between: (1) the entity named as the Service Provider in the signature section below ("**Service Provider**"); and (2) the entity named as the Customer in the signature section below ("**Customer**"), for the provision by Service Provider to Customer of Service Provider's software and/or services (such software and/or services being the "**Services**" and such agreement being the "**Main Agreement**"). This DPA is deemed to be effective as of the effective date of the Main Agreement (such date being the "**Effective Date**"). Service Provider and Customer are sometimes referred to in this DPA individually as a "**Party**" and collectively as the "**Parties**".

Definitions

In this DPA:

Applicable Law	means as applicable and binding on the Customer, Service Provider and the Services respectively:
	any law, statute, regulation, by-law or subordinate legislation in force from time to time to which a Party is subject and/or in any jurisdiction that the Services are provided to or in respect of;
	the common law and laws of equity as applicable to the Parties from time to time;
	any binding court order, judgment or decree; or
	any applicable direction, policy, rule or order that is binding on a Party and that is made or given by any regulatory body having jurisdiction over a Party or any of that Party's assets, resources or business;
Data Controller	has the meaning given to that term (or to the term 'controller') in Data Protection Laws;

Data Processor	has the meaning given to that term (or to the term 'Processor') in Data Protection Laws;
Data Protection Laws	means Applicable Law relating to the processing, privacy and/or use of personal data including (as applicable and binding on the Customer, Service Provider and the Services respectively): (i) in respect of the United Kingdom ("**UK**"): the Data Protection Act 2018 ("**UK DPA**"); the UK GDPR (which has the meaning given to it in the UK DPA) ("**UK GDPR**"); and the Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019/419; (ii) in respect of the European Union ("**EU**"): the GDPR and all relevant member state laws or regulations giving effect to, replacing or supplementing the same; and (iii) any Applicable Laws amending, extending, replacing, re-enacting or consolidating any of the above from time to time;
Data Protection Losses	means all liabilities arising under Data Protection Laws, including all: costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and to the extent permitted by Applicable Law: administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; compensation which is ordered by a Supervisory Authority to be paid to a Data Subject; and the reasonable costs of compliance with investigations by a Supervisory Authority;
Data Subject	has the meaning given to that term in Data Protection Laws;
Data Subject Request	means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;
EEA	means the European Economic Area;
EU SCCs	means the European Commission's Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 as set out in the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 and as set out in Schedule 3 of

this Agreement, or any set of clauses approved by the European Commission which amends, replaces or supersedes these;

GDPR means the EU's General Data Protection Regulation (Regulation (EU) 2016/679);

International Transfer Clauses means the EU SCCs and, where applicable, the UK Addendum;

Personal Data has the meaning given to that term in Data Protection Laws;

Personal Data Breach means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;

Processing has the meaning given to that term in Data Protection Laws (and related terms such as "**Process**" have corresponding meanings);

Processing Instructions has the meaning given to that term in Section 2.1.1;

Protected Data means Personal Data received by the Service Provider from or on behalf of the Customer in connection with the performance of Service Provider 's obligations under this DPA or otherwise under the Main Agreement;

Sub-Processor means another Data Processor engaged by Service Provider for carrying out Processing activities in respect of the Protected Data on behalf of the Customer;

Supervisory Authority	means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws;
UK Addendum	means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK ICO under section 119A of the Data Protection Act 2018 which came into force on 21 March 2022, incorporated by reference, and by way of this link, and deemed added to in accordance with Section 6.

References to any Applicable Laws (including to the Data Protection Laws and each of them) and to terms defined in such Applicable Laws shall be replaced with or incorporate (as the case may be) references to any Applicable Laws replacing, amending, extending, re-enacting or consolidating such Applicable Law (including the GDPR and any new Data Protection Laws from time to time) and the equivalent terms defined in such Applicable Laws, once in force and applicable.

A reference to a law includes all subordinate legislation made under that law.

1   Data Processor and Data Controller

1.1   The Parties agree that, for the Protected Data, the Customer shall be the Data Controller and Service Provider shall be the Data Processor.

1.2   Service Provider shall Process Protected Data in compliance with Data Protection Laws and the terms of this DPA.

1.3   The Customer warrants, represents and undertakes that:

1.3.1   it shall comply with all Data Protection Laws in connection with the Processing of Protected Data and the terms of this DPA;

1.3.2   all data sourced by the Customer for use in connection with the Services, prior to such data being provided to or accessed by Service Provider for the performance of the Services under this DPA, shall comply in all respects, including in terms of its collection, storage and Processing, with Data Protection Laws (which shall include the Customer obtaining all consents necessarily required, providing all of the required notices and information to Data Subjects and maintaining for the term of this DPA the necessary legal grounds for transferring the Protected Data to Service Provider and allowing Service Provider to perform the Processing contemplated by this DPA);

1.3.3   all instructions given by it to Service Provider in respect of Personal Data shall at all times be in accordance with Data Protection Laws;

1.3.4   it has undertaken due diligence in relation to Service Provider's Processing operations, and it is satisfied that:

(a)   Service Provider's Processing operations are suitable for the purposes for which the Customer proposes to use the Services and engage Service Provider to Process the Protected Data; and

(b)   Service Provider has sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of Data Protection Laws; and

1.3.5   it shall notify the Service Provider in the event of any change to the nature of the Protected Data, including its type and the categories of the relevant Data Subjects.

1.4   The Customer shall not withhold, delay or condition its agreement to any change requested by Service Provider in order to ensure the Services and Service Provider (and each Sub-Processor) can comply with Data Protection Laws.

2   Instructions and details of Processing

2.1   Insofar as Service Provider Processes Protected Data on behalf of the Customer, Service Provider shall:

2.1.1   unless required to do otherwise by Applicable Law, Process the Protected Data as agreed under the Main Agreement and in accordance with Service Provider's standard procedures, this DPA, and Schedule 1 hereto (together, the "**Processing Instructions**");

2.1.2   if Applicable Law requires it to Process Protected Data other than in accordance with the Processing Instructions, inform the Customer of any such requirement before Processing the Protected Data (unless Applicable Law prohibits such information on important grounds of public interest); and

2.1.3   inform the Customer if Service Provider becomes aware of a Processing Instruction that, in Service Provider's opinion, infringes Data Protection Laws, provided that:

(a)   this shall be without prejudice to Section 1.3; and

(b)   to the maximum extent permitted by Applicable Law, Service Provider shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in

connection with any Processing in accordance with the Customer's additional Processing Instructions following the Customer's receipt of that information.

3   Technical and organisational measures

3.1   Service Provider shall implement and maintain the technical and organisational measures set out in Schedule 2, provided that Service Provider reserves the right to make changes to such technical and organisational measures, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects.

3.2   Any additional technical and organisational measures are subject to agreement by Service Provider and shall be at the Customer's cost and expense.

3.3   The Customer shall ensure that, if feasible, any Protected Data in respect of which Service Provider is requested to provide support and maintenance services under this agreement are anonymised prior to Service Provider being granted access to them.

4   Using staff and other Processors

4.1   Customer agrees that Service Provider may engage the Sub-Processors which the Service Provider is using as at the Effective Date. Service Provider will impose on such Sub-Processors data protection terms that protect the Protected Data to the same standard provided for by this DPA. A list of the Sub-Processors Service Provider relies upon as at the Effective Date (and which shall be deemed to be approved by Customer), including their functions and locations, is set out in Schedule 1.

4.2   Service Provider may, upon providing Customer reasonable prior notice, add or make changes to the Sub-Processors it engages. To the extent a new, additional or replacement Sub-Processor is engaged by Service Provider after the Effective Date to Process Protected Data pursuant to this DPA, Customer may object to the appointment of the additional Sub-Processor, provided it does so within 7 calendar days of Service Provider's notice and on reasonable grounds relating to the protection of the Protected Data, in which case Service Provider shall have the right to cure the objection through one of the following options (to be selected at Service Provider's sole discretion):

4.2.1   Service Provider will cancel its plans to use the Sub-Processor with regard to Protected Data or will offer an alternative to provide the Services without such Sub-Processor;

4.2.2   Service Provider will take the corrective steps requested by Customer in its objection (which resolve Customer's objection) and proceed to use the Sub-Processor with regard to Protected Data; or

4.2.3   Service Provider may cease to provide, or Customer may agree not to use, (temporarily or permanently) the particular aspect of the Services that would involve the use of such Sub-Processor with respect to Protected Data, subject to a mutual agreement of the Parties to adjust the remuneration for the Services.

If none of the above options are reasonably available and the objection has not been resolved to the mutual satisfaction of the Parties within 30 days after Service Provider's receipt of Customer's objection, either Party may terminate the Main Agreement for its convenience pursuant to the terms of the Main Agreement, or, if the Main Agreement contains no such terms, on no less than 60 days' advance written notice.

4.3   Service Provider may replace a Sub-Processor without advance notice to Customer if the reason for the change is beyond Service Provider's reasonable control, in which event Service Provider shall notify Customer of the replacement as soon as reasonably practicable and Customer shall retain the right to object to the replacement Sub-Processor pursuant to Section 4.2 above.

4.4   Service Provider shall ensure that all Service Provider personnel authorised to Process Protected Data are subject to a binding written contractual obligation with Service Provider to keep the Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case Service Provider shall, where practicable and not prohibited by Applicable Law, notify the Customer of any such requirement before such disclosure) or are under an appropriate statutory obligation of confidentiality.

5   Assistance with the Customer's compliance and Data Subject rights

5.1   Service Provider shall, taking into account the nature of the Processing, provide commercially reasonable assistance by appropriate technical and organizational measures, as reasonably practicable and insofar as it is possible, to enable Customer to respond to any Data Subject Request, including rights of access, correction, restriction, objection, erasure, or data portability, as applicable. Service Provider shall refer all Data Subject Requests it receives to the Customer within 3 working days of receipt of the request, provided that for unreasonably complex or numerous requests (as determined by Service Provider in its sole and reasonable discretion) the Customer shall pay Service Provider's fees at Service Provider's rates from time to time in force for recording, referring, or otherwise dealing with the Data Subject Requests in accordance with this Section 5.1. For the avoidance of doubt, Customer is responsible for responding to, and meeting the requirements under Data Protection Laws in respect of, Data Subject Requests.

5.2   Service Provider shall provide such reasonable assistance as the Customer reasonably requires (taking into account the nature of Processing and the information available to Service Provider) to the Customer in ensuring compliance with the Customer's obligations under Data Protection Laws with respect to:

   5.2.1   security of Processing;

   5.2.2   data protection impact assessments (as such term is defined in Data Protection Laws);

   5.2.3   prior consultation with a Supervisory Authority regarding high risk Processing; and

   5.2.4   notifications to the Supervisory Authority and/or communications to Data Subjects by the Customer in response to any Personal Data Breach,

provided the Customer shall pay Service Provider's generally applicable fees for providing the assistance in this Section 5.2, including time and materials rates or fees for additional technical measures such as software.

6   International data transfers

6.1   Subject to the terms of the Main Agreement, the Customer agrees that Service Provider may transfer Protected Data to any organisation based in a country, territory or jurisdiction outside the UK or the EEA, provided any such transfer by Service Provider of Protected Data shall be effected in accordance with Data Protection Laws.

6.2   In the event that Customer is subject to the GDPR and transfers Protected Data to Service Provider for Processing outside the EEA, and Service Provider is not subject to the GDPR, and the transfer is not on the basis of an adequacy decision as described in Article 45 of the GDPR; and

   6.2.1   in relation to transfers of Protected Data where Customer is Data Controller and Service Provider is Data Controller, then the Parties shall comply with the Module 1 version of the EU SCCs;

   6.2.2   in relation to transfers of Protected Data where Customer is Data Controller and Service Provider is Data Processor, then the Parties shall comply with the Module 2 version of the EU SCCs; and

   6.2.3   in relation to transfers of Protected Data where Customer is Data Processor and Service Provider is Data Processor (processing the Protected Data on behalf of a third party Data Controller), then the Parties shall comply with the Module 3 version of the EU SCCs.

6.3   In the event that Customer is subject to the UK GDPR and transfers Protected Data to Service Provider for Processing outside the UK, and Service Provider is not subject to

the UK GDPR, and the transfer is not on the basis of an adequacy decision as described in Article 45 of the UK GDPR, the EU SCCs shall apply in accordance with sub-Sections 6.2.(a) to 6.2.(c) (whichever Module is applicable) and shall be deemed amended as specified by the UK Addendum, which shall be deemed executed by the Parties and incorporated into and form an part of this DPA. Where the UK Addendum applies in accordance with this sub-Section 6.3:

6.3.1   (A) Tables 1 and 3 in Part 1 of the UK Addendum shall be deemed completed with the relevant information set out in the Appendix to the EU SCCs and the Schedules of this DPA; (B) in Table 2, the "Addendum EU SCCs" are deemed to be the EU SCCs appended to this DPA including the Appendix Information (as defined in the UK Addendum); and (C) Table 4 in Part 1 is deemed completed by selecting "neither party"; and

6.3.2   any conflict between the terms of the EU SCCs and the UK Addendum will be resolved in accordance with Sections 9, 10 and 11 of the UK Addendum.

7   Information and audit

7.1   Service Provider shall, in accordance with Data Protection Laws, make available to the Customer such information as is reasonably necessary to demonstrate Service Provider's compliance with the obligations of Data Processors under Data Protection Laws.

7.2   Audits by Customer of Service Provider's activities under this DPA will be as set out in the Main Agreement. If the Main Agreement does not include audit rights, Service Provider and Customer will discuss and agree in advance on the reasonable start date, scope and duration of, and security and confidentiality controls applicable to any audit, and Service Provider reserves the right to charge a fee (based on Service Provider's reasonable costs) for any such audit. Audits shall be limited to once per calendar year. Service Provider will provide further details of any applicable fee and the basis of its calculation to Customer in advance of any such audit. Any such audit shall be conducted in such a manner that the Service Provider's undertakings toward third parties (including, but not limited to, the Service Provider's customers, partners, and vendors) are in no way jeopardized. Prior to any audit, all Customer's representatives or external auditors participating in any such audit shall execute customary confidentiality undertakings towards the Service Provider.

8   Breach notification

8.1   In respect of any Personal Data Breach involving Protected Data, Service Provider shall, without undue delay after becoming aware of the Personal Data Breach:

8.1.1   notify the Customer of the Personal Data Breach; and

8.1.2   provide the Customer with details of the Personal Data Breach necessarily required under Data Protection Laws.

9   Term

9.1   This DPA shall remain in force as long as the Service Provider Processes the Protected Data on behalf of the Customer.

10   Deletion or return of Protected Data and copies

10.1   Service Provider shall, at the Customer's written request, either delete or return all the Protected Data to the Customer in such form as the Customer reasonably requests within a reasonable time after the earlier of:

10.1.1   the end of the provision of the relevant Services related to Processing; or

10.1.2   once Processing by Service Provider of any Protected Data is no longer required for the purpose of Service Provider's performance of its relevant obligations under this DPA

unless storage of any data is required by Applicable Law, in which case Service Provider shall inform the Customer of any such requirement.

11   Liability, indemnities and compensation claims

11.1   The Customer shall indemnify and keep indemnified Service Provider in respect of all Data Protection Losses suffered or incurred by, awarded against or agreed to be paid by, Service Provider and any Sub-Processor arising from or in connection with any:

11.1.1   non-compliance by the Customer with the Data Protection Laws;

11.1.2   Processing carried out by Service Provider or any Sub-Processor pursuant to any Processing Instruction that infringes any Data Protection Law; or

11.1.3   breach by the Customer of any of its obligations under Sections 1 to 12 (inclusive), except to the extent Service Provider is liable under Section 11.2.

11.2   Service Provider shall be liable for Data Protection Losses (howsoever arising, whether in contract, tort (including negligence) or otherwise) under or in connection with this DPA:

11.2.1 only to the extent caused by the Processing of Protected Data under this DPA and directly resulting from Service Provider's breach of Sections 1 to 12 (inclusive); and

11.2.2 in no circumstances to the extent that any Data Protection Losses (or the circumstances giving rise to them) are contributed to or caused by any breach of this DPA by the Customer (including in accordance with Section 2.1.3(b)).

11.3 If a Party receives a compensation claim from a person relating to Processing of Protected Data, it shall promptly provide the other Party with notice and full details of such claim. The Party with conduct of the action shall:

11.3.1 make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of the other Party (which shall not be unreasonably withheld or delayed); and

11.3.2 consult fully with the other Party in relation to any such action, but the terms of any settlement or compromise of the claim will be exclusively the decision of the Party that is responsible under this DPA for paying the compensation.

11.4 The Parties agree that the Customer shall not be entitled to claim back from Service Provider any part of any compensation paid by the Customer in respect of such damage to the extent that the Customer is liable to indemnify Service Provider in accordance with Section 11.1.

11.5 This Section 11 is intended to apply to the allocation of liability for Data Protection Losses as between the Parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

11.5.1 to the extent not permitted by Applicable Law (including Data Protection Laws); and

11.5.2 that it does not affect the liability of either Party to any Data Subject.

12   Survival of data protection provisions

12.1 Sections 1 to 13 (inclusive) shall survive termination (for any reason) or expiry of this DPA and continue:

12.1.1 indefinitely in the case of Sections 9 to 13 (inclusive); and

12.1.2 until 12 months following the earlier of the termination or expiry of this DPA in the case Sections 1 to 8 (inclusive), provided always that any termination or expiry of Sections 1 to 8 (inclusive) shall be without prejudice to any accrued rights or remedies of either party under any such Sections at the time of such termination or expiry.

13   Miscellaneous

13.1   In case of any conflict between this DPA and the Main Agreement, the provisions of this DPA shall take precedence as regards the Processing of Protected Data unless expressly stated otherwise herein.

13.2   In the event the International Transfer Clauses apply pursuant to Section 6, in case of any conflict between the main body and Schedules 1 and 2 of this DPA and the International Transfer Clauses, the provisions of the International Transfer Clauses shall take precedence.

13.3   Any claims brought under or pursuant to this DPA or otherwise related hereto shall be subject to the terms and conditions of the Main Agreement, including, but not limited to, the exclusions to and limitations of liability set forth therein which shall apply to the liabilities and indemnities under and in connection with this DPA.

Exhibit B

Technical and Organisational Security Measures

The Processor is ISO 27001 certified and will continue to maintain these certifications and/or other substantially similar or equivalent certifications for the term of the Agreement. The technical and organisational measures defined herein are implemented on the basis of the international standard ISO 27001. The Processor shall maintain controls materially as protective as those provided in ISO 27001 or other substantially similar or equivalent certification requirements.

The Processor utilises third party data centres that maintain current ISO 27001 certifications and/or SSAE 18 SOC 1 Type II or SOC 2 Attestation Reports. The Processor will not utilise third party data centres that do not maintain the aforementioned certifications and/or attestations, or other substantially similar or equivalent certifications and/or attestations.

Upon the Controller's written request (no more than once in any 12 month period), the Processor shall provide within a reasonable time, a copy of the most recently completed certification and/or attestation reports (to the extent that to do so does not prejudice the overall security of the Solution and Services). Any audit report submitted to the Controller shall be treated as Confidential Information and subject to the confidentiality provisions of the Agreement between the parties.

The following descriptions provide an overview of the technical and organisational security measures implemented. It should be noted however that, in some circumstances, in order to protect the integrity of the security measures and in the context of data security, detailed descriptions may not be available, however additional information regarding technical and organisational measures may be found in the Security Policy. It's acknowledged and agreed that the Security Policy and the technical and organisational measures described therein will be updated and amended from time to time, at the sole discretion of the Processor. Notwithstanding the foregoing, the technical and organisational measures will not fall short of those measures described in the Security Policy in any material, detrimental way.

1. **Entrance Control**

Technical or organisational measures regarding access control, especially regarding legitimation of authorised persons:

The aim of the entrance control is to prevent unauthorised people from physically accessing such data processing equipment which processes or uses Personal Data.

Due to their respective security requirements, business premises and facilities are subdivided into different security zones with different access authorisations. They are monitored by security personnel. Access for employees is only possible with a pre-approved security fob for building access and key lock for server room access. All other persons have access only after having registered before at reception.

Access to special security areas for remote maintenance is additionally protected by a separate access area. The constructional and substantive security standards comply with the security requirements for data centres.

2. **System Access Control**

Technical and organisational measures regarding the user ID and authentication:

The aim of the system access control is to prevent unauthorised use of data processing systems being used for the processing of Customer Data.

Remote access to the data processing systems is only possible through the Processor's secure VPN tunnel or equivalent methods with high levels of security. If the users first authenticate to the secure tunnel, after successful authentication authorisation is executed by providing a

unique username and password to a centralised directory service. All access attempts, successful and unsuccessful are logged and monitored.

Additional technical protections are in place using firewalls and proxy servers and state of the art encryption technology that is applied where appropriate to meet the protective purpose based on risk.

3. Data Access Control

Technical and organisational measures regarding the on-demand structure of the authorisation concept, data access rights and monitoring and recording of the same:

Measures regarding data access control are targeted on the basis that only such data can be accessed for which an access authorisation exists and that data cannot be read, copied, changed or deleted in an unauthorised manner during the processing and after the saving of such data.

Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorisation concept. In accordance to the "least privilege" and "need-to-know" principles, each role has only those rights which are necessary for the fulfilment of the task to be performed by the individual person.

To maintain data access control, state of the art encryption technology is applied to the Personal Data itself where deemed appropriate to protect sensitive data based on risk.

4. Transmission Control

Technical and organisational measures regarding the transport, transfer, transmission, storage and subsequent review of Personal Data on data media (manually or electronically).

Transmission control is implemented so that Personal Data cannot be read, copied, changed or deleted without authorisation, during transfer or while stored on data media, and so that it can be monitored and determined as to which recipients a transfer of Personal Data is intended.

The measures necessary to ensure data security during transport, transfer and transmission of Personal Data as well as any other company or Customer Data are detailed in the Security Policy. This standard includes a description of the protection required during the processing of data, from the creation of such data to deletion, including the protection of such data in accordance with the data classification level.

For the purpose of transfer control, an encryption technology is used (e.g. remote access to the company network via two factor VPN tunnel and full disk encryption). The suitability of an encryption technology is measured against the protective purpose.

The transfer of Personal Data to a third party (e.g. customers, sub-contractors, service providers) is only made if a corresponding contract exists, and only for the specific purposes. If Personal Data is transferred to companies located outside the EEA, the Processor provides that an adequate level of data protection exists at the target location or organisation in accordance with the European Union's data protection requirements, e.g. by employing contracts based on the Standard Contractual Clauses.

5. **Data Entry Control**

Technical and organisational measures regarding recording and monitoring of the circumstances of data entry to enable retroactive review.

System inputs are recorded in the form of log files therefore it is possible to review retroactively whether and by whom Personal Data was entered, altered or deleted.

6. **Data Processing Control**

Technical and organisational measures to differentiate between the competences of principal and contractor:

The aim of the data processing control is to provide that Personal Data is processed by a commissioned data processor in accordance with the Instructions of the principal.

Details regarding data processing control are set forth in the Agreement and DPA.

7. **Availability Control**

Technical and organisational measures regarding data backup (physical/logical):

Data is stored in triplicate across 2 data centres, with 2 separate cross connections. The data centres can be switched in the event of flooding, earthquake, fire or other physical destruction or power outage protect Personal Data against accidental destruction and loss.

If Personal Data is no longer required for the purposes for which it was processed, it is deleted promptly. It should be noted that with each deletion, the Personal Data is only locked in the first instance and is then deleted for good with a certain delay. This is done in order to prevent accidental deletions or possible intentional damage.

8. **Separation Control**

Technical and organisational measures regarding purposes of collection and separated processing:

Personal Data used for internal purposes only e.g. as part of the respective customer relationship, may be transferred to a third party such as a subcontractor, solely under consideration of contractual arrangements and appropriate data protection regulatory requirements.

Employees are instructed to collect, process and use Personal Data only within the framework and for the purposes of their duties (e.g. service provision). At a technical level, multi-client capability includes separation of functions as well as appropriate separation of testing and production systems.

Customer Data is stored in a way that logically separates it from other customer data.

The Controller is assigned a unique encryption key, generated using a FIPS 140-2 compliant crypto library, which is used to encrypt and decrypt all of the Controller's archived data. In addition to the unique encryption keys, all data being written to the storage grid includes the Controller's unique account code. The Processor's systems that write data to the storage grid retrieve he encryption key from one system and the customer code from another, which serves as a cross check against two independent systems. The Controller's encryption key is further encrypted with a Processor key stored within a centralised and restricted key management system. In order for the Processor to access Customer Data via the master key, the key management system provisions individual keys following a strict process of approval that includes multiple levels of executive authorisation. Use of these master encryption keys is limited to senior production engineers and all access is logged, monitored, and configured for alerting by security via a centralised Security Incident and Event Management ("SIEM") system. The Controller's archived data is encrypted at rest using AES256 bit encryption and data in transit is protected by Transport Layer Security ("TLS").

Exhibit C

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

---

[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 of 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 [...].

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;

(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);

(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

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.

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.

(a)   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.

(b)   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.

(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 personal data breach, including measures to mitigate its possible adverse effects.

---

[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.

(d)   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.

(e)   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.

(f)   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.

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

---

[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.

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.

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.

---

[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.

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.

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].

---

[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.

8.2   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).

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;

(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.

---

[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.

(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.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a)   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 14 days 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.[7] 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 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

---

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

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)   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 14 days 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 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.[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.

(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.

---

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

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.[9] 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

---

[9]   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.

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.

(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.

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.

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.

(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

(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.

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

(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;

(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[10];

(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.

---

[10]   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.

technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation (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 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

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.

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 (and the controller, where applicable) 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.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

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 Ireland.

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 Ireland.

(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.