DATA PROCESSING AGREEMENT

THE UNDERSIGNED

[Company XYZ], registered and maintaining its office at [building], [street], [postal code], [city], [country], herein legally represented by Mr/Mrs [name], hereinafter referred to as "[**Data Controller**]**"** or the "**Controller**";

and

The private company with limited liability **Directness B.V. (CustomerGauge)**, with its registered office van Diemenstraat 182, in this matter represented by its director Mr Adam Dorrell, hereinafter referred to as "**CustomerGauge"** or "**Processor**";

hereinafter to be jointly referred to as: "**Parties**" and individually as "**Party**";

TAKING INTO CONSIDERATION THAT:

- Parties have entered into an Agreement (Terms of Service CustomerGauge) with respect to the Provisioning of the "CustomerGauge" Net Promoter Measurement platform via Software as a Service (Cloud) solution to support Data Controllers activities to gauge the loyalty of Data Controllers customers hereinafter: '**Agreement**'. Data Controller will upload all required event based customer and mobility user survey related data to the Net Promoter Measurement platform, which manages and reports on event based submitted surveys. These services (as per the Terms of Service) may involve the processing of personal data in the sense of the applicable legislation for the protection of personal data, currently the General Data Protection Regulation (GDPR);
- For the processing on behalf of the client, CustomerGauge functions as the Processor and the client as the Controller in the sense of the applicable legislation for the protection of personal data, as the former will process personal data for the latter, without being subject to its authority and the Controller determines the purposes and the means of the processing

of personal data, on the understanding that details of the means can be determined by Controller considering its specific expertise;

- As part of the Agreement, Controller and CustomerGauge subsequently wish to enter into this data processing agreement (hereinafter: "Data Processing Agreement").

DECLARE TO HAVE AGREED AS FOLLOWS, TAKING INTO ACCOUNT THE ABOVE:

1 Definitions

1.1 In addition to the definitions (such as data subject and processing) as used in the applicable legislation for the protection of personal data (currently the General Data Protection Regulation), the following terms are used in this Data Processing Agreement, each written with a capital letter, whether the definitions are used in plural or singular:

Agreement:	the agreement (Terms of Service) entered into between the Controller and the Processor
Annex:	appendix to the Data Processing Agreement, which forms an integral part of this Data Processing Agreement;
Data Processing Agreement:	this agreement which forms part of the Agreement;
Data Protection Law:	the applicable legislation for the protection of personal data, currently General Data Protection Regulation (GDPR);
Personal Data:	the personal data as referred to in the Data Protection Law, which are processed by the Processor for the benefit of the Controller under the Agreement.
Standard Contractual Clauses	means the Standard Contractual Clauses (EU) 2021/914 as of 4 June 2021. Any reference made to the Standard Contractual Clauses herein, shall refer to the Standard Contractual Clauses document available in Annex A and B to this DPA.

Paraph: Paraph:

2 Applicability and actual processing

2.1 The Processor shall process Personal Data solely on the written instructions from the Controller (including the assignment as set out in the Agreement) or where an applicable statutory provision or a judicial order should compel Processor to do so or is required by legitimate request from a competent supervisory authority (such as the Dutch Data Protection Authority). This does not affect the responsibility of the Controller to ensure that its instructions are compliant with the applicable legislation. Insofar such instructions entail additional work (and costs) for the Processor or/and have consequences for an agreed time schedule, Parties first have to reach an agreement on such matters.

2.2 The Processor shall process the Personal Data in a lawful and fair manner in accordance with its obligations as the Processor under this Processing Agreement and the Data Protection Law. The categories of personal data, categories of data subjects, nature and purpose of the processing set and specified by the Controller as well as the processing operations specified by the Processor and the categories of employees involved are set out in Annex A to this Data Processing Agreement.

2.3 The Controller is responsible for Personal Data being accurate and kept up to date. The Controller is also obliged to verify the Personal Data being accurate and up to date.

2.4 The Controller guarantees the Processor that the processing of the Personal Data commissioned by or on behalf of the Controller is not unlawful and does not infringe the rights of data subjects, and that the Personal Data have been obtained in a manner that is compliant with the applicable statutory regulations.

2.5 In so far as this is reasonably within the Processor's control and with due consideration for the nature of the Processing, the Processor shall support the Controller, in so far as possible and by means of appropriate technical and organizational measures, in meeting its statutory obligation under the Data Protection Law, more specifically the rights of parties involved, such as: (i) making available for the party involved a copy of their processed personal data or otherwise allow this party to gain insight in these data, thereby taking into account both the protection of data of others and the confidentiality of

other data that are confidential in their nature, (ii) deleting, correcting or supplementing personal data, and/or (iii) demonstrating that personal data have been deleted or corrected, (iv) enabling the party involved to exercise other rights under the Data Protection Law. The Processor shall be entitled to charge the Controller for any costs involved.

2.6 This Data Processing Agreement forms an integral part of the Agreement and the provisions therein apply in full to this Data Processor Agreement; in the event a provision of this Data Processing Agreement should conflict with a provision of the Agreement, the provision in this Data Processing Agreement shall prevail over the provision of the Agreement.

3 Protection of Personal Data & Control

3.1 The Processor shall implement appropriate technical and organizational measures, taking into account the state of the art and the costs of implementation, appropriate to the known nature of the Personal Data and the assignment of processing the Personal Data, to protect Personal Data from loss, or unlawful processing, as referred to in the Data Protection Law (Article 32 GDPR) with due observance of the provisions of the Agreement (including this Data Processing Agreement).

3.2 The Processor has taken measures to provide appropriate continuity and security of service. A certification or statement is available to support these measures.

3.3 The Controller shall immediately inform the Processor of any instruction, order or other notice given by a competent relevant supervising authority concerning the Personal Data.

4 Audit

4.1 The Controller shall be entitled to supervise compliance with the responsibilities of the Processor in this Data Processing Agreement. Upon the Controller's request, the Processor shall enable the Controller to such supervision once a year on a date, at a time and within a scope to be determined by parties in mutual consultation. In addition to the previous, the

Controller – on a date, at a time and within a scope to be determined by parties in mutual consultation – shall be entitled to supervise compliance with the responsibilities of the Processor in this Data Processing Agreement more often than once a year if the Controller sees cause to do so because of a reasoned suspicion of non-compliance.

4.2 The Processor shall enable the supervisory authority (the Dutch Data Protection Authority), at its request, to supervise the processing activities as performed by Processor on behalf of Controller under the Agreement. Processor shall inform Controller thereof.

4.3 The Processor shall in all reasonableness and at the charge of the cost support the audit referred to in 4.1 and 4.2.

4.4 The Controller shall bear the costs of the investigation referred to under 4.1 and 4.2, except where and to the extent that the outcome of such investigation leads to the apparent conclusion that the Processor has imputably failed its obligations laid down in article 3.1, in which event the Processor will bear the reasonable actual costs of the investigation after producing the underlying invoices.

4.5 The Controller shall be assisted by an independent certified IT auditor in the investigation referred to under article 4.1. This person must be prepared to sign a non-disclosure agreement prior to the investigation.

4.6 The investigation, which will also extend to the documentation and other data involved in the investigation, and the outcome of the investigation shall be treated with strict confidentiality by the Controller and by the auditor as referred to under 4.5, unless and to the extent any applicable statutory provision and/or request of a competent authority should compel them to disclose any of their findings.

4.7 The Controller shall see to it that the investigation referred to under 4.1 is carried out in such a way that the Processor will be inconvenienced as little as possible and under the conditions that both the protection of personal data of third parties and the confidentiality of the data of third parties that are confidential in their nature are guaranteed.

4.8 The Controller shall make available for the Processor, as soon as possible, a complete and unmodified copy of the investigation's relevant outcome in a structured, commonly used and (machine-)readable format.

4.9 Parties shall consult each other regarding the outcome as referred to under 4.8 in order to take necessary measures to comply with the provisions laid down in article 3.1 within a reasonable period of time.

4.10 As soon as possible after Parties have received any instruction, whether binding or not, from the supervisory authority (the Dutch Data Protection Authority) to amend the organizational and protection measures, Parties shall consult each other in order to take the required measures to comply with the instruction and to determine who will bear which costs.

4.11 In the event the statutory provision in the applicable legislation for the protection of personal data should be amended, Parties shall consult each other as soon as possible, in order to make the required adjustments in the technical and organizational measures and/or this Data Processing Agreement and to determine who will bear which costs.

5. Confidentiality

5.1 The Processor is obliged to observe confidentiality with respect to the Personal Data that are provided by the Controller, except where an applicable statutory provision, a judicial order or legitimate request from a competent relevant supervisory authority should compel the Controller or Processor to disclose such data or where this should necessarily arise from the Agreement (including the Data Processing Agreement) or should arise from an additional, written instruction by the Controller.

5.2 The Processor shall see to it that anyone acting under its instructions is obliged to observe confidentiality as referred to in the previous paragraph with respect to the Personal Data they become aware of.

5.3 If the Processor has to provide Personal Data on the basis of an applicable statutory provision, the Processor will verify the grounds of the request and the identity of the applicant, and will inform the Controller prior to complying this request, unless applicable laws and regulations prohibit this.

6. Data Breach Notification

6.1 Upon becoming aware of a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the personal data transmitted, stored or otherwise processed by the Processor on behalf of the Controller under the Agreement (**Breach**), the Processor shall, without undue delay, (i) notify the Controller in compliance with the Data Protection Act; and (ii) take reasonable measures in accordance with 3.1 to prevent (further) breach and/or limit the breach.

6.2 The Processor shall support the Controller and keep the Controller informed, in all reasonableness and fairness, taking into consideration the nature of the processing and the information that has been made available, with respect to personal data breach and new developments in the field of personal data breach.

6.3 The notification referred to under article 6.1 shall take place though email/phone/text to [contact information contact].

6.4 The Processor shall, where necessary, assist the Controller informing the supervisory authority and data subjects concerned adequately, regarding the Personal Data Breach, in accordance with the Data Protection Law.

6.5 Without prejudice to the provisions laid down in article 5.1 and insofar as necessary for legal defence, Parties will maintain strict confidentiality regarding Breaches and will only report Breaches to the supervisory authority and data subject(s) concerned, in accordance with the provisions of the Data Protection Law. With the provision that if data subjects can only be informed through non-individual media, the Controller is entitled to use such non-individual media to inform data subjects with due regard for the interests of the Processor, in accordance with the relevant policy rules of the Dutch Data Protection Authority.

7. Use of sub-processors

7.1 The Processor shall be entitled to subcontract any of its activities that exist or partially exist of processing Personal Data, or that require Personal Data to be processed, to subcontracted processors ("sub-processors") that are established in the European Economic Area. The Processor shall not be entitled to subcontract any of its activities that exist or partially exist of processing Personal Data, or that require Personal Data to be processed to any third party that is established outside the European Economic Area without the Controller's prior consent in writing, which consent shall not be unreasonably withheld.

7.2 When subcontracting a sub-processor, the Processor will impose the sub-processor the same data protection obligations as set out in this Data Processing Agreement, unless a data processing agreement (EU model contracts c/q standard contractual clauses decision of the EC) has been or has to be entered into between the third party and the Controller directly in respect to the relevant processing.

8. Liability

8.1 The Controller is fully responsible and is therefore fully liable for the intended purpose of the processing, the content of the Personal Data entered by or on behalf of it or otherwise provided, its instructions, including the provision to third parties, the duration

of the storage of the Personal Data, the ways of processing and the means used for that purpose, except in so far as any act or omission is attributable to the Processor.

8.2 Processor is under no circumstances liable for a fine imposed on the Controller by the Dutch Data Protection Agency in the event the Dutch Data Protection Agency has taken the degree to which blame can be attributed into consideration and has imposed the fine(s) accordingly on the Party/Parties concerned. For the remainder, the liability arrangements as included in the Agreement apply.

9. Term and consequences of termination (retention period)

9.1 The term of this Data Processing Agreement is equal to the term of the Agreement from the date the Data Processing Agreement is signed by both parties. In the event the Agreement ends, this Data Processing Agreement will end by operation of law. The Data Processing Agreement cannot be terminated prematurely separately of the Agreement.

9.2 Any obligations which, according to their nature, are meant to remain in force after the termination (*ontbinding*) of this Data Processing Agreement shall continue to apply after its termination. The relevant provisions include, amongst other things, obligations arising from provisions with respect to confidentiality, liability and applicable law.

9.3 After the Data Processing Agreement's term has expired, the Processor shall be obliged – without undue delay and at the Controller's option – (a) to render its cooperation, upon the Controller's request and at the Controller's expense, to provide a back-up of the Personal Data that are under the Processor's control on the Processor's system, within a reasonable period of time after the end of the Agreement, in a then current readable standard format and on a then current standard medium; or (b) to delete the Personal Data that are under the Processor's control on the Processor's system; and (c) to remove all existing copies, unless a statutory provision should provide otherwise. The Processor shall be entitled to charge the Controller for any costs involved. The Controller shall be obliged to inform the Processor of its choice for sub a or b in due time and in writing

before the end of the Agreement, unless this cannot be reasonably expected from the Controller, in which event the reasoned request is to be sent to the Processor ultimately within two calendar weeks following the end of the Agreement unless Parties agree upon another period within the context of an exit strategy.

9.4 No amendments of this Data Processing Agreement shall be binding upon either Party, unless it is in writing and duly signed by both Parties.

10. International Data Transfer

10.1 In the event of an International Data Transfer, meaning any processing (including transfers and onward transfers) of Personal Data originating from or via Controller from the EEA, a Country with an EU adequacy decision, or a country with similar adequacy requirements as contained in Art. 45 et seq. GDPR, by Provider or any of its Subprocessors outside the EEA and outside a Country with an EU adequacy decision, such processing shall be done by Processor in line with (i) a decision by the European Commission in the meaning of Art. 45 GDPR or (ii) appropriate safeguards as required by Article 46 GDPR.

10.2 If an International Data Transfer is based on the Standard Contractual Clauses, the following shall apply:

a) *If the Provider is located outside the EEA, the Restricted Transfer shall be governed by Modules 2 and 3 of the Standard Contractual Clauses which are incorporated herein by reference. Controller enters into the Standard Contractual Clauses as data exporter acting as (a) Controller (in which case Module 2 of the Standard Contractual Clauses applies), and (b) Processor for its Affiliates (in which case Module 3 of the Standard Contractual Clauses applies).*

b) If Processor commissions a Subprocessor located outside the EEA, the Processor shall enter into the Standard Contractual Causes (Module 3) with such Subprocessor.

c) Any further onward transfer must comply with the applicable Module of the Standard Contractual Clauses. In case Controller is located outside the EEA and acts as a data importer under Standard Contractual Clauses with its Affiliates, the third-party beneficiary clause stipulated by Clause 9 (e) of the Standard Contractual Clauses shall be in favor of the respective Affiliate acting as the data exporter under such Standard Contractual Clauses.

d) The Parties are aware that the applicable Data Protection Law or enforcement practice of data protection authorities in countries located outside the EEA (such as the United Kingdom), does not recognized the Standard Contractual Clauses (EU) 2021/914 as adequate mean to protect international data transfers, but continues to rely on the the Standard Contractual Clauses 2010/87/EU. In this case, international data transfers originating from Controllers located in such countries, shall additionally be governed by the Standard Contractual Clauses 2010/87/EU, which are incorporated herein by reference.

e) In case an International Data Transfer is not based on Standard Contractual Clauses, Clause 14 and 15 of the Standard Contractual Clauses shall apply mutatis-mutandis to such transfer under, unless the respective International Data Transfer contains in substance, the same rights and obligations concerning (i) local laws and practices affecting compliance with the Data Protection Law, and (ii) obligations in case of access by public authorities as contained in Clauses 14 and 15 of the Standard Contractual Clauses.

f) Processor agrees and understands that local Applicable Data Protection Law (including in jurisdictions other than those addressed in the first paragraph), may contain similar or additional transfer restrictions. In such case Provider agrees to use reasonable efforts and to cooperate with Controller in good faith to address those requirements.

11. Disputes and governing law

11.1 This Data Processing Agreement shall be governed by the laws of the Netherlands.

11.2 All disputes arising from the performance of this Data Processing Agreement shall be submitted to the competent judge or arbitrator as agreed upon in the Agreement.

Accepted:	**Accepted:**
Directness B.V. (CustomerGauge) Address: van Diemenstraat 182, 1013 CP Place: Amsterdam Country: The Netherlands	**[Company name]** ..... Address: Place: ..... Country: .....
On behalf of Directness B.V. Name: ..... Date: ..... Place: ..... Signature:	On behalf of [company name]: Name: ..... Date: ..... Place: ..... Signature: .....
Paraph:	Paraph:

Annex A – GDPR Compliant Personal Data Statement

Overview of the processing purpose, the categories of Personal data, categories of data subjects, processing operations and the categories of employees involved.

Type Personal data (e.g. Name and address details, financial records)	**Processing purpose**	**Type of employees** (categorised by position, e.g. helpdesk employees, systems administrators)	**Processing acts of the employees** (categorized per position E.g. maintenance, hosting, support.	**Type of data subject involved** (e.g. job applicant)	**Duration of Processing**
Name	*Customer Experience*	*Helpdesk, Account Managers, Senior Managers, Admins*	*To improve customer experience*	*Customers*	*Life of customer contract (and beyond if appropriate)*
Company name					
Email					
Job Role					
Job Title					
Phone Number					
Company Revenue/demographics					
Location					
Customer Comment and Score					
Account Manager/Agent Name					
Product Purchase/Usage					
(Login Details)					

Paraph: Paraph:

Annex B

Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council based on Commission Implementing Decision (EU) 2021/914 of 4 June 2021

SECTION I

Clause 1, Purpose and scope

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) for the transfer of personal data to a third country.

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 IA (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 the DATA PROCESSING AGREEMENT (hereinafter each 'data importer')

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

These Clauses apply with respect to the transfer of personal data as specified in the DATA PROCESSING AGREEMENT.

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

Clause 2 Effect and invariability of the Clauses

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

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

Clause 3 Third-party beneficiaries

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); Module Four: Clause 18.

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

Clause 4 Interpretation

1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
3. 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.

Paraph: Paraph:

Clause 6 Description of the transfer(s)

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

Clause 7 – Optional Docking clause

1. 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.
2. 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.
3. 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:

1. where it has obtained the data subject's prior consent;
2. where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
3. where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

1. (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:
1. (i) of its identity and contact details;
2. (ii) of the categories of personal data processed;
3. (iii) of the right to obtain a copy of these Clauses;
4. (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.

2. (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.

3. (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.

4. (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

1. (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.

2. (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.

3. (c) The data importer shall ensure that the personal data is adequate, relevant and limited to

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

1. (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.

2. (b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
3. (c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
4. (d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
5. (e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
6. (f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.
7. (g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

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

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses,

under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

1. (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;
2. (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;
3. (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;
4. (iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
5. (v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or
6. (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

1. (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.
2. (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

1. (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.
2. (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 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.

2. (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.
3. (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.
4. (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 (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:

1. (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;
2. (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;
3. (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
4. (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

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

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

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

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

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

MODULE THREE: Transfer processor to processor

8.1 Instructions

1. (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.
2. (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.

3. (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.

4. (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.

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

1. (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.
2. (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.
3. (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.
4. (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 (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:

1. (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;
2. (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;
3. (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
4. (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

1. (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.
2. (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.
3. (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.
4. (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.
5. (e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
6. (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.
7. (g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

1. (a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
2. (b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
3. (c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.
4. (d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

1. (a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
2. (b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.
3. (c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

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

Clause 9 Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) ***OPTION 1: SPECIFIC PRIOR AUTHORISATION*** The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least thirty (30) days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) 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.

2. (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. 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.
3. (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.
4. (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.
5. (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

1. (a) ***OPTION 1: SPECIFIC PRIOR AUTHORISATION*** The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least thirty (30) days prior to the engagement of the sub-processor, together with the information necessary

to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

2. (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. 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.

4. (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.
5. (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.

Clause 10 Data subject rights

MODULE ONE: Transfer controller to controller

1. (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. 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.

2. (b) In particular, upon request by the data subject the data importer shall, free of charge:
1. (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);
2. (ii) rectify inaccurate or incomplete data concerning the data subject;
3. (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.
3. (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.
4. (d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

- inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
- 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.

5. (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.
6. (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.
7. (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

1. (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.
2. (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.
3. (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

1. (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.
2. (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.
3. (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

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

Clause 11 Redress

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

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 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:

1. (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;
2. (ii) refer the dispute to the competent courts within the meaning of Clause 18.

4. (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.
5. (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
6. (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

1. (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.
2. (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.
3. (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.
4. (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.
5. (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

1. (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.
2. (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.
3. (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.

4. (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.
5. (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.
6. (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.
7. (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

1. (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.

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

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

Clause 14
Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

1. (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.
2. (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
1. (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;
2. (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;
3. (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.

3. (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.
4. (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
5. (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.
6. (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

15.1 Notification

1. (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:
1. (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

2. (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.***]***

2. (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.

3. (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.]

4. (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.

5. (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

1. (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).

2. (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.]

3. (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

1. (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
2. (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).
3. (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
1. (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;
2. (ii) the data importer is in substantial or persistent breach of these Clauses; or
3. (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

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

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

Clause 17 Governing law

MODULE ONE: Transfer controller to controller MODULE TWO: Transfer controller to processor MODULE THREE: Transfer processor to processor

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

MODULE FOUR: Transfer processor to controller

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

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

1. (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
2. (b) The Parties agree that those shall be the courts of Germany.
3. (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.
4. (d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of Amsterdam.