JET - DATA PROCESSING AGREEMENT (DPA)

PARTIES

This DPA is entered into between JET ("JET" "we" or "us"), and ("Supplier", "you"). Capitalised terms used herein but not defined in this DPA shall have the meaning assigned to them in the Agreement.

DEFINITIONS

- **Agreement** means the commercial agreement executed between the parties in relation to performance of Services, and for clarity includes any relevant Service Orders, Order Forms, Statements of Work, or other contract documents which form part of the agreement under which you provide the Services to us.
- **Data Processing Particulars** means the instructions and details of the personal data processing to be performed by you, including the subject matter, duration, nature and purpose, and the types and categories of personal data, as set forth in the Agreement.
- **Data Protection Legislation** means all laws, regulations and regulatory guidance containing rules for the protection of individuals with regard to the Processing of Personal Data including applicable national, federal, provincial or state legislation and/or binding regulations (e.g. GDPR) implementing or made pursuant to them, as amended or updated from time to time and/or any successor legislation.
- **Controller** has the meaning given to them in the Data Protection Legislation.
- **Processor** has the meaning given to them in the Data Protection Legislation.
- **GDPR** means 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, as may be amended from time to time.
- **JET** means the JET entity referred to above with which you have entered into the DPA (and "our", "us" and "we" shall be construed accordingly).
- **JET Personal Data** means Personal Data provided or made available by us JET to you as a Data Processor under this DPA.
- **EU Model Clauses** means the standard contractual clauses approved by the EU Commission for the transfer of personal data subject to GDPR to processors established in third countries, as applicable and available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en or any other standard contractual clauses issued by the EU Commission , which replace such clauses from time to time, each of which are hereby incorporated into this DPA as if they have been set out in full herein.
- **UK International Data Transfer Agreement** means the International Data Transfer Addendum to the EU Model Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022, or any other transfer safeguard issued by the UK Information Commissioner or governing agency such as the introduction of the US data bridge, which may replace such current safeguards from time to time, which is hereby incorporated into this DPA as if they have been set out in full herein.
- **Personal Data** means as defined in the Data Protection Legislation.
- **Personnel** means any employee, agent, contractor, work-for-hire or any other person working or assigned under the direct authority of Processor
- **Processing** means as defined in the Data Protection Legislation. "Process" or "Processed" shall be construed accordingly.
- **Security Incident** means the reasonably suspected or actual accidental or deliberate or unlawful or unauthorised acquisition, destruction, loss, alteration, access, use or disclosure of JET Personal Data transmitted, stored or otherwise Processed, or any other breach in the protection of such information, including any violation or attempted violation by any person of any obligation concerning the confidentiality of Personal Data in the meaning ascribed to in Data Protection Legislation in connection with this DPA or any other breach of Clause 9.
- **Services** means the services to be provided by you in connection with this DPA, as further set out in the Agreement.
- **Security Measures** means the physical, technical, organisational security measures necessary to ensure the adequate protection of Personal Data, in compliance with Data Protection Legislation and which are set out in Annex 1 of this DPA.

PROCESSING PERSONAL DATA

You agree that the obligations contained in this DPA shall be complied with by you where you are instructed to Process JET Personal Data for the purpose of procurement of the Services to us and within the scope of nature and purpose of the processing, categories of data subjects and Personal Data as set out in the Data Processing Particulars .

1 Relationship of the parties

JET, as the Controller, or as authorised by a JET Affiliate which is the Controller, appoints you as a Processor to Process the JET Personal Data described in the Data Processing Particulars. In this context, applicable Data Protection Legislation may not define Controllers or Processors as defined under the GDPR, however comparable concepts of security supervisors, database owners, and database managers or possessors serve as the equivalent of Controller or Processor under GDPR but as defined under applicable Data Protection Legislation and as set-out in this DPA for the purpose of safe custody or processing on behalf of JET.

2 Data Processing

a. You shall Process JET Personal Data as a Processor only for the purposes described in the Agreement, as set out in this DPA or as necessary to perform your obligations under this DPA and strictly in accordance with JET's instructions as set out in this DPA or as provided in writing by us from time to time, except with the consent of the individual to whom the Personal Data relates to the extent and in the manner required by Data Protection Legislation.

b. If you are ever unsure about our instructions, you should contact us to seek clarification or further instructions as soon as possible.

3 Compliance with Data Protection Legislation

a. You represent and warrant that you shall:

i. comply at all times with the Data Protection Legislation;

ii. process all JET Personal Data in accordance with applicable Data Protection Legislation and notify us promptly, without undue delay, if in the delivery of the Services or performance of the Processing activities covered by this DPA (as an experienced supplier of such services), you identify any potential areas of actual or potential non-compliance with the Data Protection Legislation;

iii. except to the extent you perform this processing solely to provide the Services to us or otherwise with our prior written

consent, not (a) convert any JET Personal Data into anonymised, pseudonymised, depersonalised, aggregated or statistical data; or (b) use any JET Personal Data for "big data" analysis or purposes; additionally, you will not match any JET Personal Data with or against any other Personal Data which would (i) put us in breach of our obligations under Data Protection Legislation or (ii) impact the confidentiality, integrity and availability of systems used to Process JET Personal Data;

iv. not use Personal Data forming part of the JET Personal Data for any purpose which may be inconsistent with the instructions of JET and with those notified to the Data Subjects on or before the time of collection. (whether yours or any third party's);

b. JET is entitled to temporarily suspend the Processing in whole or in part if you are unable to meet your obligations under the DPA until such time that the non-compliance is remedied. To the extent such remedy is not available, JET is entitled to terminate the relevant part of the Processing with immediate effect. JET is also entitled to terminate the DPA with immediate effect if suspension of the Processing by JET pursuant to this provision exceeds a period of six (6) calendar months.

4 Confidentiality and Your Personnel

a. You shall ensure that your Personnel are (i) contractually bound and obligated to maintain the security and confidentiality of any JET Personal Data as set out in this DPA, or are otherwise subject to statutory obligations of confidentiality to the same extent and (ii) informed of and comply with the obligations of this DPA. You will provide your Personnel access to JET Personal Data only to the extent necessary to perform the Processing and in compliance with the applicable Data Protection Legislation and this DPA..

b. You shall ensure that only your Personnel (including contractors) who are required to have access to JET Personal Data shall have such access. You will ensure that all such Personnel (including contractors) are aware of the Data Protection Legislation, our instructions and your obligations under it and this DPA and have received suitable and sufficient training in the care and handling of any JET Personal Data.

c. You shall keep and maintain JET Personal Data confidential and will not disclose Personal Data in any way without the prior written approval of JET, except where, (i) the disclosure is required for the performance of the Processing, or (ii) where JET Personal Data needs to be disclosed to a competent public authority to comply with a legal obligation or as required for audit purposes, or (iii) as otherwise required by law. If a law or court order compels you to disclose Personal Data, you must first inform us of the legal requirement and give us an opportunity to object or challenge the requirement, unless the law or court order prohibits such notice to us.

d. Except where Data Protection Legislation provides otherwise, you shall keep a record of any disclosure that is made for a minimum period of six months from the date of the disclosure.

e. The obligation of confidentiality under this article shall continue to apply following the termination of this DPA.

5 Data subject rights

You shall promptly, and in any event no later than five (5) business days after receiving a request, forward to us and otherwise cooperate with and assist us including by way of appropriate technical and organisational measures any requests from data subjects (and other third party requests, including from any national regulator) of any JET Personal Data pursuant to Data Protection Legislation (including the ability to correct, delete, block or port JET Personal Data and rights of access and disclosure).

6 Deletion or return of JET Personal Data

a. Subject to applicable law and upon our written request, you shall either delete in such a way that the Personal Data will no longer be able to be used and will have been rendered inaccessible; or return all copies (if requested in a machine-readable format), whether written, electronic or other form of media, of JET Personal Data and cease Processing such JET Personal Data, in each case using Security Measures.

b. You shall cease Processing JET Personal Data at the earliest of (a) after the business purposes for which the JET Personal Data was Processed have been completed (b) the termination of this DPA and/or (c) upon request of JET at any time. JET may require you to promptly confirm and warrant in writing that you have returned, deleted and/or destroyed all copies of JET Personal Data.

c. Until the JET Personal Data is deleted or returned as described in clause 6(a), you shall continue to ensure compliance with this DPA. In case local laws applicable to you prohibit return or deletion of JET Personal Data, you warrant and represent that you will continue to ensure compliance with this DPA and you will only process such JET Personal Data to the extent and for as long as required under that local law.

7 Records

You shall maintain a record of all categories of Processing activities (as defined and set out in applicable Data Protection Legislation) carried out on behalf of JET which shall be made available to us upon request. The records shall be kept in writing including in electronic form and you (or where applicable, your representative) shall make the records available to us and to the supervisory authority on request.

8 Security

a. You have implemented and will maintain appropriate Security Measures, internal controls and information Security Measures routines intended to protect JET Personal Data against accidental, unauthorised or unlawful access, disclosure, alteration, loss, or destruction to ensure a level of security appropriate to the risk presented by Processing JET Personal Data. These shall at all timesbe of at least the minimum standard required by Data Protection Legislation and be consistent with good industry practice for the protection of Personal Data.

b. You shall comply with the JET Third Party Security Standards (available here: https://s205.q4cdn.com/266311280/files/doc_downloads/2025/04/Third-Party-Security-Standard-for-Suppliers.pdf) in force and as may be amended from time to time and JET's Technical and Organisational Measures to ensure the security of data as set out in Annex 1 of this DPA.

c. JET may request the Processor to implement further Security Measures and the Processor shall be obliged to adjust the Security Measures being applied if such adjustment is necessary for a continued provision of an appropriate level of security.

d. The Processor shall ensure that the Security Measures it implements and will implement are appropriate and adequate for the execution and procurement of the Services under this DPA.

9 Notification of incidents

a. You shall notify us without delay (and in any event within twenty-four (24) hours) of any Security Incident and we shall be entitled to conduct any verification relating to confidentiality requirements. You must:

b. notify us via JET DPO Office address privacy-concerns@takeaway.com of the Security Incident, provide us with as much information as possible and regularly update the content of the information without undue delay in accordance withData Protection Legislation. Such information shall include, but not be limited, to:

(i) the nature of the incident;

(ii) how and when the Security Incident was discovered;

(iii) the date, time and duration of the Security Incident and who may have had access to the Personal Data;
(iv) the categories and number of data subjects affected by the Security Incident;
(v) which types/categories of Personal Data were involved with the Security Incident;
(vi) what type of Security Measure(s) were breached;
(vii) whether there is evidence of criminal or malicious intent;
(viii) whether and, if so, which measures were taken to mitigate possible adverse effects of the Security Incident and to prevent future incidents;
(ix) description of likely adverse consequences of the Security Incident; and
(x) any further information necessary for JET to determine if the Security Incident creates a real risk of significant harm to a data subject, or is otherwise required by us in order to comply with data breach notification requirements under applicable Data Protection Legislation.

c. Immediately following your notification to us of a Security Incident, the parties shall coordinate with each other to investigate the Security Incident. You agree to fully cooperate with us in our handling of the matter, including, without limitation: (i) assisting with any investigation; (ii) providing us with physical access to the facilities and operations affected; (iii) facilitating interviews with your Personnel and others involved in the matter; and (iv) making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law, regulation, industry standards, or as otherwise required by us.

d. You shall, at your own expense, use best efforts to immediately contain, mitigate and remedy any Security Incident, reduce the risk of injury and prevent any further Security Incident or recurrence of such Security Incident, including, but not limited to taking any and all action necessary to comply with applicable privacy rights, laws, regulations, and standards. You shall reimburse us for all actual costs incurred by us in responding to and mitigating damages caused by any Security Incident, including all costs of notice and/or remediation. Further, it is expressly agreed that we may, in our sole discretion, cease Processing Personal Data or other data with you if such action may reasonably mitigate the Security Incident.

e. You must fully cooperate with us in respect of any Security Incident, including but not limited to develop and execute a response plan. You agree that we shall have the sole right to determine: (i) whether notice of the Security Incident is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies, or others as required by law or regulation, or otherwise in our discretion; and (ii) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation. Notwithstanding the foregoing, you shall at our request co-operate and shall assist us in the coordination of any notice as we may direct.

f. You must provide us with reasonable cooperation in taking measure(s) to record, report and address the Security Incident, including implementing measures to mitigate its possible adverse effects.

g. Neither you or any Authorised Sub-Processor (as defined below) may (a) delay notifying us on the basis that an investigation is incomplete or ongoing and (b) make or permit any announcement to any other third party (other than legally required by a national regulator), without our consent (which may be subject to conditions at the our sole discretion).

10 Sub-Processing

a. You shall not engage, use or permit any third party to Process JET Personal Data without our prior written authorisation(which may be withheld or subject to conditions at our discretion). Subject to this Section 10, we hereby authorise you to use the sub-processors expressly set forth in this DPA or the Agreement, solely for the processing activities and subject to any conditions described therein for such sub-processor.

b. If we have authorised the use of such third parties (known as an "Authorised Sub-Processor") for the Processing of JET Personal Data, you shall include in any contracts to be executed with any Authorised Sub-Processors who will Process Personal Data directly or indirectly on our behalf, provisions in our favour which are at least equivalent to those in this DPA and they shall be bound by the same level of obligations as you are under this DPA.

c. You shall remain fully liable and accountable to us for the performance of each Authorised Sub-Processor, as well as for any acts or omissions of each Authorised Sub-Processor in regard to its Processing of JET Personal Data.

d. You shall (a) provide us with details of any Authorised Sub-Processor upon request and (b) notify us of any proposed sub-contractor, in advance of requesting the authorisation referred to above. You shall provide copies of documentation to evidence your compliance with above upon our request.

e. If you plan to change any Authorised Sub-Processor or plan to engage with a different sub-Processor, you shall notify us in writing including all relevant details of the proposed appointment (including without limitation the name, location, and specific processing to be performed by the proposed sub-processor) without delay and in any event no less than thirty (30) days before engaging such sub-Processor to process any JET personal data. Notice shall be given by email to privacy-concerns@takeaway.com, with a copy to the primary JET business contact set forth in the Agreement in accordance with the notice provisions therein. We may object to your proposed use of any such sub-processor in writing within thirty (30) days from our receipt of such notice. In such case, (a) the parties will engage in good faith discussions to seek a mutually acceptable resolution to such objection, (b) you will not use such sub-processor to process any JET Personal Data until such mutually acceptable resolution has been agreed, and (c) if the objection is not resolved within thirty (30) days from JET's objection, JET shall be entitled to terminate the Agreement and this DPA without liability immediately upon notice to you.

11 Transfer of Data

You shall not permit any Processing of JET Personal Data outside the European Economic Area without our prior written consent unless you or an Authorised Sub-Processors is required to transfer the JET Personal Data in compliance with Data Protection Legislation and applicable laws prohibit notifying us. If JET Personal Data subject to this DPA is transferred from a country to another country which is not subjected to an adequacy decision under Data Protection Legislation, such data transfer will be governed by the terms of the applicable EU Model Clauses and/or UK International Data Transfer Agreement as agreed in Annex 2 ("Cross Border Data Transfer Mechanisms"), which are hereby incorporated by reference into this DPA. Where required under Data Protection Legislation, Parties shall collaborate to ensure the transfer documentation is duly signed.

12 Co-operation and audit

a. Upon us giving reasonable written advance notice, you shall permit us (or our representatives subject to reasonable confidentiality undertakings) without delay to conduct periodic security checks and audits of your (or an Authorised

Sub-Processor(s)) systems and processes in relation to the Processing of JET Personal Data. Such audits shall be at our expense and during normal working hours. You shall comply with all our reasonable requests or directions to verify and/or procure that you are in full compliance with your obligations under this DPA. If the audit demonstrates you have breached any obligation under the DPA, you shall immediately cure that breach and pay or reimburse JET for all reasonable costs of the audit. You hereby accept that you will implement the measures required for improvement if and any suggested in the audit report by taking into account risks associated with the Processing, the state of art and intended use of JET Personal Data.

b. Upon our written request, to confirm compliance with this DPA, as well as any applicable laws and industry standards, you shall promptly and accurately complete a written information security questionnaire provided by us, or a third party on our behalf, regarding your business practices and information technology environment in relation to all Personal Data being handled and/or services being provided by you to us pursuant to this DPA.

c. You shall cooperate and assist us with any other (a) privacy- and data protection impact assessments; (b) consultations with and/or notifications to relevant regulators; and (c) other legal or procedural requirements that we consider are relevant under Data Protection Legislation. We shall provide reasonable notice to you in advance of any of the above. In addition, at our request, you will provide all other information that is reasonably required to demonstrate compliance with the arrangements set out under this DPA. If and when needed, as the Processor you will be able to demonstrate your compliance with the requirements under this DPA by means of a valid data processing certificate; an equivalent certificate or an audit report issued by an independent expert. You shall fully cooperate with reasonable requests from us to maintain accurate records required under applicable Data Protection Legislation, such as records of processing details as well as specific privacy assessment documentation including transfer impact assessment following from applicable Data Protection Legislation in relation to Processing of Personal Data by the Processor.

13 Liability

Notwithstanding any other right or remedy which we may have, in the event of a breach of any article of this DPA (or any other contractual relationship), you agree to i) indemnify and hold us harmless (and keep us indemnified) and ii) defend us at your expense against all loss, liability, penalties, costs, claims, damages or expenses which we may incur or become liable due to any failure by you, by an Authorised Sub-Processor or your Personnel or contractors to comply with any of the obligations under this DPA, or any data breaches involving JET Personal Data caused directly or indirectly by you, your Authorised Sub-Processor, your Personnel, or contractors. Your liability arising in connection with this Clause 13 will not be subject to the limitations and exclusions of liability set out in any other contractual relationship.

14 Notices

All notices, confirmations and other statements made by the parties in connection with this DPA shall be in writing and shall be per e-mail to contracts@justeattakeaway.com and privacy-concerns@takeaway.com.

15 Governing Law and Jurisdiction

Unless as otherwise set out in the Agreement, this DPA is governed by Dutch law , and each party irrevocably submits to the non-exclusive jurisdiction of the courts of Amsterdam, the Netherlands.

16 Automated Decision Making

You shall not use Personal Data to render any decisions based exclusively on an automated processing of such information, unless explicitly requested by us or with our prior written approval .

17 Miscellaneous

a. Changes due to Data Protection Legislation: Parties may propose amendment(s) to this DPA if it reasonably considers it to be necessary to address the requirements of any applicable Data Protection Legislation or amendment thereof. If either Party gives such notice, the Parties shall promptly discuss the proposed amendment(s) and negotiate in good faith with a view to agreeing and implementing those amendments designed to address the identified requirements as soon as is reasonably practicable.

b. Your failure to comply with any of the provisions of DPA is a material breach of this Agreement. In such event, we may terminate the Agreement effective immediately upon written notice to you without further liability or obligation to you.

c. In the event of any conflict between this DPA and the Agreement, this DPA will take precedence. In the event of a conflict between this DPA and the applicable EU Model Clauses or UK International Data Transfer Agreement, the applicable EU Model Clauses or UK International Data Transfer Agreement will prevail.

Annex 1: JET'S TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF DATA

All third parties working for, together with, or on behalf of JET, that require access to JET data, information assets or facilities must comply with JET's minimum level information security measures.

The minimum level of information security measures must:

- be determined on the basis of envisaged risks for individual data subjects ('risk-based approach');
- take into account the state of the art of data processing technologies, security threats and vulnerabilities;
- be evaluated periodically, and updated when required by changes in the state of the art ('dynamic approach').

GENERALLY ACCEPTED SECURITY STANDARDS

Third parties are expected to comply with relevant generally accepted security standards such as

- technology-neutral standards such as ISO/IEC 27001:2013, ISO/IEC 27002:2022, ISO/IEC 27017:2015 (cloud services), SOC-2.
- organisational level technical controls frameworks such as CIS critical controls V8, NIST CSF.
- standards which describe the technical measures in detail e.g. the PCI Security Standards for the handling of credit cards, NIST's standards for cloud computing, the OWASP Foundation's web application (Secure Coding Practices) and mobile application (MASVS) guidelines.

Upon the JET's written request, the third party shall provide within a reasonable time, a copy of the most recently completed certification and/or attestation reports of the technical and organisational security measures implemented.

INFORMATION SECURITY POLICIES AND MEASURES

Third parties are expected to enforce a risk based approach towards information security, meaning the level of protection provided is in line with risks identified and have implemented and maintain a complete set of Information Security policies and corresponding procedures, which have been approved by its management and disclosed to all its employees and relevant third parties (sub-service providers) that include, but is not limited to:

- Measures for **user identification** and **access management** including authentication to only grant authorised users access to IT assets based on role based access control, change or revoke access rights in a timely manner when no longer required and management of privilege access rights.
- Measures for ensuring ongoing **confidentiality, integrity, availability** and **resilience** of systems and services processing (personal) data such as:
    - password, key, certificates, or other authentication secrets management.
    - regular software updates including but not limited to web browsers, virus scanners and operating systems.
    - IT asset management including the measures for the protection of end user devices and the secure disposal of IT assets that are no longer in use.
    - ensuring system configuration, including default configuration.
    - ensuring reliable network access infrastructure to maintain business resilience and support uninterrupted productivity.
    - regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing.
- Measures for the protection and and **non-disclosure** of (personal) data during transmission and storage, including
    - the implementation of a data classification management framework based on the sensitivity, value and criticality of data.
    - a non-disclosure policy implemented and communicated to employees involved in the processing of (persona) data.
    - the pseudonymisation, encryption or hashing of (personal) data. These measures include proper key management and up to date (disk & file) encryption technologies.
- Measures for ensuring the ability to **restore** the availability and access to (personal) data in a timely manner in the event of a physical or technical incident. This includes adequate **business continuity management** that is periodically tested.
- Measures for ensuring **physical security** against access by unauthorised people, damages or disturbances of facility locations and IT assets at which (personal) data are processed. The provided level of protection is in line with risks involved.
- Measures for ensuring **events logging** regarding (personal) data including attempts to acquire unauthorised access to (personal) data and any disturbances which could lead to changes in or loss of (personal) data. Log files are periodically checked for any indications of unauthorised access or use and adequate action is taken when necessary.
- Measures to properly address **vulnerabilities** in a timely and adequate manner.

- Measures to timely and adequately address **information security incidents**. Covering incident response, internal escalation and decision-making. The incident management process includes the event of a data breach and takes into account the necessity to perform an assessment to understand if notification to relevant stakeholders including authorities and data subjects is required.
- A **security awareness program** to properly train all its employees working for or on behalf of the third-party organisation. Employees regularly receive training to understand the security policy and security procedures of the third-party organisation. They are aware that they are responsible for promoting a security-savvy culture and for maintaining the confidentiality, integrity and availability of information (assets) with which they work.
- Measures around **secure software development** including privacy by design principles.
    - Measures to ensure **lawfulness** to make sure that the whole processing lifecycle is in line with the relevant legal grounds of processing.
    - Measures to ensure **data minimisation**: to only process (personal) data if the purpose of the processing could not reasonably be fulfilled by other means. The processing is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
    - Measures to ensure **purpose limitation** and only collect data for specified, explicit, and legitimate purposes, and not further process the data in a manner that is incompatible with the purposes for which they were collected.
    - Measures to ensure **fairness** to prevent the processing of personal data that is is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading.
    - Measures to ensure **transparency** about how personal data is collected, used and shared.
    - Measures to ensure the **accuracy** of personal data to safeguard the quality of personal data and make sure that it is kept up to date, and every reasonable step is taken to ensure that personal data that is inaccurate (considering the purposes for which they are processed) are erased or rectified without delay.
    - Measures for **storage limitation** to ensure that personal data is kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data is processed. This includes a data retention policy.
    - Measures for ensuring **accountability** to demonstrate compliance with all of the above mentioned measures.
- Measures for allowing data **portability** to allow individuals to obtain and reuse their personal data for their own purposes across different services.
- Measures for **certification/assurance** of processes and products.

ROLES AND RESPONSIBILITIES

Third parties working for, together with, or on behalf of JET are expected to collaborate with JET to define clear roles and responsibilities around the control implementation required to mitigate the identified risks.

Annex 2: Cross Border Data Transfer Mechanisms

1. **Order of Precedence**. In the event the Services are covered by more than one Transfer Mechanism, the transfer of Personal Data will be subject to a single Transfer Mechanism in accordance with the following order of precedence: (a) the EU Model Clauses as set forth in Section 3 of Annex 2 (EU Standard Contractual Clauses); (b) the UK International Data Transfer Agreement as set forth in Section 4 of Annex 2 (UK International Data Transfer Agreement) and, if neither (a) nor (b) is applicable, then (c) other applicable data Transfer Mechanisms permitted under applicable Data Protection Legislation.

2. **EU Model Clauses.** The parties agree that the EU Standard Contractual Clauses will apply to Personal Data that is transferred via the Services from the EEA or Switzerland, either directly or via onward transfer, to any country or recipient outside the EEA or Switzerland that is: (a) not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for personal data. For data transfers from the EEA that are subject to the EU Standard Contractual Clauses, the Module 2 (Controller to Processor) of the EU Standard Contractual Clauses will be deemed entered into (and incorporated into this Addendum by this reference) and completed, where applicable:
(i) Clause 7 of the EU Standard Contractual Clauses, the optional docking clause will not apply;
(ii) Clause 9 of the EU Standard Contractual Clauses, Option 2 will apply and the time period for prior written notice of sub-processor changes will be as set forth in Section 7.2 (Current Sub-processors and Notification of Sub-processor Changes) of this Addendum;
(iii) Clause 11 of the EU Standard Contractual Clauses, the optional language will not apply;
(iv) Clause 14 of the EU Standard Contractual Clauses, Parties have agreed to document a transfer impact assessment. Data Importer will provide the relevant information needed to complete such transfer impact assessment by providing the information:
   (1) Where will the data be processed?
   (2) Which transfer tool will be relied on?
   No additional information will be needed if data exporter and data importer will rely on the EU Model Clauses and/or the UK International Data Transfer Agreement for any restricted transfers under applicable Data Protection Legislation.
   (3) Is the transfer tool relied upon effective in the circumstances?
   (4) Which supplementary measures, in view of above, will be implemented to comply with its commitments under applicable Data Protection Legislation with regard to any restricted transfers?
   (5) What are the re-evaluation intervals?
(v) in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by the law as agreed upon in the DPA;
(vi) in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved as agreed upon in the DPA;
(vii) in Annex I, Part A of the EU Standard Contractual Clauses:

Data Exporter: we

- Contact details: The email address(es) as set out in Clause 9 (Notification of incidents) of the DPA.
- Data Exporter Role: The Data Exporter's role is set forth in Clause 1 (Relationship of the Parties) of the DPA.
- Signature and Date: By entering into the Agreement, Data Exporter is deemed to have signed these EU Standard Contractual Clauses incorporated herein, including their Annexes, as of the effective date of the Agreement.

Data Importer: you

- Contact details: The email address(es) as set out in the Agreement for your Data Protection Officer or other contact capable of handling data protection inquiries.
- Data Importer Role: The Data Importer's role is set forth in Clause 1 (Relationship of the Parties) of the DPA.
- Signature and Date: By entering into the Agreement, Data Importer is deemed to have signed these EU Standard Contractual Clauses, incorporated herein, including their Annexes, as of the effective date of the Agreement;

(viii) in Annex I, Part B of the EU Standard Contractual Clauses:

- The categories of data subjects are set forth in the Data Processing Particulars.
- The Sensitive Data transferred is set forth in the Data Processing Particulars.
- The frequency of the transfer is a continuous basis for the duration of the Agreement.

- The nature of the processing is set forth in the Data Processing Particulars..
- The purpose of the processing is set forth in the Data Processing Particulars..
- The period for which the personal data will be retained is set forth in the Data Processing Particulars..
- For transfers to sub-processors, the subject matter, nature, and duration of the processing is set forth in the DPA;

(ix) in Annex I, Part C of the EU Standard Contractual Clauses: Dutch Data Protection Authority will be the competent supervisory authority; and

(x) Annex 1 (Description of Security Measures) of the DPA serves as Annex II of the EU Standard Contractual Clauses.

3. **UK International Data Transfer.** The parties agree that the UK International Data Transfer Agreement Addendum will apply to personal data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is: (a) not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for personal data. For data transfers from the United Kingdom that are subject to the UK International Data Transfer Agreement, the UK International Data Transfer Agreement will be deemed entered into (and incorporated into this Annex 2 by this reference) and completed as follows:

   (a) In Table 1 of the UK International Data Transfer Agreement, the parties' details and key contact information is located in Section 2 of this Annex 2.

   (b) In Table 2 of the UK International Data Transfer Agreement, information about the version of the Approved EU SCCs, modules and selected clauses which this UK International Data Transfer Agreement is appended to is located in Section 2 (EU Standard Contractual Clauses) of this Annex 2.

   (c) In Table 3 of the UK International Data Transfer Agreement:

   - The list of Parties is located in Section 2 of this Annex 2.
   - The description of the transfer is set forth in the Data Processing Particulars.
   - Annex III is located in Annex 1 ((Description of Security Measures) of the DPA
   - The approved sub-processors are governed as set forth in Clause 11 of the DPA

   (d) In Table 4 of the UK International Data Transfer Agreement, both the Importer and the exporter may end the UK International Data Transfer Agreement in accordance with the terms of the UK International Data Transfer Agreement.

4. **Switzerland.** The parties agree to apply the formal recognition of the EU Model Clauses by the Swiss Federal Data Protection and Information Commissioner (FDPIC), including its adopted amendments:

   (a) the FDPIC is the exclusive supervisory authority in accordance with Clause 13 and Annex I.C of the EU SCCs;

   (b) the governing law in accordance with Clause 17 of the EU SCCs shall be Swiss law in case the data transfer is exclusively subject to the Swiss Federal Act on Data Protection, as amended or replaced (FADP);

   (c) the term "member state" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 of the EU SCCs; and

   (d) references to the GDPR in the EU SCCs shall also include the reference to the equivalent provisions of the FADP.

5. Conflict. To the extent there is any conflict or inconsistency between the EU Standard Contractual Clauses or UK International Data Transfer Agreement and any other terms in this Addendum, the Agreement, the provisions of the EU Standard Contractual Clauses or UK International Data Transfer Agreement, as applicable, will prevail.