

## LEASECRUNCH STANDARD CONTRACTUAL CLAUSES

These LeaseCrunch Standard Contractual Clauses by and between the customer identified on the applicable Order Form (“**Customer**”), and LeaseCrunch LLC. (“**LeaseCrunch**”) are incorporated into, and form part of, the Data Processing Agreement available at <https://leasecrunch.com/legal/dpa>

Controller to Processor

### SECTION I

#### *Clause 1*

##### **Purpose and scope**

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of data to a third country.
- (b) The Parties:
  - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter ‘entity/ies’) transferring the personal data, as listed in Annex I.A (hereinafter each ‘data exporter’), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each ‘data importer’) have agreed to these standard contractual clauses (hereinafter: ‘Clauses’).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

#### *Clause 2*

##### **Effect and invariability of the Clauses**

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

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

### ***Clause 3***

#### **Third-party beneficiaries**

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
- (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
  - (iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
  - (iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
  - (v) Clause 13;
  - (vi) Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

### ***Clause 4***

#### **Interpretation**

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

### ***Clause 5***

#### **Hierarchy**

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

### ***Clause 6***

#### **Description of the transfer(s)**

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

### ***Clause 7 – Optional***

### **Docking clause**

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## **SECTION II – OBLIGATIONS OF THE PARTIES**

### ***Clause 8***

#### **Data protection safeguards**

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

#### **8.1 Instructions**

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

#### **8.2 Purpose limitation**

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

#### **8.3 Transparency**

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

## **8.4 Accuracy**

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

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

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

## **8.6 Security of processing**

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have

committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

## **8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offenses (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:

- (i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

- (iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

## **8.9 Documentation and compliance**

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter must choose 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.

## ***Clause 9***

### **Use of sub-processors**

- (a) The data importer has the data exporter's general authorization for the engagement of subprocessor(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 giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that

provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfills its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

- (c) The data importer shall provide, at the data exporter's request, a copy of such a subprocessor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfill its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the subprocessor contract and to instruct the sub-processor to erase or return the personal data.

### ***Clause 10***

#### **Data subject rights**

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

### ***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 authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

## ***Clause 12***

### **Liability**

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



- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### ***Clause 13***

#### **Supervision**

- (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 behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including

remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

#### ***Clause 14***

##### **Local laws and practices affecting compliance with the Clauses**

- (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 authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - (iii) any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

- (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 fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the 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**

**15.1 Notification**

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
- (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

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

## **15.2 Review of legality and data minimisation**

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

## **SECTION IV – FINAL PROVISIONS**

### ***Clause 16***

#### **Non-compliance with the Clauses and termination**

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses. In these cases, it shall inform the competent supervisory authority of such noncompliance. Where

the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

#### ***Clause 17***

##### **Governing law**

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 Ireland.

#### ***Clause 18***

##### **Choice of forum and jurisdiction**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Ireland.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

## ANNEX I

### A. LIST OF PARTIES

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

Address: Customer's address identified in the applicable Order Form

Contact person's name, position and contact details: Customer's contact identified in the applicable Order Form

Activities relevant to the data transferred under these Clauses: Customer shall provide LeaseCrunch with access to Customer's IT environment to allow LeaseCrunch to provide the applicable Services.

Signature and date: See Order Form

Role (controller/processor): Controller

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

Name: LeaseCrunch LLC.

Address: 790 N Milwaukee Street Suite 302, Suite 302, Milwaukee, WI 53202

Contact person's name, position and contact details: [privacy@leasecrunch.com](mailto:privacy@leasecrunch.com), LeaseCrunch Privacy Team

Activities relevant to the data transferred under these Clauses: LeaseCrunch shall process Customer's Personal Data to provide the Services, which may include (depending on the particular Service) hosting Customer's Personal Data, using software agents within Customer's IT environment, or scanning Customer's IT environment. Signature and date: See Order Form

Role (controller/processor): Processor

### B. DESCRIPTION OF TRANSFER

*Categories of data subjects whose personal data is transferred*

Any data subjects whose Personal Data is contained in Data Exporter's data being used in the LeaseCrunch Solutions, as set out in the Agreement which describes the provision of LeaseCrunch services to Customer, including Customer's account administrator, users, and representatives, including, without limitation, Customer's employees, contractors, partners, suppliers, customers, and clients.

### *Categories of personal data transferred*

Any Personal Data that is provided by Data Exporter to Data Importer in connection with the Agreement and the DPA, including, without limitation, contact information such as name, address, telephone or mobile number, email address, and passwords.

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

N/A

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

Continuous as needed to provide the Services.

### *Nature of the processing*

LeaseCrunch shall process Customer's Personal Data to provide the Services, which may include (depending on the particular Service) hosting Customer's Personal Data, using software agents within Customer's IT environment, or scanning Customer's IT environment.

### *Purpose(s) of the data transfer and further processing*

To provide the Services to Customer pursuant to the Services Agreement.

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

The data will be retained for the time period needed to accomplish the purposes of Processing, unless otherwise required by applicable law.

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

All transfers will last for the duration of the Agreement between the parties.

## **C. COMPETENT SUPERVISORY AUTHORITY**

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

The data exporter's competent supervisory authority will be determined in accordance with Data Privacy Law and, where possible, will be the Irish Data Protection Commissioner.

---

**ANNEX II**  
**TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

1. **DEFINITIONS.** Capitalized terms used herein shall have the meanings ascribed to them in the main body of the Services Agreement and Data Processing Agreement to which this Annex II is attached to, this Annex II, or as otherwise defined below.

“**Authorized Representatives**” means LeaseCrunch’s Representatives who have a need to know or otherwise access data exporter’s Personal Data to enable LeaseCrunch to perform its obligations under the Services Agreement and this Annex II, and who are bound in writing by confidentiality and other obligations sufficient to protect Data exporter’s Personal Data in accordance with the terms and conditions of the Services Agreement and this Annex II.

2. **STANDARD OF CARE.** LeaseCrunch will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as described herein applicable to the specific Services purchased by data exporter or otherwise made reasonably available by LeaseCrunch. LeaseCrunch will not materially decrease the overall security of the Services during the term.

3. **INFORMATION SECURITY.**

- 3.1. **Compliance with Laws and Regulations.** LeaseCrunch’s creation, collection, receipt, access, use, storage, disposal, and disclosure of Data exporter’s Personal Data does and will comply in all material respects with Applicable Laws.

- 3.2. **Written Information Security Policy.** LeaseCrunch shall implement and maintain a written information security program including appropriate policies, procedures, and risk assessments that are reviewed at least annually.

- 3.3. **Safeguards.** LeaseCrunch shall implement commercially reasonable administrative, physical, and technical safeguards designed to protect Data exporter’s Personal Data from unauthorized access, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage that are no less rigorous than generally accepted industry practices and shall otherwise ensure that all such safeguards, including the manner in which Data exporter’s Personal Data is created, collected, accessed, received, used, stored, processed, disposed of, and disclosed, comply in all material respects with applicable data protection and privacy laws, as well as the terms and conditions of the Services Agreement and this Annex.

- 3.4. **Minimum Safeguards.** At a minimum, LeaseCrunch’s safeguards for the protection of Data exporter’s Personal Data shall include: (a) limiting access of Data exporter’s Personal Data to Authorized Representatives; (b) securing business facilities, data centers, paper files, servers, backup systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (c) implementing network, application, database, and platform security; (d) securing information transmission, storage, and disposal; (e) implementing authentication and access



controls within media, applications, operating systems, and equipment; (f) encrypting Data exporter's Personal Data stored on any mobile media; (g) encrypting Data exporter's Personal Data transmitted over public or wireless networks; (h) conducting risk assessments, penetration testing, and vulnerability scans and implementing a corrective action plan to designed to correct any issues, as appropriate, that are reported as a result of the testing; (i) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks for its employees consistent with applicable law; and (j) providing appropriate privacy and information security training to LeaseCrunch's employees.

#### 4. **SECURITY INCIDENT PROCEDURES.**

- 4.1. **Incident Response Plan.** LeaseCrunch maintains a cyber incident breach response plan in accordance with generally accepted industry standards and will implement the procedures required under such plan on the occurrence of a Security Incident.
- 4.2. **Security Contacts.** LeaseCrunch shall: (a) provide Customer with the name and contact information of LeaseCrunch which shall serve as Customer's primary security contact and shall be available to assist Customer via telephone on Business Days during the hours of 8:00 AM and 5:00 PM Central Time and all other times via email as a contact in resolving obligations associated with a Security Incident; and (b) notify Customer via telephone or email of a Security Incident impacting Customer's Personal Data without undue delay.
- 4.3. **Notification of Security Incidents.** Following LeaseCrunch's notification to Customer of a Security Incident, the Parties shall coordinate with each other to investigate the Security Incident. LeaseCrunch agrees to reasonably cooperate with Customer, at Customer's expense, in Customer's handling of the matter, including, without limitation: (a) assisting with any investigation; and (b) making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law, regulation, industry standards, or as otherwise reasonably required by Customer.
- 4.4. **Security Incident Containment.** LeaseCrunch shall take reasonable steps to immediately contain and remedy any Security Incident and prevent any further Security Incident, including, but not limited to taking any and all action necessary to comply with applicable privacy rights, laws, regulations, and standards.
- 4.5. **Notice to Affected Individuals.** Unless required by Applicable Law, LeaseCrunch agrees that it shall not inform any third-party of any Security Incident involving Customer's Personal Data without first obtaining Customer's prior written consent, other than to inform a complainant that the matter has been forwarded to Customer's legal counsel. Further, LeaseCrunch agrees that Customer shall have the sole right to determine: (a) 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 Customer's discretion; and (b) 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, nothing in this Section 4.5 shall prohibit LeaseCrunch from making a general statement, or a statement related to any other customer of LeaseCrunch's data, to any individuals, regulators, law enforcement agencies, consumer reporting agencies, or others.

- 4.6. **Record Maintenance.** LeaseCrunch agrees to maintain and preserve all documents and records related to a Security Incident, in accordance with to LeaseCrunch's document retention policy.
- 4.7. **Cooperation.** LeaseCrunch agrees to reasonably cooperate with Customer in any litigation, investigation, or other action deemed reasonably necessary by Customer to protect its rights relating to the use, disclosure, protection, and maintenance of Data exporter's Personal Data.
- 4.8. **Prevention.** In the event of any Security Incident, LeaseCrunch shall promptly use its reasonable efforts to prevent a recurrence of any such Security Incident.

### ANNEX III

**LIST OF SUB-PROCESSORS:** A list of sub-processors is available at <https://leasecrunch.com/legal/dpa>

## **UK INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU STANDARD CONTRACTUAL CLAUSES**

This **Addendum** is made part of the **Standard Contractual Clauses (SCCs)** agreed between:

**Data Exporter (UK): Customer** incorporated in the UK, (the "**UK Data Exporter**");

**Data Importer:** LeaseCrunch LLC, a company incorporated in the United States, with its registered office at 790 N Milwaukee Street Suite 302, Suite 302, Milwaukee, WI 53202 (the "**Data Importer**").

### **1. Introduction and Purpose**

This Addendum modifies the Standard Contractual Clauses (SCCs) entered into between the UK Data Exporter and the Data Importer to reflect the requirements of the **UK GDPR** and the UK Data Protection Act 2018. It ensures that the transfer of personal data from the **United Kingdom (UK)** to a third country is conducted in compliance with UK data protection laws.

### **2. Incorporation of the Standard Contractual Clauses**

The SCCs, as approved by the European Commission on [insert relevant date of SCCs], are hereby incorporated by reference into this Addendum, subject to the following modifications and amendments to reflect UK data protection law.

### **3. Modifications to the SCCs**

The SCCs shall be interpreted in accordance with UK GDPR as follows:

1. **References to the "GDPR":** All references to "Regulation (EU) 2016/679 (General Data Protection Regulation)" or "GDPR" shall be interpreted as references to the **UK GDPR** as defined in Section 3 of the UK Data Protection Act 2018.
2. **References to the "EU" or "Member State":** All references to the "European Union" or "EU Member State" shall be replaced with "United Kingdom" where relevant to the transfer of personal data from the UK.
3. **Supervisory Authority:** References to the "supervisory authority" or "competent supervisory authority" shall be construed as references to the **UK Information Commissioner's Office (ICO)**.
4. **Governing Law:** Clause 9 of the SCCs (Governing Law) shall be interpreted such that the governing law for this Addendum and the SCCs (as applied to UK data transfers) shall be the **laws of England and Wales**.
5. **Jurisdiction:** References to "courts of an EU Member State" shall be replaced with the "courts of England and Wales" for disputes arising under UK data protection law.

### **4. Transfer Impact Assessment (TIA)**

Both the UK Data Exporter and the Data Importer confirm that they have conducted a Transfer Impact Assessment (TIA) for the transfer of personal data from the UK to the third country and

have identified appropriate supplementary measures, if necessary, to ensure compliance with the UK GDPR.

## **5. Data Subject Rights**

The Data Importer agrees to assist the UK Data Exporter in fulfilling any requests received from UK data subjects under the UK GDPR, including:

- Right of access to personal data;
- Right to rectification or erasure of personal data;
- Right to object to or restrict the processing of personal data;
- Right to data portability, where applicable.

## **6. Termination**

If the SCCs or this Addendum are found to be invalid or unenforceable under UK law, the UK Data Exporter may terminate the data transfer agreement upon written notice, and the Data Importer agrees to either return or securely delete the transferred personal data, unless otherwise required by law.

## **7. Liability**

The parties agree that the liability provisions of the SCCs shall apply to this Addendum, with references to "Member State" interpreted as the "United Kingdom" and "supervisory authority" interpreted as the **UK ICO**.

## **8. Miscellaneous**

Any terms not specifically modified by this Addendum shall remain as stated in the SCCs. This Addendum shall take precedence over the SCCs in the event of any conflict between the terms, to the extent necessary to comply with UK data protection laws.