DATA PRIVACY ADDENDUM

This Data Privacy Addendum ("**Addendum"**) is incorporated into and amends the Agreement (as defined below). < Client> ("Client") and JLL (including any member(s) of the Jones Lang LaSalle corporate group that is or are party to the Agreement) agree as follows:

1. DEFINITIONS

"**Authorized Sub-processors**" means entities JLL engages to provide services for Client that Client has approved to perform the services.

"**Client**" means Company.

"Controller" means the party that determines the purpose and means of processing personal information.

"**Data Privacy Laws**" means any laws, regulations, and secondary legislation, and orders and industry standards implementing or supplementing such provisions, concerning privacy or data protection, including but not limited to the General Data Protection Regulation (GDPR) and the California Consumer Protection Act (CCPA).

2. USE OF PERSONAL INFORMATION AND HANDLING RESTRICTIONS

Where required by applicable Data Privacy Laws, JLL will be data processor and Client will be the data Controller for all Personal Information. Client will ensure that all privacy notices required to enable JLL and any Authorized Sub-processors to carry out their obligations in relation to the Personal Information are provided to the relevant data subjects. Client will ensure that any Personal Information transferred to JLL can be lawfully Processed by JLL or any authorized sub-processors. JLL acknowledges that it provides services as specified in, or otherwise performed pursuant to the Agreement. JLL will only Process Personal Information on Client's instructions and solely as necessary for JLL to perform the Services and its obligations under this Addendum, as described in the Agreement, or to perform another business purpose as permitted under applicable Data Privacy Laws. JLL will not Process Personal Information for any other purpose. For the avoidance of doubt, JLL must keep confidential all Personal Information and must not sell, resell, lease, assign, rent, sublicense, distribute, transfer, disclose, time-share, or otherwise exchange Personal Information (or any portion thereof) for any reasons (whether or not for monetary or other consideration), except to the extent that a disclosure or transfer is required by law or is reasonably required by JLL to facilitate its business or maintain its infrastructure. The acts or omissions of JLL's affiliates (including its employees, agents, representatives, contractors, and subcontractors) regarding Personal Information are deemed the acts or omissions of JLL. The Parties agree that any transfer or disclosure of Personal Information between Client and JLL under the Agreement is not for monetary or other valuable consideration and therefore does not constitute a sale of Personal Information. To the extent the Services involve cross-border transfers of Personal Information by JLL, JLL will comply with applicable Data Privacy Laws. JLL will maintain records and information that demonstrate its compliance with all applicable Data Privacy Laws and the requirements of this Addendum and will make all such records and information available to Client or an auditor Client selects for the purpose of auditing JLL's compliance. Such audits are limited to one per 12-month period.

3. DETAILS OF PROCESSING

The **subject matter and duration** of Processing are set out in the Agreement, including this Addendum. Processing ceases upon termination or expiration of the Agreement and any retention periods required under local law.

The **purpose** of Processing is to perform the Services and the **nature** of Processing will consist of using, recording, editing, storing, and accessing Personal Information, for the purpose of performing Services under the Agreement.

Categories of individuals whose Personal Information may be Processed, unless otherwise defined elsewhere in the Agreement, may include the following in respect of Client: employees, contractors, vendors, building occupants / tenants / landlords / visitors, and others, and the representatives of each.

The **obligations and rights** of JLL are set out in the Agreement, including this Addendum.
If Art. 28(3) GDPR or other Data Privacy Law obliges the Parties to agree on certain details of Processing, then:
(a) Appendix 1 must be completed and attached; and
(b) The parties agree to the details of Processing as set out in that Appendix.

4. ACCESS LIMITATIONS

JLL will endeavor to provide access to Personal Information to those personnel who have a need to know to enable JLL to perform its obligations under the Agreement, and who have agreed in writing to comply with the requirements of this Addendum as if they were JLL. JLL will obtain Client's prior written authorization before appointing any third party to Process Personal Information, except for third parties necessary to facilitate JLL's business operations or infrastructure support, and will ensure that arrangements with any such third party are governed by a written contract including terms that offer at least the same level of protection for Personal Information as those set out in this Addendum, and which meet the requirements of applicable Data Privacy Laws.
JLL will, in accordance with any written request from Client, delete or return Personal Information (and ensure that any third parties it engages do the same) at the end of the provision of the Services for which the Personal Information was Processed.

JLL may retain copies of Personal Information in accordance with any legal or regulatory requirements or any guidance issued by a supervisory authority relating to deletion or retention.

5. COMPLIANCE WITH DATA PRIVACY LAWS

JLL will provide Client with all reasonably requested assistance and cooperation to enable Client to comply with its obligations under the Data Privacy Laws arising under the Agreement, including cooperating with Client to respond to any individuals' requests, inquiries, or assertion of rights under the Data Privacy Laws with respect to Personal Information. JLL must provide its assistance within any reasonable timeframe specified by Client. If JLL receives a request directly from an individual or legal / regulatory authority concerning Personal Information, JLL must, to the extent not prohibited by applicable law or any regulatory authority, promptly forward the request to Client for handling, direct the individual to submit the request as indicated in Client's privacy statement, and cooperate with any Client instructions regarding the request.

6. PRIVACY PROTECTION

Without in any way limiting any requirements or provisions of the Agreement or this Addendum, JLL warrants that it has adopted and implemented, and will maintain for as long as this Addendum is in effect or as long as JLL Processes Personal Information (whichever is later), technical and organizational measures designed to protect all Personal Information against accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure, and access, and against all other unlawful activities. JLL will promptly provide to Client upon written request a written description of the technical and organizational security measures JLL has implemented to comply with this section. JLL will encrypt Personal Information during transmission using industry standard protocols and also encrypt at rest any high risk (sensitive) Personal Information (as defined by applicable Data Privacy Laws). JLL will implement and maintain security measures, procedures, and practices appropriate to the nature of Personal Information and adequate under the Data Privacy Laws designed to protect Personal Information from unauthorized access, destruction, use, modification, or disclosure ("**Privacy / Security Incident**"). JLL will inform Client without undue delay when it becomes aware of any Privacy / Security Incident unless the incident is unlikely to result in a risk to the rights and freedoms of the individuals concerned and will timely provide all information and cooperation reasonably requested by Client. JLL will promptly take reasonable measures and actions necessary to remedy or mitigate the effects of the Privacy / Security Incident and will keep Client informed of all material developments in relation to it. Unless applicable law requires, JLL will not notify any third party other than JLL's insurers or professional advisers or regulatory authority of a Privacy / Security Incident without Client's prior written authorization.

7. COMPLIANCE

JLL will comply with all Data Privacy Laws in the fulfilment of its obligations and otherwise in its rendering of Services to Client. JLL represents and warrants that it has implemented written guidelines to ensure its compliance with its obligations under this Addendum and will provide those written guidelines to Client on request.

8. GENERAL

Except as expressly set forth in this Addendum, the terms of the Agreement shall remain unmodified and in full force and effect. If there is a conflict between the terms of the Agreement and the terms of this Addendum, the terms of this Addendum shall prevail. If applicable law requires survival of any terms of this Addendum, such terms will survive after expiration or termination of the Processing. This Addendum is part of and governed by the terms and conditions of the Agreement.

APPENDIX I

EUROPEAN TRANSFER MECHANISMS

Applicable Standard Contractual Clauses Incorporated by Reference

Where Controller transfers (directly or via onward transfer) Personal Data that originated from Europe or the UK (as applicable) to Processor located in a country that does not provide an adequate level of protection for Personal Data (as described in European Data Protection Law), the parties agree the following:

EU Standard Contractual Clauses

A. In relation to Personal Data that is protected by the EU GDPR, the New EU SCCs **MODULE 2 Controller to Processor** shall apply, are incorporated by reference https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en, and are completed as follows:

1) Module Two will apply;

2) in Clause 7, the optional docking clause does not apply;

3) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be ten (10) days;

4) in Clause 11, the optional language will not apply;

5) in Clause 17, Option 1 will apply, and the New EU SCCs will be governed by the Member State where the Data Exporter is established except for those countries without 3rd party beneficiary rights, the Parties agree that this shall be the law of Germany;

6) in Clause 18(b), disputes shall be resolved before the courts of the Member State in which the Data Exporter is established; and

7) Appendix I including, Annexes I, II and III of the New EU SCCs are attached below.

UK Standard Contractual Clauses as applicable

B. Subject to paragraph (C), below, in relation to Protected Data or Personal Data (as applicable) that is protected by the UK GDPR, the EU SCCs will apply in accordance with paragraphs (i), (ii), (iii), and (iv) above, is incorporated herein https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en, and shall be completed as follows:

1) Any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the UK GDPR, references to "EU", "Union" and "Member State law" shall be interpreted as references to English law, and references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the relevant data protection authority and courts in England;

2) Appendix 1 of the EU SCCs shall be deemed completed with the information set out in Annexes I, II and III below (as applicable);

C. To the extent that and for so long as the EU SCCs as implemented in accordance with paragraphs (A) - (B) above cannot be used to lawfully transfer Protected Data or Personal Data (as applicable) in compliance with the UK GDPR, the UK SCCs shall be incorporated by reference https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/sccs-after-transition-period/, and form an integral part of this DPA and shall apply to transfers governed by the UK GDPR. For the purposes of the UK SCCs, the relevant Annexes of the UK SCCs shall be populated using the information contained in Annexes I, II and III (as applicable); and

D. It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict.

E. Alternative transfer arrangements. To the extent Controller adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses adopted pursuant to applicable European Data Protection Law) for the transfer of Personal Data not described in this DPA ("Alternative Transfer Mechanism"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with European Data Protection Law and extends to the territories to which Personal Data is transferred) and Processor agrees to execute such other and further documents and take such other and further actions as may be reasonably necessary to give legal effect such Alternative Transfer Mechanism. In addition, if and to the extent that a court of competent jurisdiction or a supervisory authority with binding authority orders or determines (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer such Personal Data, Processor

acknowledges and agrees that Controller may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of such Personal Data.

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: The entity identified as "Company".

Address: The address of Company or as otherwise agreeed between JLL and Company.

Contact person's name, position and contact details: The person that executed this Agreement on behalf of Company.

Activities relevant to the data transferred under these Clauses:

Personal data will be transferred for the purposes of providing the agreed Services as detailed in part B.

Signature and date: By using the Services to transfer data to Third Countries, Company will be deemed to have signed this Annex.

Role (controller/processor): Controller

Data importer(s):

Name: Jones Lang LaSalle Americas, Inc. and its affiliates

Address: 200 East Randolph Street, Suite 4400 Chicago, Illinois USA

Contact person's name, position and contact details: The person that executed the Agreement on behalf of JLL.

Privacy Contact: PrivacyGlobal@jll.com

Activities relevant to the data transferred under these Clauses:

Personal data will be transferred for the purposes of providing the agreed Services as detailed in part B.

Signature and date: By transferring Customer Data to Third Countries on Customer's instructions, JLL will be deemed to have signed this Annex I.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Commercial Information, e.g., records of personal property, products or services purchased, obtained, or considered

Business Contact details (Commercial/Client/Tenant)

Financial Information, e.g. Commercial/Client/Tenant)

Network Activity Data: used to provide analytics for example

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

- Continuous

Nature of the processing

- The provision of services to JLL in accordance with the Agreement.

Purpose(s) of the data transfer and further processing

- To provide services to JLL as described in the 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 personal data is to be retained until the termination of the Agreement unless otherwise agreed by the parties or required by applicable law.

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

- The subject matter, nature and duration of the processing are described in the Agreement.

C. Competent supervisory authority

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

1) The EU Member State in which the data exporter is established.

Annex II

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

EXPLANATORY NOTE:

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

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

Organisational Measures (apply to all the data categories above**)**	Acceptable Use Policies	Access Reviews	Security Awareness & Training	Background Checks of staff	Business Continuity Plans	Change Management
	Data Processing Agreements	Disaster Recovery Plans (IT recovery)	Incident Response Plans	Internal audits	Data disclosed on Need-To-Know	Non-Disclosure Agreements
	Password Policies	Penetration Tests	Phishing tests/ teachable moments	Regular Test Plan	Secure Development Program	Secure Disposal
	Secure Premises	Segmented Access Control	Supervision	Surveillance	Table-Top Exercises	Third-party audits
	Vendor Assessments					

Technical Measures (apply to all data categories above)	Access Control Lists	Anti-Malware at all our user devices and servers	Automated Anti-Virus Updates	Biometric Access Control (datacentres)	Breach Detection Tools	Data Backup
	DLP (Data Loss Prevention)	Encrypted at Rest	Encrypted in Transit	Firewalls	Inactivity timeout within JLL device / application	Intrusion Detection Tools
	Intrusion Prevention Tools	Security Event Logging	Logical Access Control	Mobile Device Management (MDM) Tools	Multi-Factor Authentication	Network Authentication
	Security Cameras (offices/data centres)	Single Sign On	Static and/or Dynamic Code Testing	Connect to service / data via VPN	Vulnerability Detection Tools	Web Application Firewall

ANNEX III

LIST OF SUB-PROCESSORS

JLL may use all or some of the following sub-processors in the management of our services to you. For any questions about our use of sub-processors, please contact your client account manager.

Controller authorises the use of these sub-processors https://www.us.jll.com/en/sub-processors.