DPA SCHEDULE 1

STANDARD CONTRACTUAL CLAUSES (SCCs)

1. **Incorporation of Standard Contractual Clauses.**

The Parties agree that the applicable Standard Contractual Clauses ("SCC") are hereby entered into and form part of the Parties' DPA:

1.1 Where CoStar processes Personal Data as a Controller pursuant to the terms of the Agreement, CoStar and its relevant Affiliates are located in countries that are not subject to an adequacy decision by the European Commission, and Customer and its relevant Affiliates are established in the EEA, Module One (transfer controller to controller), Clauses 1 to 6, 8 and 10 to 18 apply.

1.2 Where CoStar Processes Personal Data as a Processor pursuant to the terms of the Agreement, CoStar and its relevant Subprocessor Affiliates are located in countries that are not subject to an adequacy decision by the European Commission, and Customer and its relevant Affiliates are established in the EEA**,** Module Two (transfer controller to processor), Clauses 1 to 6 and 8 to 18 apply**.**

2. **Standard Contractual Clause Optional Provisions**

In addition to Section 1, where the Standard Contractual Clauses identify optional provisions (or provisions with multiple options) the following shall apply in the following manner:

2.1 Clause 7 (Docking Clause) is omitted;

2.2 In Clause 9(a) (Use of subprocessors) (Module 2 only) – Option 2 shall apply and the parties shall follow the process and timings agreed in the DPA to appoint subprocessors;

2.3 In Clause 11(a) (Redress) (Module 1, 2) – the Optional provision shall **NOT** apply;

2.4 In Clause 17 (Governing Law) (Module 1,2) the Parties agree that Option 2 shall apply according to the following:

(a) where the Customer is established in the EEA, the law of the Member State in which the Customer is established, provided such Member State law allows for third-party beneficiary rights;

(b) where the Customer is established in the UK, the law of England and Wales;

(c) where the Customer is established other than in the UK or EEA, the law of the Member State in which the Customer has appointed its representative under Article 27 of the GDPR; or

(d) otherwise, the law of the Republic of Ireland

2.5 In Clause 18 (Choice of forum and jurisdiction) (Module 1, 2) – the Parties submit themselves to the jurisdiction of the courts of that country whose law applies according to this Schedule.

3. **Supplementary Terms to Standard Contractual Clauses**

3.1 **Documentation and compliance**. For the purposes of Clause 8.9(b) (Module One) and Clause 8.9(e) (Module Two), the review and audit provisions in the Agreement and DPA, if applicable, shall apply.

3.2 Notification and Transparency.

(a) The Parties acknowledge and agree that CoStar, where required by the Standard Contractual Clauses, to notify the competent supervisory authority, shall first provide Customer with the details of the notification, permitting Customer to have prior written input into the relevant notification, where Customer so desires to do, and without delaying the timing of the notification unduly.

(b) For purposes of Clause 8.2 – Module 1, Clause 8.3 – Module 2 and Clause 15.1(a), the Parties agree and acknowledge that it may not be possible for CoStar to make the appropriate communications to data subjects and accordingly, Customer shall (following notification by the Data Importer) have the option to be the party who makes any communication to the data subject, and CoStar shall provide the level of assistance set out in the DPA.

3.3 **Liability**. For the purposes of Clause 12, the liability of the Parties shall be limited in accordance with the limitation of liability provisions in the Agreement.

3.4 **Signatories**. Notwithstanding the fact that the Standard Contractual Clauses are incorporated herein by reference without being signed directly, CoStar and Customer each agree that their execution of the Agreement is deemed to constitute its execution of the Standard Contractual Clauses, and that it is duly authorized to do so on behalf of, and to contractually bind, the Data Exporter or Data Importer (as applicable) accordingly.

4. **Annexes**.

4.1 For the purpose of Annex I of the Standard Contractual Clauses, the Agreement, this DPA (including Annex A and any applicable processing schedules) set out the information regarding the Parties, the description of the transfer and the competent supervisory authority.

4.2 For the purpose of Annex II of the Standard Contractual Clauses, the Security Measures schedule to this DPA (including any brand-specific Security Documentation annexes) contains the technical and organizational measures.

4.3 The specifications for Annex III of the Standard Contractual Clauses regarding subprocessors are determined by this DPA and any Subprocessor list maintained by CoStar in accordance with it.

DPA SCHEDULE 2
(SCC ANNEX I)

DETAILS OF PROCESSING

A. LIST OF PARTIES

1. Data Exporter & Data Importer:

The full name, address and contact details for the Data Exporter and Data Importer (as defined below) are set out in the Agreement; and

(a) In the case of Module 1, the data exporter and Controller is Customer and its relevant Affiliates which are established in the EEA, and the data importer and Controller is CoStar and its relevant Affiliates located in non-adequacy approved third countries for the Services identified in Annex A;

(b) In the case of Module 2, the data exporter and Controller is Customer and its relevant Affiliates which are established in the EEA, and the data importer and Processor is CoStar and its relevant Subprocessors located in non-adequacy approved third countries for the Services identified in Annex A;

B. DESCRIPTION OF TRANSFER

1. Categories of data subjects

The categories of data subjects whose personal data are transferred may include:

- employees, contractors and other personnel of Customer and its Affiliates;
- individual representatives and contacts of Customer's customers, suppliers and business partners;
- users and visitors of CoStar Group Services operated for or used by Customer (including the brands listed in Annex A); and
- any other individuals whose personal data Customer chooses to submit to or collect through the Services in accordance with the Agreement.

2. Categories of personal data

The categories of personal data transferred are determined by Customer's configuration and use of the Services identified in Annex A, and may include some or all of the following:

- identity and identification data (for example, name, user ID);
- contact information (for example, email address, postal address, telephone number);
- professional details (for example, title, company, role);
- technical and usage data (for example, IP address, device identifiers, log data, timestamps, browser and operating system information, referrer URL, interactions with CoStar's online systems, websites, applications, emails and APIs)

- transactional or financial details to the extent submitted by Customer in connection with its use of the Services (for example, billing or payment-related data); and
- any other personal data that Customer or its Affiliates choose to submit to, or collect through, the Services in unstructured or structured form in accordance with the Agreement.

3. Special categories of personal data (if applicable)

The transferred personal data includes the following special categories of data: CoStar's Terms of Use prohibits Customer from using the Services to solicit, display, store, process, send or transmit special categories of data. The Services identified in Annex A are not intended to be used to collect or process special categories of personal data. Accordingly, special categories of data are **not expected** to be transferred.

If, contrary to these requirements, special categories of data are processed, Customer is responsible for ensuring a lawful basis and appropriate safeguards, and CoStar will apply the Security Measures described in the DPA and applicable security schedules

The 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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures are: The applied restrictions or safeguards are those described in the Security Measures schedule to this DPA.

4. Frequency of the transfer

The frequency of the transfer is: The transfer is carried out on a continuous basis and is determined by Customer's configuration of the Services identified in Annex A.

5. Subject matter and nature of the processing

The subject matter of the processing is: CoStar's provision of the Services under the Agreement (including, as applicable, listing and marketing services, analytics and reporting, discovery and directory services, hosting and capture services, and lease and asset management services) and related activities such as storage, hosting, retrieval, transmission, display, analysis and other processing of personal data as necessary to provide, secure and support the Services.

6. Purpose(s) of the data transfer and further processing:

The purpose/s of the data transfer and further processing *is:*

- to provide, operate and support the Services to Customer under and in accordance with the Agreement;
- to provide technical support, issue diagnosis and error correction, and to maintain and improve the security, availability and performance of the Services; and
- to carry out any other processing expressly described in the Agreement and this DPA.

7. Duration

The period for which the personal data will be retained, or the criteria used to determine that period, are as set out in the DPA and Agreement (including any applicable retention, deletion and backup provisions).

8. Subprocessor (if applicable)

For transfers to subprocessors, specify subject matter, nature, and duration of the processing: For transfers to subprocessors, the subject matter, nature and duration of the processing are as described in the Agreement, this DPA and the Subprocessor schedules. Subprocessors may have access to the personal data for the term of this DPA or until their engagement ends or access is removed in accordance with the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with clause 13 of the SCCs
Where the data exporter is established in an EU Member State: The supervisory authority of the country in which the data exporter is established is the competent authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR: The competent supervisory authority is the Member State in which the representative is established.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) without, however, having to appoint a representative pursuant to Article 27(2) of the GDPR: The competent supervisory authority is the supervisory authority in Ireland, namely the Data Protection Commission (https://www.dataprotection.ie/).

DPA SCHEDULE 3
(SCC ANNEX II & III)

ANNEX II
COSTAR TECHNICAL AND ORGANIZATION SECURITY MEASURES ("TOM")

3-1 Overview

CoStar maintains technical and organizational measures designed to protect Personal Data against unauthorized or unlawful Processing and against accidental loss, destruction or damage (the "Security Measures"). This Schedule 3 describes how those Security Measures apply by brand and service. These measures apply in addition to any confidentiality and security obligations in the Agreement.

3-2 CoStar Group brands (other than Matterport, Visual Lease)

For CoStar-branded products and services and the other brands listed in Annex A excluding Matterport and Visual Lease, CoStar applies the Security Measures described in Annex 3-1 **(CoStar Security Measures)**, as updated from time to time in accordance with the DPA. Any updates will not materially reduce the overall level of protection for Personal Data.

3-3 Matterport Platform and Capture Services

For Matterport products and services, the Security Measures are those set out in **Schedule 3-2 (Matterport Technical and Organizational Security Measures)**, which are incorporated here by reference as provided by Matterport. These measures apply to the Matterport Services in full and may be updated by Matterport in accordance with Schedule 3-2, provided that such updates do not result in a material degradation in the protection of Personal Data.

3-4 Visual Lease

For Visual Lease products and services, the Security Measures are those set out in **Schedule 3-3 (Visual Lease Security Measures)**, which are incorporated here by reference as provided by Visual Lease. These measures may be updated by Visual Lease from time to time, provided that such updates do not result in a material degradation in the protection of Personal Data.

3-4 Real Estate Manager

For Visual Lease products and services, the Security Measures are those set out in **Schedule 3-4 (Real Estate Manager)**, which are incorporated here by reference as provided by Real Estate Manager. These measures may be updated by Real Estate Manager from time to time, provided that such updates do not result in a material degradation in the protection of Personal Data.

Schedule 3-1
CoStar Group Security Measures

Software, such as antivirus and antimalware, threat detection tools to identify and address technical flaws.

- Encryption and pseudonymisation.
- Physical security, such as CCTV cameras.
- Passwords and MFA (multi-factor authentication).
- Information security policies governing the approach to data protection and GDPR compliance.
- Business continuity plans, to explain the actions the organisation will take in response to an information security incident.
- Risk assessments to identify information security threats and determine appropriate controls.
- Staff awareness training.
- Reviews and audits to assess the effectiveness of the measures that have been implemented, and to identify opportunities for improvement.

Schedule 3-2
Matterport Technical and Organizational Security Measures

Matterport's technical and organizational security measures ("TOM") describe the controls implemented by Matterport to protect personal data and ensure the ongoing security, confidentiality, integrity, and availability of Matterport's products and services as described in any customer Agreement (the "Services").

I. Overview.

This document is a high-level overview of Matterport's TOMs. More details on the measures we implement are available upon request. Matterport reserves the right to modify or revise these TOMs at any time at its discretion without notice, provided that such modification or revision does not result in a material degradation in the protection provided for personal data that Matterport processes in providing its various Services.

Evidence of the measures implemented and maintained by Matterport described below may be provided to the customer, upon written request. Matterport will provide such evidence no more than once per year, in the form of up-to-date attestations, reports or extracts from independent bodies. Customers may also request at any time Matterport's Trust Package, which includes the most recent SOC2 Type II report, and the latest penetration testing report by visiting Matterport's Trust Center located at https://Matterport.com/trust.

Last updated: January 15, 2026

II. Shared Responsibility.

Matterport's TOMs apply to all standard service offerings provided by Matterport, except for those areas where the customer shares the responsibility for security and privacy TOMs.

Matterport adopts a shared responsibility model where responsibility for data security is shared between Matterport and the customer. This shared model can help relieve the customer's operational burden.

Matterport is responsible for protecting the infrastructure that runs all the Services offered within Matterport's cloud Services. This infrastructure is composed of the hardware, software, networking, and facilities that run the cloud-based Services. Matterport operates, manages, and controls the components from its host operating system and virtualization layer down to the physical security of the facilities in which the service operates. Matterport hosts all its applications with Amazon Web Services (AWS) in a multi-tenancy environment. This allows Matterport to deploy, at scale, its code base to all its infrastructure, so the Services can serve multiple customers. Matterport currently does not support single-tenancy environments. Customer is responsible for the management of the user accounts, and visibility of its models. Customer may have additional responsibilities depending on the type of cloud Services that a customer selects. The type of cloud Services determines the amount of configuration work the customer must perform as part of its security responsibilities.

III. Technical and Organizational Measures.

Matterport maintains the following TOM to protect personal data:

1. **Information Security Program.** Matterport will maintain organizational, management and dedicated staff responsible for the development, implementation, and maintenance of Matterport's information security program.

2. **Security Policies**. Matterport will maintain information security policies and make sure that policies and measures are regularly reviewed and amend such policies as Matterport deems reasonable to maintain protection of Services and data processed therein.

3. **Risk Management.** Matterport will assess risks related to processing of personal data and create an action plan to mitigate identified risks. Matterport will maintain risk assessment procedures for the purposes of such periodic review and assessment of risks to the Matterport organization, monitoring and maintaining compliance with Matterport policies and procedures, and reporting the condition of its information security and compliance to senior internal management.

4. **Physical Security**. AWS maintains physical and environmental security of Matterport's Infrastructure containing customer confidential information designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor, and log movement of persons into and out of Matterport facilities, and (iii) guard against environmental hazards such as heat, fire, and water damage.

5. **System and Network Security.**

- **Network Security.** Matterport will maintain network security controls such as firewalls, remote access control via virtual private networks or remote access solutions, network segmentation,

and detection of unauthorized or malicious network activity via security logging and monitoring, designed to protect systems from intrusion and limit the scope of any successful attack.

- **Data Security**. Matterport will maintain data security controls which include logical segregation of data, restricted (e.g., role-based) access and monitoring, and where applicable, utilization of commercially available and industry-standard encryption technologies.

- **Encryption**. Matterport employs encrypted and authenticated remote connectivity to Matterport computing environments and customer systems. Matterport maintains a cryptographic standard that aligns with recommendations from industry groups, government publications and other reputable standards groups. This standard is periodically reviewed, and selected technologies and ciphers may be updated in accordance with the assessed risk and market acceptance of new standards.

    In-Transit Encryption. All network traffic flowing in and out of the Services data centers, including customer data, is encrypted in transit.

    At-Rest Encryption. Customer data created by the customer, is encrypted at rest with 256-bit AES encryption.

6. **User Access Management**. Matterport will maintain logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review, and revoking/changing access promptly when employment terminates or changes in job functions occur).

- Password Management. Matterport will maintain password controls designed to manage and control password strength, expiration, and usage including prohibiting users from sharing passwords. Matterport shall ensure password hardening standards are in place that align with accepted industry security frameworks to ensure sufficient controls.

- Workstation Protection. Matterport will implement protections on end-user devices and monitor those devices to be in compliance with the security standard requiring screen lock timeout, malware software, firewall software, remote administration, unauthenticated file sharing, hard disk encryption and appropriate patch levels. Controls are implemented to detect and remediate workstation compliance deviations. Matterport will securely sanitize physical media intended for reuse prior to such reuse and will destroy physical media not intended for reuse.

- Media Handling. Matterport will implement protections to secure portable storage media from damage, destruction, theft or unauthorized copying and the personal data stored on portable media through encryption and secure removal of data when it is no longer needed. Additional similar measures will be implemented for mobile computing devices to protect personal data.

7. **Auditing and Logging.** Matterport will maintain system audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review. Matterport will create, protect and retain such log records to the extent needed to enable monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate information system activity, including successful and unsuccessful account logon events, account management, events,

security events, object access, policy change, privileged functions, administrator account creation/deletion and other administrator activity, data deletions, data access and changes, firewall logs, and permission changes.

8. **Change Management.** Matterport will maintain change management procedures and tracking mechanisms designed to test, approve, and monitor all changes to Matterport technology and information assets. Any modifications to applications by Matterport (or a third party) that will create a major change or discontinuity – other than modifications linked to corrective maintenance – will be communicated to customers before being put into production so that customer may take the necessary measures to address any such discontinuity.

9. **Threat and Vulnerability Management.** Matterport will maintain measures meant to regularly identify, manage, assess, mitigate and/or remediate vulnerabilities within the Matterport computing environments. Measures include:

- Patch management
- Anti-virus / anti-malware
- Threat notification advisories
- Vulnerability scanning (all internal systems)
- Annual penetration testing (Internet facing systems) within remediation of identified vulnerabilities by a third-party security firm.

10. **Security Incidents**. Matterport will maintain incident response procedures designed to allow Matterport to investigate, respond to, mitigate, and notify of events related to Matterport technology and information assets. Matterport will follow documented incident response procedures to comply with applicable laws and regulations including data breach notification to any Data Controller, without undue delay, but in any event within forty-eight (48) hours, after Matterport's validation of a personal data breach known or reasonably suspected to affect customers' personal data.

11. **Business Continuity Plans.** Matterport will maintain defined business resiliency/continuity and disaster recovery procedures, as appropriate, designed to maintain service and recovery from foreseeable emergency situations or disasters, consistent with industry standard practices.

12. **Vendor Management.** Matterport maintains a formal vendor management program, including vendor security reviews for critical vendors, to ensure compliance with Matterport's information security policies. Matterport may engage and use vendors, acting as subprocessors, that access, store, or process certain customer data. Matterport maintains updated information on its subprocessors on its website at https://Matterport.com/Matterport-subprocessors

13. **Privacy by Design.** Matterport will incorporate Privacy by Design principles for systems and enhancements at the earliest stage of development as well as educate all employees on security and privacy annually.

14. **Security of Disposed and Retained Data.** Matterport retains operational procedures and controls for the secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Matterport possession. Matterport retains back-up data in cloud storage for seven (7) days and may retain other data in accordance with applicable laws pursuant to Matterport's internal retention policies.

Schedule 3-3
Visual Lease Security Measures

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

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 freedoms of natural persons.

Visual Lease shall maintain compliance with the security principles as outlined in the GDPR and UK GDPR.

Measures of pseudonymisation and encryption of personal data:

- Encryption at rest and encryption in transit;
- Encryption key kept in the US;

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services:

- Confidentiality arrangements;
- Information security policies and procedures;
- Backup procedures;
- Remote storage;
- Mirroring of hard disks (e.g., RAID technology);
- Uninterruptible power supply;
- Anti-virus/firewall protection, security patch management;
- Intrusion prevention, monitoring and detection;
- Availability controls to protect personal data against accidental destruction or loss;

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:

- Business continuity plan;
- Disaster recovery procedure;
- Incident response plan;

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing:

- Internal and external audit program, audit reports and documentation;
- Periodic testing of back up processes and business continuity procedures;
- Risk evaluation and system monitoring on a regular basis;

- Vulnerability and penetration testing on a regular basis, not no less than annually;

Measures for user identification and authorization:

- Internal policies and procedures;
- User authentication controls, including secure methods of assigning selecting and storing access credentials and blocking access after a reasonable number of failed authentication access;
- Restricting access to certain users;
- Access granted based on a need-to-know, supported by protocols for access authorization, establishment, modification and termination of access rights;
- Logging and reporting systems;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access personal data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;

Measures for the protection of data during transmission*:*

- Encryption in transit;
- Transport security;
- Network segregation;
- Logging;

Measures for the protection of data during storage*:*

- Encryption at rest;
- Access controls;
- Separation of databases and logical segmentation of VLC personal data from data of other vendor customers;
- Segregation of functions (production/testing/development);
- Procedures for storage, amendment, deletion, transmission of data for different purposes;

Measures for ensuring physical security of locations at which personal data are processed:

- Establishing security areas, restriction of access paths;
- Establishing access authorizations for employees and third parties with a need-to-know;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;

- Door locking (electric door openers etc.);
- Security staff, janitors;
- Surveillance facilities, video/CCTV monitor, alarm system;
- Securing decentralized processing equipment and personal computers;

Measures for ensuring events logging:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g., password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Encryption at rest and in transit;

Measures for ensuring system configuration, including default configuration:

- Up-to-date baseline configuration documentation and settings;

Measures for internal IT and IT security governance and management:

- Information security policies and procedures;
- Incident response plan;
- Regular internal and external audit;
- Review and supervision of information security program;

Measures for certification/assurance of processes and products:

- SOC I, Type 2

Measures for ensuring data minimisation:

- Documentation regarding which data categories need to be processed;
- Ensure that the minimum amount of data is processed to fulfill the purpose of the processing;

Measures for ensuring data quality:

- Personal data is kept accurate and up to date;
- Data is corrected upon request or where necessary;

Measures for ensuring limited data retention:

- Records retention schedule;
- Data retention policy;
- Personal data is deleted or irreversibly anonymized after expiration of the retention period or deleted post-termination upon written request from Client Administrator;

Measures for ensuring accountability:

- Internal policies and procedures;

- Records of data processing activities;
- Adequate agreements with third parties;
- Vendor onboarding process and questionnaire;
- Monitoring of contract performance;
- InfoSec training program;

Measures for allowing data portability and ensuring erasure:

- Personal data is made available upon request in an electronically portable format using industry standards;
- Reduction methods are used, where necessary;
- Secure disposal of information stored on magnetic and non-magnetic media that prevents potential recovery of the information.

For transfers to (sub) processors, also describe the specific technical and organisational measures to be taken by the (sub) processor to be able to provide assistance to the controller and, for transfers from a processor to a subprocessor, to the data exporter Data importer maintains a process to ensure that each subprocessor that processes personal data of data exporter is required to:

1. Process personal data only on behalf of and in accordance with the instructions of the data importer;

2. Inform the data importer of any requests from data subjects to exercise their rights under the GDPR, and to provide assistance to the data importer in relation to the handling of such requests;

3. Assist the data importer in relation to its obligations to (a) implement appropriate technical and organizational measures to ensure the security of data processing, (b) carry out a data protection impact assessment, and (c) to the extent required by applicable law, consult with the relevant supervisory authority, and assist the data importer in relation to the data importer's obligations to provide the same assistance to the data exporter;

4. Implement, maintain and comply with a documented procedure for reviewing and responding to requests to access or disclose personal data that are received from foreign government authorities;

5. Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk associated with the processing by the subprocessor;

6. Delete personal data or return it to the data importer on termination of the relationship between the data importer and subprocessor; and

7. Notify the data importer of a personal data breach and provide reasonable assistance to the data importer to prevent, mitigate, or rectify such personal data breach, and to enable the data importer to satisfy its obligation to notify the data exporter of a personal data breach.

Schedule 3-4
Real Estate Manager Technical and Organizational Security Measures

Real Estate Manager (REM)'s technical and organizational measures are described at https://trust.costargroup.com/?product=realestatemanager and are incorporated by reference. REM may update these measures from time to time, provided the overall security is not materially diminished.

Last updated: January 15, 2026

ANNEX III

LIST OF SUBPROCESSORS

4-1 General

CoStar may engage Subprocessors to support the provision of the Services. CoStar remains responsible for its Subprocessors and will impose data protection obligations on them that provide at least the level of protection required by the DPA. Customer's rights to receive notice of and object to new Subprocessors are described in the DPA.

4-2 CoStar Group brands (excluding Matterport, Visual Lease or REM)

For CoStar-branded products and services and the other brands listed in Annex A, **excluding Matterport and Visual Lease**, the current Subprocessors are those listed in **Annex 4-1 (CoStar Subprocessors)** or, if indicated there, at the URL specified in Schedule 4-1.

4-3 Matterport Platform and Capture Services

For Matterport products and services, the current Subprocessors are those **Annex 4-2 (Matterport Subprocessors)** or, if indicated there, at the URL specified in Schedule 4-2.

4-4 Visual Lease

For Visual Lease products and services, the current Subprocessors are those **Annex 4-3 (Visual Lease Subprocessors)** or, if indicated there, at the URL specified in Schedule 4-3.

4-4 Real Estate Manager

For Visual Lease products and services, the current Subprocessors are those **Annex 4-4 (REM Subprocessors)** or, if indicated there, at the URL specified in Schedule 4-4.

Annex 4-1
CoStar Group Subprocessors

Data exporter authorizes the Subprocessors disclosed and available in CoStar's Trust Center at https://trust.costargroup.com/ to process customer data and to provide and operate the CoStar Services to which they have subscribed under their Agreement. CoStar may update the list from time to time in accordance with this DPA.

Annex 4-2
Matterport Subprocessors

Data exporter authorizes the Subprocessors disclosed via the applicable hyperlink(s) below (also available in Matterport's Trust Center at http://www.Matterport.com/trust) to process customer data and to provide and operate the Matterport's Services to which they have subscribed under their Agreement:

Last updated: January 15, 2026

https://Matterport.com/Matterport-subprocessors

Matterport may update the list from time to time in accordance with this DPA.

Annex 4-3
Visual Lease Subprocessors

Data exporter authorizes the Subprocessors below to process customer data and to provide and operate the Visual Lease's Services to which they have subscribed under their Agreement:

Infrastructure & Sales Enablement Subprocessors				
VL may use the following Subprocessors to provide infrastructure that assists with the delivery of VL Services:				
Subprocessor	**Location of Subprocessor**	**Subject Matter of Processing**	**Nature of Processing**	
Pendo.io	301 Hillsborough Street, Raleigh, NC 27603, USA	Product Analytics	**Combining powerful software usage analytics with in-app guidance and user feedback capabilities on behalf of VL**	
Jira	350 Bush Street, Floor 13, San Francisco, CA 94104, USA	Customer Support and Account Management	**Bug/issue tracking in-app tool on behalf of VL**	
Salesforce	415 Mission Street, 3rd Floor, San Francisco, CA, 94105, USA	Customer Support and Account Management	**Manage customer data, sales operations, and marketing campaigns on behalf of VL**	
Amazon Web Services	410 Terry Avenue N., Seattle, WA, 98109, USA	Cloud Infrastructure	**Providing compute power, content delivery, database storage, etc., on behalf of VL**	
Hubspot	25 1st Street, Cambridge, MA 02141, USA	Customer Support and Account Management	**Providing a centralized customer database on behalf of VL**	
OwnBackup	940 Sylvan Avenue, Englewood Cliffs, NJ, 07632, USA	Backup Platform for Salesforce	**Provides cloud data protection on behalf of VL**	

Salesloft	1180 W. Peachtree Street, NW, Suite 600, Atlanta, GA 30305, USA	Customer Support and Account Management	**A cloud-based sales engagement platform on behalf of VL**	
PowerBi (Microsoft)	One Microsoft Way, Redmond WA, 98052, USA	Product Analytics	**A data visualization and reporting platform on behalf of VL**	
Drift	222 Berkeley Street, Boston, MA 02116, USA	Customer Support Chatbox	**Facilitates communication with website visitors in real-time on behalf of VL**	
Sendoso	655 Montgomery Street, Suite 1720, San Francisco, CA 94111, USA	Account Management	**A platform for the delivery of corporate gifts on behalf of VL**	
Vonage Contact Center	23 Main Street, Holmdel, NJ 07733, USA	Customer Support	**Providing integrated communication services on behalf of VL**	
Seismic	12390 El Camino Real, San Diego, CA 92130, USA	Sales Support	**Sales enablement and digital sales engagement solution on behalf of VL**	
Clari	1154 Sonora Court, Sunnyvale, CA, 94086, USA	Sales and Account Management	**Manage sales pipeline and forecast future revenue on behalf of VL. The use of Clari is optional and only upon instruction of Client**	
Zoom	55 Almaden Blvd., 6th Fl, San Jose, CA, 95113, USA	Video Conferencing System	**Software-based video conferencing solutions**	

Annex 4-4
REM Subprocessors

Data exporter authorizes the Subprocessors disclosed and available in REM's Trust Center at https://trust.costargroup.com/?product=realestatemanager to process customer data and to provide and operate the REM Services to which they have subscribed under their Agreement. REM may update the list from time to time in accordance with this DPA

Last updated: January 15, 2026

DPA SCHEDULE 4
UK AND SWISS ADDENDUM

1. **UK ADDENDUM**

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

1.1. Part 1: Tables

Table 1: Parties. DPA Schedule 2 is hereby incorporated.

Table 2: Selected SCCs, Modules and Selected Clauses. DPA Schedule 1 is hereby incorporated.

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties is set forth in DPA Schedule 2.
Annex 1B: Description of Transfer is set forth in DPA Schedule 2.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data is set forth in DPA Schedule 3.
Annex III: List of Sub processors (Modules 2 and 3 only) is as set forth in DPA Schedule 3.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☐ neither Party

1.2. Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs, those terms shall have the same meaning as in the Approved EU SCCs, and where not defined there, in the DPA. In addition, the following terms have the following meanings:

Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfills the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

> "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";

c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

    b. reflects changes to UK Data Protection Laws;

19. The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

20. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the Addendum; and/or

    b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

21. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

2. **SWISS ADDENDUM**

As stipulated in the DPA, this Swiss Addendum shall apply to any processing of Customer Personal Data subject to Swiss data protection law or to both Swiss data protection law and the GDPR.

2.1. Interpretation of this Addendum

(a) Where this Addendum uses terms that are defined in the Standard Contractual Clauses as further specified in Schedule 1 of this DPA, those terms shall have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:
– "This Addendum" means This Addendum to the Clauses.
– "Clauses" means The Standard Contractual Clauses as further specified in Schedule 1 of this DPA.
– "Swiss Data Protection Laws" means The Swiss Federal Act on Data Protection of 19 June 1992 and the Swiss Ordinance to the Swiss Federal Act on Data Protection of 14 June 1993, and any new or revised version of these laws that may enter into force from time to time.
(b) This Addendum shall be read and interpreted in the light of the provisions of Swiss Data Protection Laws, and so that it fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.
(c) This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Data Protection Laws.
(d) Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

2.2. Hierarchy. In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

2.3. Incorporation of the Clauses

(a) In relation to any processing of personal data subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the GDPR, this Addendum amends the DPA including as further specified in Schedule 1 of this DPA to the extent necessary, so they operate:

(i) for transfers made by the data exporter to the data importer, to the extent that Swiss Data Protection Laws or Swiss Data Protection Laws and the GDPR apply to the data exporter's processing when making that transfer; and
(ii) to provide appropriate safeguards for the transfers in accordance with Article 46 of the GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

(b) To the extent that any processing of personal data is exclusively subject to Swiss Data Protection Laws, the amendments to the DPA including the SCCs, as further specified in Schedule 1 of this DPA and as required by clause 2.1 of this Swiss Addendum, include (without limitation):

(i) References to the "Clauses" or the "SCCs" means this Swiss Addendum as it amends the SCCs and
(ii) Clause 6 Description of the transfer(s) is replaced with:

"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 those specified in Schedule 1 of this DPA where Swiss Data Protection Laws apply to the data exporter's processing when making that transfer."

(iii) References to "Regulation (EU) 2016/679" or "that Regulation" or ""GDPR" are replaced by "Swiss Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" or "GDPR" are replaced with the equivalent Article or Section of Swiss Data Protection Laws to the extent applicable.
(iv) References to Regulation (EU) 2018/1725 are removed.
(v) References to the "European Union", "Union", "EU" and "EU Member State" are all replaced with "Switzerland".
(vi) Clause 13(a) and Part C of Annex I are not used; the "competent supervisory authority" is the Federal Data Protection and Information Commissioner (the "FDPIC") insofar as the transfers are governed by Swiss Data Protection Laws.
(vii) Clause 17 is replaced to state:

"These Clauses are governed by the laws of Switzerland insofar as the transfers are governed by Swiss Data Protection Laws".

(viii) Clause 18 is replaced to state:

"Any dispute arising from these Clauses relating to Swiss Data Protection Laws shall be resolved by the courts of Switzerland. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence. The Parties agree to submit themselves to the jurisdiction of such courts."

Until the entry into force of the revised Swiss Data Protection Laws, the Clauses shall also protect personal data of legal entities and legal entities shall receive the same protection under the Clauses as natural persons.

2.4. To the extent that any processing of personal data is subject to both Swiss Data Protection Laws and the GDPR, the DPA including the Clauses as further specified in Schedule 1 of this DPA will apply (i) as is and (ii) additionally, to the extent that a transfer is subject to Swiss Data Protection Laws, as amended by clauses 2.1 and 2.3 of this Swiss Addendum, with the sole exception that Clause 17 of the SCCs shall not be replaced as stipulated under clause 2.3(b)(vii) of this Swiss Addendum.

2.5. Customer warrants that it has made any notifications to the FDPIC which are required under Swiss Data Protection Laws.