Exhibits to the SaaS Agreement

Last Updated: June 1, 2026

Integration with Unify's Software and Services Agreement

This Exhibits document is incorporated by reference into, and forms an integral part of, the Software and Services Agreement (the "Agreement") entered into between the Customer and the Service Provider. The terms and conditions set forth in these Exhibits are binding and shall have the same force and effect as if included in the main body of the Agreement. In the event of any conflict between the terms of this Exhibits document and the main Agreement, the terms of the Agreement shall prevail, unless expressly stated otherwise in a specific Exhibit; provided that the order of precedence in Section 14.12 of the Agreement applies.

Exhibit A: Software Service Level Agreement

1. Service Levels. The Purpose of this Service Level Agreement (the "SLA") is to identify and define the characteristics and levels of performance and availability that Unify will provide and Customer will receive from the Software and the Unify System pursuant to the Agreement to which the SLA is attached. Unless otherwise indicated, the capitalized terms used in the SLA have the same meanings as they do in the Agreement.

2. Access & Connectivity. The Provider will host the Unify LIV Web Portal, the Software and the Customer Data on the Unify System and, in accordance with this Agreement, Customer will have access thereto via the world-wide web, using a current, supported web browser (for example, the latest versions of Google Chrome, Apple Safari, Microsoft Edge, or Mozilla Firefox). The Provider shall be solely responsible for maintaining connectivity between the Provider System and its Internet service provider. The Provider shall have no responsibility whatsoever for ensuring the connectivity between such Internet service provider and Customer.

3. Capacity Planning. The Provider will review System capacity and Customer needs on a regular basis or as requested by Customer, without cost to Customer, and where deemed necessary by the Provider or Customer in its reasonable discretion, the Provider will scale the System hardware and server infrastructure to accommodate increasing demand and maintain desired service levels.

4. Availability

The availability of Unify LIV (including the Web Admin Site and the Mobile App) will be 99.5% per calendar month. Availability will be calculated as follows:

Availability = 100 – (100 × Total Downtime / Total Possible Uptime), where Total Downtime refers to the sum of all minutes of system downtime in a given month, and Total Possible Uptime refers to the total minutes in the given month, excluding downtime caused by:

- (a) Scheduled Maintenance,
- (b) General Internet Failures, and failures of third-party providers outside the Provider's control (including cloud-hosting, payment-processing, SMS, email, and app-store providers),
- (c) Force Majeure events, or
- (d) Component, software, or hardware failures not within the Provider's control.

For clarity, the following are excluded from Total Downtime: Scheduled Maintenance and Unscheduled Maintenance; Customer-caused issues or Customer equipment/network problems; suspensions permitted under the Agreement; and outages of third-party providers described above.

The Provider will provide a monthly report of Availability to the Customer within 10 days following the end of each month. If the Provider fails to meet the Availability target for any given month, the Provider will credit the Customer an amount equal to 5% of the regularly billed fees for that month.

Service credits under this Section 4 are the Customer's sole and exclusive remedy, and the Provider's entire liability, for any failure to meet the Availability target, except for the Customer's termination rights expressly stated below. To receive a credit, the Customer must request it in writing within thirty (30) days after the end of the affected month; credits are applied against future invoices and are not redeemable for cash.

If the Provider fails to meet the Availability target for two consecutive months or three times in any 12-month period, the Customer may request that the Provider resolve the issue within 30 days. If unresolved, the Customer may terminate this Agreement without further obligation or liability (other than payment for Services already provided). If the Availability is below 85% in any given month, the Customer may terminate this Agreement immediately.

5. Scheduled Maintenance. The Provider will have the right, up to twice per month (not to exceed 10 hours per month) during the Term, to render the System inaccessible to perform Scheduled Maintenance, including updates, upgrades, and performance enhancements. Scheduled Maintenance is excluded from System Downtime calculations. Maintenance windows will be communicated at least 48 hours in advance, and will typically occur during off-peak hours.

Standard Scheduled Maintenance windows will be scheduled to occur during low-usage hours for the Customer's primary location (in the local time zone identified in the Order Form or onboarding configuration) and will be scheduled to avoid active evening resident-usage hours; nightly backups will occur during the same low-usage window. The Provider will identify the applicable time zone and maintenance window in the Order Form or onboarding configuration.

The Provider also reserves the right to change Scheduled Maintenance by providing the Customer with 48 hours prior notice in a reasonable method elected by the Provider. The Provider shall use commercially reasonable efforts to minimize the System Downtime even during Scheduled Maintenance activities.

6. Unscheduled Maintenance. Subject to Section 7, the Provider will also have the right at any time to render the System inaccessible to Customer in order to provide any emergency maintenance, repairs, upgrades or other services to the System deemed necessary by the Provider, in its discretion ("Unscheduled Maintenance"). The Provider will provide the Customer with notice of Unscheduled Maintenance as soon as possible by a reasonable method elected by the Provider.

7. System Downtime. "System Downtime" refers to the unavailability of the System to Authorized Users resulting solely from unplanned component, software, or hardware failures, excluding Scheduled Maintenance, general Internet failures, Force Majeure events, third-party provider outages, Customer-caused issues, or failures outside the Provider's control.

8. Unrelated Problems. The Provider will cooperate with third parties and Customer's technical support personnel at their request in good faith, in an effort to resolve problems with communications, networks, hardware and software unrelated to the System that impact on the availability thereof to Customer, provided that the Provider will have no responsibility for such problems.

9. Customer Obligations. General Customer obligations are set out in Schedule "I". Customer obligations specific to individual Services and Software are set out in Schedule "A".

10. Continuity. The Provider will perform the following, at its own expense:

- (a) The Provider will use commercially reasonable efforts to ensure continued availability in the event that the System or any material part or parts thereof becomes unavailable or inaccessible to Customer.
- (b) System Redundancy. The Provider will have available the following redundant infrastructure: (i) Redundant Internet connectivity through physically diverse connections, (ii) Redundant servers for immediate switch-over to back up in event of server or component failure.
- (c) Back-up; Offsite Storage. On a daily basis throughout the Term, the Provider will create backup copies of the Customer Data stored in the System. On a weekly basis, the Provider will create a backup copy of the Customer Data stored in the System, and securely store such copies in a separate data facility. All copies of daily backups shall be retained by the Provider for at least two (2) weeks and monthly backups to be retained for at least one (1) year following the creation of those backup copies. These backups support the Recovery Point Objective (RPO) of twenty-four (24) hours and the Recovery Time Objective (RTO) of four (4) hours referenced in Section 8.3 of the Agreement. Following termination, backup copies of Customer Data are deleted or overwritten in the ordinary course within the retention periods stated above and remain subject to the confidentiality and security obligations of the Agreement until deleted.
- (d) Other Means. If deemed necessary by the Provider or Customer, the Provider will use other commercially reasonable efforts to permit Customer to access the Software and the Customer Data by using or engaging hardware, software, and facilities functionally-equivalent to the Unify System from a substitute supplier.

11. Hosting & Data Residency. The Software and Customer Data are hosted on commercially reasonable cloud infrastructure (currently Google Cloud Platform). Where offered, the Customer may elect a data-residency region (United States or Canada) in the Order Form; absent an election, the Provider's default region for the Customer's market applies. The Provider's use of cloud and other sub-processors, and notice of material changes to sub-processors, is addressed in Section 8 of the Agreement and any data processing addendum entered into by the parties.

12. Security. The Provider will establish industry standard security features for regulating access to the non-public Unify LIV Web Portal, including the Software and the Customer Data, and shall provide documentation of such security features to Customer so that Customer can cooperate with the Provider in the implementation of security protocols and procedures. Detailed security and data-protection obligations are addressed in Section 8 of the Agreement and any data processing addendum entered into by the parties

13. Software Support. Support Services in connection with the Software are set forth in Exhibit B (Support Services & Hosting Services).

Exhibit B: Support Services & Hosting Services

1. Standard Support Services

1.1 Services Included. From and after the Agreement Effective Date, the Provider will provide the following Standard Support Services to Customer with respect to the Software in the manner set forth herein:

- (a) Telephone & Online Support, including: (i) identification and resolution of errors, failures, and malfunctions of the Software; (ii) explanation of functions and features of the Software; (iii) clarification of Documentation relating to the Software; (iv) guidance in the operation of the Software; (v) consultation on data processing problems in connection with the Software;
- (b) Problem and error correction, including repairs, corrections, and bug fixes, reasonably necessary to correct problems, errors, failures and malfunctions of the System of which the Provider becomes aware in order to make such System function in accordance with the Specifications and the Service Level Agreement, and such other Bug Fixes (as defined in the Agreement).

The term "Specifications" is defined as the documented performance standards and expected functionalities of the Software and Services as outlined in the Order form.

1.2 Support Availability. Support will be provided on an as-required basis, Monday through Friday during Service Hours (defined below). All inquiries should be addressed to support@livwith.com, or logged through the Provider's online help center.

1.3 Service Hours: The Provider Help Desk will be available to receive phone calls and/or emails from the Customer between the hours of 9:00 a.m. and 5:00 p.m. the Provider's standard support hours on business days, in the time zone of the region identified in the Order Form. Extended or local-hours coverage is available as a paid add-on ("Service Hours"). The Provider shall provide upon request by Customer a price quotation for extending the Service Hours.

1.4 Service Desk Response during Service Hours. For all Customer emails received during Service Hours, the Provider's Customer Service Representative will: (a) Assign a priority code (as described in Section 1.6) to the ticket; (b) Provide a good faith estimate for the time required for resolution, having regard to the nature of the question or problem and the priority code assigned to it; and (c) Attend each service request in the order of the priority codes and date of receipt of the call.

1.5 Support after Service Hours. The Maintenance and Support Services do not include support outside Service Hours for priority 2 and 3 service requests. Service fees in respect of support outside Service Hours for priority 2 and 3 service requests are in addition to the Maintenance and Support fees. Support outside Service Hours shall be invoiced to Customer at the end of each month in which such services are rendered to Customer at Provider's premium time and support rates for such services. Such support may be subject to a minimum charge of 1 hour per occurrence. Any Support outside Service Hours for priority 2 and 3 service requests shall be approved by the Customer in writing prior to being initiated.

1.6 Definitions and Priority Codes. (a) "Priority 1" means a problem in the Software that disables the functionality of the Software for a Licensed User, or a confirmed security incident affecting Customer Data. (b) "Priority 2" means a problem in the Software that has a serious adverse impact on the functionality of the Software. (c) "Priority 3" means a problem that is not a Priority 1 or Priority 2 problem, and that has a material effect on the functionality of the Software.

1.7 Response. The Provider will respond to each service call as follows in accordance with the corresponding priority codes.

- (a) Priority 1: Provider will assign an incident manager and respond to Customer within 120 minutes, and use its commercially reasonable efforts, working diligently, to repair the error, defect or problem. If such error, defect or problem is not resolved within 24 hours of receipt, Provider qualified staff will work with Customer personnel continuously, either virtually, at Provider's location, or, at Customer's request, at any Customer location.
- (b) Priority 2: Provider will assign an incident manager and respond to Customer within 12 hours, and use its commercially reasonable efforts, working diligently during 16 to 24 Service Hours, to repair the error, defect or problem.
- (c) Priority 3: Provider will respond to Customer within twenty-four hours and use its commercially reasonable efforts to repair the error, defect or problem within 72 hours.

The level of service and order of priority shall be determined by the priority codes assigned by the Provider acting reasonably. If the Provider receives an email for a lower priority service request, service for such items will be scheduled after all higher priority service tickets have been addressed.

1.8 Customer's Obligations. Customer will provide the Provider with all available information concerning a request for Support Services and the related circumstances.

1.9 Response Times. Provider will make commercially reasonable efforts to respond to Customer requests for Support in a timely manner as per section 1.7.

2. Special Support

2.1 At Customer's request, the Provider will provide special Support Services with respect to the Software, for special Support Fees to be agreed upon. The special Support Services provided by Unify to Customer will be determined by the parties on a 'per request' basis.

B. Hosting Services

1.1 For the Term of the Agreement, the Provider agrees to provide Customer with the following Hosting Services:

- (a) Provider shall host the Software and the Customer Data on the Provider System to permit Authorized Users to access and use the Software through the Internet, and host and make available the Unify LIV Web Portal for the purpose of such access and use, and provide the foregoing in conformance with the Specifications and the Service Level Agreement.
- (b) Provider shall host the Software, the Customer Data and the Provider System on secure servers appropriately configured to host and operate the Software and process the Customer Data in accordance with the Specifications and the Service Level Agreement.
- (c) Provider shall host, store and process the Customer Data in connection with Authorized Users' use of the Software in accordance with the Specifications and perform all necessary database management and administration in connection with the foregoing;
- (d) Provider shall maintain all necessary data center local area network connectivity and network connectivity between the Provider System and the Internet through to Provider's Internet service provider;

- (f) Provider shall, at its own cost and expense, acquire, license, and maintain all related application and system servers, routers, firewalls, system software and other equipment, firmware and software necessary for the foregoing; and
- (g) Provider shall be responsible for the following: Application servers/routers/firewalls; Technical Unify System Support Services; Data protection and security; Database administration; Internet connectivity (for Unify System servers); Unify System redundancy and backups; Nightly Unify System backups; and 24×7 application monitoring to ensure proper operation of the Provider System and the Software.

2.2 Provider shall be responsible for the overall maintenance of the Provider System, which shall be provided in order to achieve the service levels set out in Exhibit A.

Exhibit C: Training and Implementation Services

It is generally anticipated that use of the Software will require minimal Training Services. Software Documentation will be provided to all Authorized Users and the Provider's staff will be available to answer any questions. Online Help Center will be available to streamline education of new users.

Provider will work in good faith with Customer to achieve successful implementation and Software roll out at new sites, and the introduction of any new modules at all sites.

Training with respect to use of the Software shall be provided to the Customer via a virtual meeting or pre-recorded sessions. At Customer's request, training can be delivered in in-person sessions, subject to a separate quote for travel and time.

Refer to **Unify LIV's Activation and Onboarding policy** for a detailed guide and steps of platform activation and onboarding activities involved.

Exhibit D: Resident Terms of Use / End-User License Agreement (EULA)

These Resident Terms of Use ("Resident Terms") form part of the SaaS Agreement between Creative Cloud Consulting Inc. ("Unify," "we," "us") and the Customer (your property, association, or manager) and govern your use, as an Authorized User, of the Unify LIV web portal, mobile application, and related services (the "Platform"). Capitalized terms not defined here have the meanings in the Agreement. By creating an account or using the Platform, you agree to these Resident Terms.

1. Eligibility and Accounts. You must be at least 18 years old (or the age of majority where you live) to create an account. You may use the Platform only for a property where the Customer has authorized your access, and only in the role assigned to you (for example, resident, owner, tenant, board or council member, property manager, concierge or front-desk staff, vendor, or administrator). You are responsible for keeping your login credentials confidential and for activity under your account, and you agree to notify us or the Customer of any unauthorized use.

2. Authorized Property Use. Your access is tied to the Customer's subscription and the property you are associated with. The Customer (not Unify) decides who may access the Platform, what role you have, and what content, rules, and charges apply to your community. The Customer may add, change, or remove your access.

3. No Emergency or Life-Safety Use. The Platform is not an emergency-response, alarm, or life-safety system and must not be relied on to report or respond to emergencies. In an emergency, call 911 (or your local emergency number) or your building's designated emergency contact. Maintenance tickets, messages, and other Platform features are not monitored for emergencies.

4. Communications, Push Notifications, SMS, and Email. By using the Platform, you agree to receive service-related communications (such as account, building, booking, parcel, and maintenance notices) through the Platform, in the form of push notifications, email, and/or SMS. You can manage push notifications in your device settings and unsubscribe from non-essential marketing emails using the unsubscribe link, or reply STOP to opt out of marketing SMS. Standard message and data rates may apply. Some service communications are necessary to use the Platform and cannot be turned off without closing your account.

5. Amenity Bookings; Cancellations, Deposits, Refunds, Penalties, and Disputes. Amenity availability, booking windows, deposits, cancellation and refund rules, fees, and penalties are set and enforced by the Customer, not Unify. Unify provides the technology that applies the Customer's rules. Questions, refund requests, and disputes about a booking, deposit, fine, or charge must be directed to the Customer (your property or association). Unify is not responsible for the Customer's rules or enforcement decisions, except to the extent a charge resulted from a verified Platform error attributable to Unify.

6. Parking and Visitor Access. Visitor parking, permits, and access features apply the Customer's rules and time limits. The Customer is responsible for enforcement (including any towing, fines, or violation charges); Unify does not make enforcement decisions.

7. Violation and Other Payments. Where enabled, you may pay fines, violation charges, deposits, or other property-related amounts through the Platform. These charges originate from the Customer. Payments are processed by a third-party Payment Processor (for example, Stripe); your use of that processor is subject to its terms. A convenience or processing fee may apply and will be disclosed before you pay. Refunds, reversals, and disputes about the validity of a charge are handled by the Customer.

8. Marketplace and Community Posts; User-Generated Content. If your community enables marketplace listings, events, or community posts, you are solely responsible for the content you post and for your transactions with other users. You retain ownership of your content but grant Unify and the Customer a limited license to host and display it on the Platform to operate the features. Unify is not a party to, and is not responsible for, transactions between users.

9. Advertising. The Platform may display advertisements or promotions from the Customer or local retailers. Advertisements are the responsibility of the advertiser and the Customer. Inclusion of an advertisement is not an endorsement by Unify, and any metrics shown (such as impressions or click-through) are informational only and not guaranteed.

10. App Store Terms. If you download the mobile app from the Apple App Store or Google Play, you also agree to that store's terms. Those stores are not responsible for the Platform, and any store-required end-user terms (including Apple's standard EULA terms) apply to your download.

11. Prohibited Conduct.

You may not

- Use the Platform to infringe upon any third party's legal rights, or violate any applicable law, your community's governing documents, or these Resident Terms
- Upload, share, or distribute viruses, malware, or malicious content.
- Attempt unauthorized access to any systems, networks, or data.
- Engage in harassment, abuse, defamation, or threats against others.
- Distribute spam or unsolicited promotional materials.
- Reverse engineer, decompile, or attempt to extract source code.
- Use automated tools such as bots or scrapers to interact with the Platform.
- Circumvent any security or access control features.
- Transmit or upload content that is unlawful, obscene, offensive, or discriminatory.
- Impersonate any person, or post another person's personal information without consent.

12. User-Generated Content

All content you submit must respect the intellectual property and privacy rights of others, exclude confidential third-party information you are not authorized to share, and be lawful, accurate, and respectful.

13. Moderation and Enforcement.

Unify and the Customer may investigate suspected violations and may remove content or suspend or terminate access for violations of these Resident Terms, consistent with the Agreement. Unify may involve law enforcement where required by law. Decisions about community rules and enforcement are made by the Customer.

14. Privacy. Your personal information is handled as described in the Unify LIV Privacy Policy and, as between Unify and the Customer, the Data Processing Addendum. Your community (the Customer) determines what data is collected through the Platform and how it is used for community operations.

15. Disclaimers; Limitation of Liability. The Platform is provided "as is" to the fullest extent permitted by law. To the maximum extent permitted by law, Unify is not liable for indirect, incidental, special, or consequential damages, and Unify's total liability to you for any claim relating to the Platform will not exceed USD $100. Some jurisdictions do not allow certain limitations, so some of these limitations may not apply to you. Nothing limits liability that cannot be limited by law.

16. Accessibility. Unify uses commercially reasonable efforts to make the Platform's core resident-facing features conform to WCAG 2.1 AA or a substantially equivalent standard. If you need assistance or an alternative format for a notice, contact support@livwith.com. Content uploaded by your community (such as PDFs and images) is the Customer's responsibility.

17. Modifications. The Provider may modify these Resident Terms from time to time. We will post the updated version and update the "last updated" date. Continued use of the Platform after changes are made constitutes acceptance of the revised terms.

18. Contact Information. For questions about these Resident Terms or for accessibility support, please contact: support@livwith.com

Exhibit E. Data Processing Addendum

Scope. This Data Processing Addendum ("DPA") forms part of the Unify LIV SaaS Agreement (the "Agreement") and governs Unify's Processing of Personal Information on behalf of the Customer in connection with the Services. It applies to Customers located in both Canada and the United States. Any jurisdiction-specific data-protection requirements for a particular Customer are addressed in the applicable Order Form or Client Rider, not in this DPA. Capitalized terms not defined here have the meanings in the Agreement.

1. Definitions

1.1 "Personal Information" means information processed through the Services that identifies or is reasonably linkable to an individual, including residents, owners, tenants, staff, vendors, and board/council members.

1.2 "Processing" means any operation performed on Personal Information, such as collection, storage, use, transmission, disclosure, or deletion.

1.3 "Controller / Business / Data Owner" means the party that determines the purposes and means of Processing. "Processor / Service Provider / Vendor" means the party that Processes Personal Information on behalf of the Controller. "Subprocessor" means a third party engaged by Unify to Process Personal Information.

1.4 "Data Protection Laws" means all privacy, data-protection, data-security, and breach-notification laws applicable to a Party's Processing of Personal Information under this DPA, including, in Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) and substantially similar provincial laws (such as those of British Columbia, Alberta, and Quebec); and, in the United States, applicable federal laws and state consumer-privacy and data-breach-notification laws (such as the California Consumer Privacy Act, as amended by the California Privacy Rights Act (CCPA/CPRA), and comparable consumer-privacy statutes of other U.S. states), in each case to the extent applicable to the Customer and the Personal Information Processed under the Agreement.

1.5 "Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information processed by Unify.

2. Roles of the Parties

2.1 Allocation. As between the Parties, the Customer is the Controller / Business / Data Owner and Unify is the Processor / Service Provider / Vendor with respect to Personal Information Processed to provide the Services. Each Party complies with its own obligations under applicable Data Protection Laws.

2.2 Processor / Service-Provider Restrictions. To the extent applicable under Data Protection Laws (including U.S. state privacy laws such as the CCPA/CPRA), Unify will not: (a) sell or share Personal Information; (b) retain, use, or disclose Personal Information for any purpose other than performing the Services or as permitted by applicable Data Protection Laws; (c) retain, use, or disclose Personal Information outside the direct business relationship; or (d) combine Personal Information with data from other sources except as permitted for a processor or service provider. Unify certifies that it understands and will comply with these restrictions.

2.3 Customer Responsibilities. The Customer is responsible for the accuracy and lawfulness of Personal Information it provides, for providing required notices to and obtaining required consents from individuals, and for the lawfulness of its instructions.

3. Processing Instructions and Purpose

3.1 Documented Instructions. Unify Processes Personal Information only on the Customer's documented instructions, which include the Agreement, the applicable Order, configuration of the Services by the Customer, and this DPA, unless required by law (in which case Unify will, where legally permitted, inform the Customer).

3.2 Nature and Purpose. The subject matter is the provision of the resident-experience and property-operations Services. Processing includes hosting, storage, transmission, display, support, backup, and related operations. Categories of data subjects and Personal Information are described in Schedule 1.

4. Confidentiality

4.1 Unify ensures that personnel authorized to Process Personal Information are bound by appropriate confidentiality obligations and receive appropriate training, and limits access on a need-to-know basis through role-based access controls.

5. Security Safeguards

5.1 Technical and Organizational Measures. Unify maintains administrative, technical, and physical safeguards designed to protect Personal Information appropriate to the risk, including: encryption of data in transit and at rest (TLS 1.2+ and AES-256 or comparable); role-based access controls; multi-factor authentication for administrative access; audit logging and activity monitoring; secure software development and API authentication (e.g., OAuth 2.0); vulnerability scanning and periodic penetration testing; and network and infrastructure protections.

5.2 Hosting. The Services are hosted on commercially reasonable cloud infrastructure (currently Google Cloud Platform). Where offered, the Customer may elect a data-residency region (United States or Canada) in the Order Form; absent an election, the Provider's default region for the Customer's market applies.

5.3 Continuous Improvement. Unify may update its safeguards provided the updates do not materially diminish the overall level of protection.

5.4 AI and Machine Learning Processing. Unify will not use Customer Personal Information to train, fine-tune, or improve generally available, shared, or third-party machine learning, artificial intelligence, or generative AI models. Any AI or machine learning functionality provided as part of the Services will process Customer Personal Information solely for the purpose of providing the Services and in accordance with the Customer's documented instructions.

Unify may use aggregated and de-identified information that no longer constitutes Personal Information under Data Protection Laws to operate, maintain, support, secure, analyze, and improve the Services,

provided that Unify implements reasonable measures designed to prevent re-identification and does not attempt to re-identify such information.

AI-generated outputs derived from Customer Personal Information will be made available only to the Customer and its Authorized Users, except as otherwise required by law or expressly authorized by the Customer.

6. Subprocessors

6.1 Authorization. The Customer provides general authorization for Unify to engage Subprocessors to provide the Services, including cloud hosting (Google Cloud Platform), payment processing (e.g., Stripe), and communications providers (e.g., SMS and email delivery), and AI and machine-learning providers (used for parcel-label recognition, ticket summarization, and similar Service features). A current list is available on request.

6.2 Flow-Down and Liability. Unify imposes data-protection obligations on each Subprocessor that are no less protective than this DPA in all material respects, and remains responsible for each Subprocessor's performance.

6.3 Changes. Unify will provide a mechanism to notify the Customer of intended additions or replacements of Subprocessors that Process Personal Information and will allow the Customer a reasonable period to object on reasonable data-protection grounds; if the Parties cannot resolve the objection, the Customer may terminate the affected Services.

7. Assistance to the Customer

7.1 Data-Subject / Consumer Requests. Taking into account the nature of the Processing, Unify will provide reasonable assistance (including appropriate technical and organizational measures and self-service functionality) to help the Customer respond to verifiable requests from individuals to access, correct, delete, or limit their Personal Information under applicable Data Protection Laws. If Unify receives such a request directly, it will, where permitted, direct the individual to the Customer.

7.2 Assessments. Unify will provide information reasonably necessary to assist the Customer with data-protection assessments and consultations required by applicable Data Protection Laws, to the extent the Customer does not otherwise have access to the information.

8. Security Incident Notification

8.1 Notice to Customer. Unify will notify the Customer without undue delay, and in any event within seventy-two (72) hours, after confirming a Security Incident involving Personal Information Processed for the Customer.

8.2 Contents. To the extent known, the notice will describe the nature of the incident, the categories and approximate number of individuals and records affected, the likely consequences, and the measures taken or proposed to address it. Unify will provide updates as more information becomes available.

8.3 Cooperation. Unify will reasonably cooperate with the Customer in investigating and mitigating the incident and in fulfilling the Customer's notification obligations to individuals and regulators under

applicable Data Protection Laws. Any jurisdiction-specific breach-cooperation requirements for a particular Customer are addressed in the applicable Client Rider.

8.4 Allocation. As between the Parties, the Customer (as Controller / Business) is responsible for determining whether notification is required under applicable Data Protection Laws and for making notifications, except where the incident was caused by Unify's breach of this DPA, in which case the Parties will reasonably cooperate on the allocation of reasonable notification costs. Unify's notice is not an acknowledgment of fault or liability.

9. Audits

9.1 Reports First. Unify will make available information necessary to demonstrate compliance with this DPA, including, where available, third-party audit reports or certifications and a summary of its security practices.

9.2 On-Site Audits. Where reports are insufficient to demonstrate compliance, the Customer may, on reasonable prior notice and no more than once per twelve-month period (absent a confirmed Security Incident or regulatory requirement), conduct an audit of Unify's relevant controls during normal business hours, subject to confidentiality and without unreasonably disrupting Unify's operations.

10. International / Cross-Border and Data Residency

10.1 Unify Processes and stores Personal Information in the data-residency region elected in the Order Form (United States or Canada, where offered). If no election is made, the Provider's default region for the Customer's market applies. Where Personal Information is transferred across borders (including between Canada and the United States), Unify will perform the transfer consistent with applicable Data Protection Laws and maintain contractual and technical safeguards providing a comparable level of protection; for Canadian Customers, Unify remains accountable for Personal Information transferred to a Subprocessor for Processing.

10.2 Where Personal Information is transferred between Canada and the United States in the course of providing the Services, Unify implements appropriate safeguards consistent with PIPEDA's accountability principle and applicable U.S. state laws, including contractual protections with Subprocessors, encryption in transit and at rest, and access controls. The data-residency election in the Order Form determines the primary processing location.

11. Return and Deletion

11.1 On termination or expiration of the Agreement, Unify will, at the Customer's election during the Termination Assistance Period (Agreement §5.6), make Customer Personal Information available for export and will delete or anonymize Personal Information within sixty (60) days, except for routine backup/archival copies that are overwritten in the ordinary course (and remain protected under this DPA until deleted) or where retention is required by law.

11.2 Retention During the Term. During the Term, Personal Information is retained as configured by the Customer or as necessary to provide the Services. The Customer is responsible for configuring retention settings consistent with its own retention obligations under Data Protection Laws.

12. Sensitive Information

The Services are not intended for the collection of special categories of sensitive Personal Information beyond what the Customer chooses to configure. The Customer is responsible for not submitting, and for not configuring the Services to collect, sensitive Personal Information (such as government identifiers, financial-account numbers beyond what the Payment Processor handles, precise health information, or biometric data) unless expressly agreed in the Order and supported by appropriate safeguards. To the extent the Customer enables features that process geolocation or other potentially sensitive data, the Customer is responsible for the required notices and consents.

13. Liability

Each Party's liability under this DPA is subject to the limitations and exclusions in the Agreement, including the Super-Cap for Certain Claims in the Agreement §13.3 and the Excluded Claims in §13.4.

14. Conflict and Term

In case of conflict between this DPA and the body of the Agreement regarding the Processing of Personal Information, this DPA controls. This DPA terminates automatically with the Agreement, but obligations relating to confidentiality, security, and deletion survive until all Personal Information is returned or deleted.

Schedule 1 — Details of Processing

Item	Description
Subject matter	Provision of the Unify LIV resident-experience and property-operations Services.
Duration	The term of the Agreement plus the deletion period in section 11.
Nature & purpose	Hosting, storage, transmission, display, support, backup, analytics, and related operations to deliver the Services.
Categories of data subjects	Residents, unit owners, tenants, applicants, guests/visitors, board/council members, property managers and staff, concierge/front-desk, and vendors.
Categories of Personal Information	Name, contact details (email, phone, mailing address), unit/building association, account credentials, communications, booking and parcel records, parking/visitor data, violation/charge records, payment-related identifiers handled via the Payment Processor, device/usage data, and (where enabled) geolocation.
Sensitive data	Not intended; only as expressly agreed in the Order (see section 12).
Subprocessors (categories)	Cloud hosting (Google Cloud Platform); payment processing (e.g., Stripe); SMS/email delivery; support tooling.