

● API TERMS OF USE

Last Revised: July 2026

Momence, Inc.

IMPORTANT: These API Terms of Use are a publication-ready legal draft subject to confirmation of the governing Momence customer agreement, legal notice address, governing law, venue, support contact, API fee structure, and any product-specific API documentation.

Thank you for using the Momence application programming interfaces, software development kits, webhooks, developer tools, sandbox environments, sample code, technical materials, and related services made available by Momence (collectively, the “Momence APIs”). By requesting credentials for, accessing, or using any Momence API, you agree to these API Terms of Use (the “API Terms”).

These API Terms supplement and form part of the agreement governing your access to the Momence platform or services, including the applicable Momence subscription agreement, order form, terms of service, data processing addendum, payment terms, privacy policy, and any other written agreement between you and Momence (collectively, the “Momence Agreement”). If there is a conflict between these API Terms and the Momence Agreement, the Momence Agreement controls, except that these API Terms control with respect to your technical access to and use of the Momence APIs unless the parties expressly agree otherwise in writing.

If you access or use the Momence APIs on behalf of an entity, you represent and warrant that you have authority to bind that entity. “You” and “your” refer to that entity and its authorized personnel. “Momence,” “we,” “us,” and “our” mean Momence, Inc. and its applicable affiliates.

1. ELIGIBILITY, REGISTRATION, AND AUTHORIZED USE

1.1 Eligibility and Authority.

You may use the Momence APIs only if you are legally capable of entering into a binding contract, are not prohibited from receiving the Momence APIs under applicable law, and have a valid Momence account or other written authorization from Momence. You may not use the Momence APIs on behalf of a competitor of Momence, to develop or enhance a competing platform, or for competitive intelligence, benchmarking, or monitoring, except with Momence’s prior written consent.

1.2 Registration Information.

You must provide complete and accurate registration, business, technical, and contact information and keep it current. Momence may require identity, security, use-case, or compliance verification before issuing or maintaining API credentials.

1.3 Permitted Purpose.

Subject to these API Terms, Momence grants you a limited, non-exclusive, revocable, non-transferable, non-sublicensable right during the term to access and use the Momence APIs solely to develop, operate, and support an integration, application, website, device, or service approved by Momence (your “Integration”) for your internal business purposes or to provide approved functionality to a Momence subscriber that has authorized your access (each, a “Subscriber”). No rights are granted by implication.

1.4 Subscriber Authorization.

You may access a Subscriber’s account or Subscriber Data only after obtaining the Subscriber’s valid, informed, and current authorization and only within the scope of that authorization. You must maintain

auditable records of such authorization and promptly cease access when authorization expires, is revoked, or is no longer reasonably necessary.

2. API CREDENTIALS AND ACCESS CONTROLS

2.1 Credentials.

API keys, secrets, tokens, client identifiers, certificates, credentials, and other authentication materials (“API Credentials”) are confidential and may be used only for the approved Integration and environment for which they were issued. You may not sell, transfer, publish, disclose, embed in client-side code, commit to a public repository, or otherwise make API Credentials available to any unauthorized person.

2.2 Security of Credentials.

You must protect API Credentials using industry-standard safeguards, including secure secrets management, least-privilege access, role-based controls, multi-factor authentication where available, encryption, logging, and periodic rotation. You are responsible for all activity occurring through your API Credentials, whether authorized by you or not, except to the extent caused solely by Momence’s breach of its obligations.

2.3 Compromise and Revocation.

You must notify Momence immediately upon discovering or reasonably suspecting any loss, disclosure, compromise, misuse, or unauthorized use of API Credentials. Momence may revoke, rotate, suspend, or replace API Credentials at any time for security, legal, operational, or compliance reasons. You must promptly implement any replacement credentials or authentication changes required by Momence.

2.4 Service Providers.

You may permit a contractor or service provider to access the Momence APIs solely on your behalf and only if: (a) the access is necessary for the approved Integration; (b) the service provider is bound by written obligations at least as protective as these API Terms; (c) access is limited to the minimum necessary; and (d) you remain fully responsible for its acts and omissions. You may not provide API access to enable an unaffiliated third party to bypass a Momence partner, integration, commercial, or certification program.

3. API DOCUMENTATION, LIMITS, AND CHANGES

3.1 Documentation.

You must access and use the Momence APIs only as described in Momence’s then-current technical documentation, specifications, implementation guidance, security requirements, and written instructions (collectively, the “API Documentation”).

3.2 Usage Limits.

Momence may establish and enforce technical or commercial limits, including rate limits, concurrency limits, quotas, data-volume limits, pagination requirements, polling restrictions, environment restrictions, and limits on the number of Subscribers or end users served. You may not circumvent or attempt to circumvent any limit. Momence may throttle or suspend excessive, abusive, inefficient, or destabilizing usage.

3.3 Modifications and Deprecation.

Momence may modify, update, replace, or discontinue any Momence API, endpoint, field, data model, authentication method, or functionality. Where commercially reasonable, Momence will provide advance notice of material breaking changes or deprecations through the API Documentation, developer communications, or other designated channel. You are responsible for maintaining compatibility and migrating from deprecated or legacy APIs within the announced period.

3.4 Sandbox and Test Data.

Any sandbox, test environment, sample data, or beta functionality is provided for testing only. You may not submit live Personal Data, payment credentials, protected health information, or other production data to a sandbox unless Momence expressly authorizes that use in writing and appropriate safeguards are in place.

3.5 Support and Certification.

Momence may require technical review, security review, testing, certification, re-certification, or demonstration of your Integration before or after production access. Any support, consultation, sample code, or implementation assistance is provided at Momence's discretion and may be subject to additional fees or terms.

4. YOUR INTEGRATION AND END USERS

4.1 Responsibility for Your Integration.

You are solely responsible for your Integration, including its design, development, hosting, operation, maintenance, security, availability, user support, accessibility, legal compliance, and all representations made about it. You must ensure that your Integration does not create confusion regarding whether it is offered, operated, sponsored, or endorsed by Momence.

4.2 End-User Terms and Privacy Notice.

Before collecting information from or providing services to any individual through your Integration, you must provide legally sufficient terms and a clear, accurate, and conspicuous privacy notice describing your identity, data practices, purposes, disclosures, retention, and available rights. Your terms must prohibit unlawful use and must not conflict with these API Terms or the applicable Subscriber's agreements with its customers or members ("End Users").

4.3 Consent and Choice.

You must obtain, document, and honor all consents, authorizations, permissions, opt-ins, and opt-outs required for your Integration and its data uses. You may not condition access to unrelated functionality on consent that is not freely given or otherwise valid under applicable law. You must promptly transmit to the Subscriber or Momence, as applicable, any withdrawal of consent, suppression request, communication preference, or privacy request that affects data processed in the Momence platform.

4.4 No Misrepresentation.

You may not misrepresent your identity, your relationship with Momence or a Subscriber, the source or accuracy of data, your Integration's capabilities, or the purpose for which data will be used. You may not use dark patterns, deceptive interfaces, or misleading prompts to obtain authorization or consent.

5. DATA RIGHTS, USE, AND RESTRICTIONS

5.1 Definitions.

"Subscriber Data" means data, content, records, files, communications, media, and information submitted to, stored in, generated through, or retrieved from a Subscriber's Momence account, including information relating to End Users, staff, bookings, memberships, appointments, classes, leads, communications, transactions, attendance, access events, forms, notes, inventory, content, and reports. "Personal Data" means information relating to an identified or identifiable individual or otherwise regulated as personal information under applicable law. "API Data" means Subscriber Data and any other data or content made available through the Momence APIs.

5.2 Limited Use.

You may collect, access, use, retain, disclose, and otherwise process API Data only: (a) as necessary to provide the approved Integration to the authorizing Subscriber; (b) within the scope of the Subscriber's authorization; (c) for the purposes clearly disclosed to the Subscriber and applicable End Users; and (d) in compliance with the Momence Agreement, API Documentation, and applicable law.

5.3 Prohibited Data Uses.

Unless Momence and the applicable Subscriber expressly authorize the use in writing and applicable law permits it, you may not:

- sell, rent, license, broker, monetize, or otherwise commercialize API Data;
- use API Data for targeted advertising, cross-context behavioral advertising, data enrichment, identity resolution, profiling, credit, insurance, employment, housing, eligibility, or similar consequential decisions;
- combine API Data with data obtained from another source to create profiles unrelated to the approved Integration;
- use API Data to train, fine-tune, validate, benchmark, or improve any general-purpose or third-party artificial intelligence or machine-learning model;
- re-identify de-identified, anonymized, aggregated, or pseudonymized data;
- scrape, harvest, bulk-download, mirror, replicate, or create a substitute database of API Data, except for limited caching or storage necessary to operate the approved Integration;
- use API Data to contact, solicit, market to, or transact with an End User except on behalf of and as authorized by the applicable Subscriber; or
- retain API Data longer than necessary for the approved purpose or applicable legal obligations.

5.4 Data Accuracy and Integrity.

You must take reasonable steps to preserve the accuracy, context, provenance, and integrity of API Data. You may not alter API Data in a misleading manner or overwrite authoritative records in the Momence platform without the Subscriber's authorization. Where your Integration writes data to Momence, you must implement appropriate validation, reconciliation, duplicate prevention, and error-handling controls.

5.5 Deletion and Portability.

Upon request by Momence or the applicable Subscriber, revocation of authorization, termination of access, or completion of the approved purpose, you must promptly stop processing and securely delete API Data in your possession or control, except to the extent retention is required by law. Upon request, you must certify deletion in writing. Any retained data remains subject to these API Terms and must be isolated from active use.

6. PRIVACY, COMMUNICATIONS, AND REGULATED DATA

6.1 Privacy Compliance.

You must comply with all applicable privacy, data protection, consumer protection, electronic communications, marketing, recording, biometric, children's privacy, and data-breach laws, including, as applicable, the GDPR, UK GDPR, ePrivacy rules, CCPA/CPRA, and other U.S. state privacy laws. Where you process Personal Data on behalf of a Subscriber, you will act only on the Subscriber's documented instructions and will not retain, use, sell, share, or disclose the Personal Data outside the direct business relationship except as permitted by law and the applicable written agreement.

6.2 Data Subject and Consumer Requests.

You must maintain procedures to receive, authenticate, and timely assist with requests to access, know, correct, delete, restrict, port, or opt out of processing. If you receive a request relating to API Data controlled

by a Subscriber or Momence, you must notify the applicable party promptly and no later than five (5) business days after receipt, unless a shorter period is required by law, and reasonably assist with the response.

6.3 Marketing and Communications.

If your Integration sends or facilitates SMS, MMS, telephone calls, emails, push notifications, direct messages, or other communications, you are responsible for compliance with all applicable requirements, including the TCPA, CAN-SPAM Act, Telemarketing Sales Rule, Do Not Call rules, carrier requirements, platform policies, quiet-hour restrictions, identification and disclosure rules, and consent and opt-out obligations. You must maintain reliable records of consent and promptly honor STOP, unsubscribe, suppression, and revocation requests across all relevant systems.

6.4 Sensitive Data.

You may access or process sensitive Personal Data, including government identifiers, precise geolocation, financial information, biometric information, information about minors, or health-related information, only if expressly necessary for the approved Integration, authorized by the Subscriber, permitted by the API Documentation, and supported by legally sufficient notice, consent, and security controls.

6.5 Health Information and HIPAA.

Momence offers features that may permit Subscribers to store intake information, SOAP notes, or other health-related data. Unless Momence has expressly agreed in writing to act as a “business associate” and the parties have executed a business associate agreement applicable to the relevant services, you may not use the Momence APIs to create, receive, maintain, transmit, or otherwise process “protected health information” subject to HIPAA. You are solely responsible for determining whether HIPAA or another health-data law applies to your Integration and for implementing all required agreements and safeguards.

6.6 Children and Minors.

You may process Personal Data relating to children or minors only when authorized by the Subscriber and permitted by law. You must obtain verifiable parental or guardian consent where required and must not use such data for targeted advertising, profiling, or purposes unrelated to the approved Integration.

7. PAYMENT AND FINANCIAL DATA

7.1 Payment Functionality.

Momence may facilitate online and in-person payments, stored payment methods, payment plans, card payments, and direct debit transactions. Your use of payment-related APIs may be subject to separate payment terms, processor or financial-institution rules, card-brand rules, network operating regulations, and additional technical requirements. Those terms control in the event of a conflict concerning payment services.

7.2 PCI DSS and Credentials.

You must comply with the Payment Card Industry Data Security Standard (“PCI DSS”) to the extent applicable. You may not request, access, store, log, transmit, or expose full magnetic-stripe data, card verification codes, PINs, unencrypted primary account numbers, bank-account credentials, or other restricted payment authentication data through the Momence APIs unless expressly supported by the API Documentation and authorized in writing by Momence. You must use approved tokens, hosted fields, or processor-controlled payment interfaces where provided.

7.3 No Payment Intermediation.

Unless expressly authorized under a separate written agreement, you may not use the Momence APIs to act as a payment facilitator, money transmitter, merchant of record, payment intermediary, collection agent, or

reseller of payment services, or to redirect, route, surcharge, split, settle, or otherwise manipulate payment transactions.

7.4 Financial Advice and Records.

API Data, including reports relating to sales, earned revenue, payroll, taxes, or transactions, is informational and may not constitute an authoritative accounting, tax, payroll, or financial record. You are responsible for independent validation, reconciliation, and compliance with recordkeeping obligations.

8. ARTIFICIAL INTELLIGENCE AND AUTOMATED FUNCTIONALITY

8.1 AI-Enabled Features.

If your Integration accesses, invokes, displays, or interacts with Momence AI-enabled features, you must comply with any applicable AI-specific terms and documentation. You must provide appropriate notice when End Users interact with automated systems and must not represent machine-generated output as human-generated where that representation would be misleading.

8.2 Human Review and High-Risk Uses.

You are responsible for evaluating AI-generated or automated output before relying on it. You may not use the Momence APIs or API Data to make solely automated decisions that produce legal or similarly significant effects, or for medical diagnosis, treatment, emergency response, safety-critical decisions, or other high-risk purposes, unless expressly authorized by Momence and supported by legally required safeguards and human review.

8.3 Inputs and Outputs.

You must not submit confidential information, sensitive Personal Data, payment credentials, protected health information, or third-party content to an AI feature unless the feature is expressly designed and approved for that data. You are responsible for the legality, accuracy, and appropriateness of prompts, inputs, instructions, and resulting actions generated by your Integration.

9. SECURITY REQUIREMENTS

9.1 Security Program.

You must maintain a documented information-security program appropriate to the nature, scope, context, and risk of your processing. At a minimum, your safeguards must include:

- encryption of Personal Data and API Data in transit and at rest using current industry standards;
- least-privilege access, unique user accounts, strong authentication, and periodic access reviews;
- secure software-development practices, code review, dependency management, and vulnerability remediation;
- logging and monitoring sufficient to detect unauthorized access, anomalous activity, and data exfiltration;
- regular risk assessments, vulnerability scanning, penetration testing appropriate to risk, and timely remediation;
- secure backup, business-continuity, and incident-response procedures; and
- appropriate personnel training and written confidentiality obligations.

9.2 Security Incidents.

You must notify Momence without undue delay, and in no event later than twenty-four (24) hours after discovery, of any actual or reasonably suspected unauthorized access to, acquisition, use, disclosure, alteration, loss, destruction, or unavailability of API Credentials, the Momence APIs, API Data, or systems used for your Integration (a "Security Incident"). Your notice must include known facts, affected data and

systems, containment measures, and a contact for coordination. You must promptly investigate, mitigate, remediate, preserve evidence, provide updates, and cooperate with Momence. You may not notify any regulator, End User, media outlet, or other third party in a manner that identifies Momence without prior consultation, except where prohibited by law.

9.3 Security Assessments.

Upon reasonable request, you must provide information sufficient to demonstrate compliance, which may include security questionnaires, policies, architecture summaries, penetration-test executive summaries, certifications, or independent audit reports. Momence may require remediation of identified risks as a condition of continued access.

9.4 Vulnerability Testing.

You may not perform vulnerability scanning, penetration testing, load testing, denial-of-service testing, or other security testing against Momence systems without prior written authorization. Suspected vulnerabilities must be reported through Momence's designated security channel and must not be publicly disclosed until Momence has had a reasonable opportunity to investigate and remediate.

10. PROHIBITED CONDUCT

You will not, and will not permit any person to:

- use the Momence APIs in violation of law, third-party rights, the Momence Agreement, or the API Documentation;
- reverse engineer, decompile, disassemble, decode, translate, or attempt to derive source code, non-public algorithms, underlying structure, or proprietary data formats, except to the limited extent such restriction is prohibited by law;
- copy, modify, create derivative works from, distribute, sublicense, sell, lease, provide service-bureau access to, or otherwise commercially exploit the Momence APIs;
- create or offer an API, data feed, platform, or service that substantially replicates or substitutes for the Momence APIs or Momence platform;
- interfere with, disrupt, overload, damage, probe, or gain unauthorized access to the Momence APIs, platform, accounts, servers, or networks;
- introduce malware, malicious code, hidden functionality, or mechanisms designed to disable, circumvent, or impair security controls;
- use automated means to access endpoints or data not expressly made available through the Momence APIs;
- remove, obscure, or alter proprietary notices, attribution, privacy choices, consent mechanisms, or security warnings;
- use API Data or the Momence APIs for unlawful surveillance, discrimination, harassment, fraud, spam, scraping, credential stuffing, or abusive activity;
- access the Momence APIs for benchmarking, publication of performance results, or competitive analysis without Momence's written approval; or
- permit access from a prohibited jurisdiction or by a sanctioned or restricted person.

11. CONTENT AND INTELLECTUAL PROPERTY

11.1 Momence Materials.

Momence and its licensors retain all right, title, and interest in and to the Momence APIs, API Documentation, platform, software, data models, schemas, formats, methods, technology, improvements, and related intellectual property ("Momence Materials"). These API Terms do not transfer ownership of any Momence Materials or Subscriber Data to you.

11.2 Your Integration.

As between the parties, you retain ownership of your Integration, excluding Momence Materials and API Data. You grant Momence a non-exclusive, worldwide, royalty-free license to access, use, reproduce, and test your Integration solely as reasonably necessary to provide, secure, support, evaluate, and enforce the Momence APIs and these API Terms.

11.3 Submitted Content.

To the extent you submit content, data, instructions, or materials through the Momence APIs, you represent and warrant that you have all rights and permissions necessary for Momence to process them to provide and improve the applicable services in accordance with the Momence Agreement and applicable privacy terms.

11.4 Feedback.

If you provide suggestions, ideas, enhancement requests, or other feedback regarding the Momence APIs, Momence may use and exploit that feedback without restriction or obligation. You assign to Momence all right, title, and interest in such feedback to the extent necessary to give effect to this provision.

11.5 Open-Source Software.

Open-source components may be subject to separate license terms. To the extent an applicable open-source license expressly conflicts with these API Terms for a specific component, that license controls solely for that component.

12. BRAND FEATURES, ATTRIBUTION, AND PUBLICITY

12.1 Brand Features.

Each party retains ownership of its names, trademarks, service marks, logos, and other brand identifiers (“Brand Features”). Except for a limited right expressly granted in the API Documentation or in writing, neither party may use the other party’s Brand Features.

12.2 Attribution.

You must display any attribution, notices, links, or branding required by the API Documentation and may not remove or obscure them. Any use of Momence Brand Features must comply with Momence’s then-current brand guidelines and inure solely to Momence’s benefit.

12.3 Public Statements.

You may not issue a press release or make a public statement suggesting sponsorship, certification, endorsement, partnership, or exclusivity with Momence without Momence’s prior written approval. Momence may identify your Integration as using or integrating with Momence, subject to any separate written confidentiality or publicity restrictions.

13. FEES AND TAXES

13.1 Fees.

Access to or use of the Momence APIs may be subject to fees, minimum commitments, overage charges, support fees, certification fees, or other charges specified in the Momence Agreement, an order form, the API Documentation, or a separate written notice. Momence may introduce or change API fees upon the notice required by the applicable Momence Agreement or, if no notice period applies, upon at least thirty (30) days’ notice.

13.2 Taxes.

Fees are exclusive of applicable taxes, duties, levies, and assessments. You are responsible for all such amounts, excluding taxes based on Momence’s net income, unless a valid exemption applies.

14. MONITORING, AUDIT, AND ENFORCEMENT

14.1 Monitoring.

Momence may monitor and log use of the Momence APIs to operate and secure the services, enforce limits, investigate misuse, verify compliance, improve performance, and protect Momence, Subscribers, and End Users. You will not interfere with such monitoring.

14.2 Audit and Cooperation.

Upon reasonable request, you must provide records and information demonstrating compliance, including evidence of Subscriber authorization, consents, data flows, retention practices, subprocessors, security controls, and deletion. If Momence reasonably believes a material violation or Security Incident has occurred, Momence may conduct or require a focused audit, subject to reasonable confidentiality protections.

14.3 Remediation.

You must promptly correct any noncompliance identified by Momence. Momence may impose additional controls, reduce permissions, require re-certification, rotate credentials, throttle traffic, disable features, or suspend access where reasonably necessary to address risk.

15. SUSPENSION AND TERMINATION

15.1 Suspension.

Momence may immediately suspend or restrict access to any Momence API if Momence reasonably believes that: (a) your use violates these API Terms, the Momence Agreement, law, or third-party rights; (b) your use threatens the security, integrity, availability, or performance of Momence systems or data; (c) a Security Incident has occurred or is likely; (d) your access is unauthorized or no longer supported by Subscriber authorization; (e) fees are overdue; or (f) suspension is required by a regulator, financial institution, network, service provider, or law.

15.2 Termination by You.

You may stop using the Momence APIs at any time, subject to any notice, minimum term, payment, and termination obligations in the Momence Agreement.

15.3 Termination by Momence.

Momence may terminate these API Terms or discontinue access to any Momence API in accordance with the Momence Agreement or, if the Momence Agreement does not address termination, upon notice. Momence may terminate immediately for material breach, security risk, unlawful use, insolvency, repeated violations, or conduct that exposes Momence, a Subscriber, or an End User to material risk or liability.

15.4 Effect of Termination.

Upon suspension, termination, expiration, or revocation of authorization, you must immediately cease the affected access and use, stop representing that your Integration is connected to Momence, remove Momence Brand Features, disable affected functionality, and delete API Data as required by Section 5.5. Sections that by their nature should survive will survive, including restrictions, confidentiality, data protection, intellectual property, disclaimers, limitations of liability, indemnification, and general provisions.

15.5 Subscriber Communications.

Momence may communicate directly with any affected Subscriber concerning suspension, termination, security, migration, continuity, or protection of Subscriber Data and End Users.

16. CONFIDENTIALITY

16.1 Confidential Information.

Non-public API Documentation, API Credentials, product roadmaps, security information, communications, pricing, technical materials, and other information disclosed by Momence that is marked confidential or reasonably should be understood as confidential are “Momence Confidential Information.” You will use Momence Confidential Information only to exercise authorized rights under these API Terms and will protect it using at least reasonable care.

16.2 Exclusions and Required Disclosure.

Confidential Information does not include information that you can document: (a) is publicly available through no breach; (b) was lawfully known without restriction; (c) was independently developed without use of the Confidential Information; or (d) was lawfully received from a third party without duty of confidentiality. You may disclose Confidential Information when legally compelled, provided you give prompt notice where permitted and reasonably cooperate in seeking protective treatment.

17. DISCLAIMERS

TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE MOMENCE APIs, API DOCUMENTATION, SAMPLE CODE, SANDBOXES, BETA FEATURES, DATA, AND RELATED MATERIALS ARE PROVIDED “AS IS” AND “AS AVAILABLE.” MOMENCE AND ITS AFFILIATES, LICENSORS, SUPPLIERS, AND SERVICE PROVIDERS DISCLAIM ALL EXPRESS, IMPLIED, STATUTORY, AND OTHER WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, ACCURACY, COMPLETENESS, SECURITY, QUIET ENJOYMENT, AND WARRANTIES ARISING FROM COURSE OF DEALING OR USAGE OF TRADE. MOMENCE DOES NOT WARRANT THAT THE MOMENCE APIs WILL BE UNINTERRUPTED, ERROR-FREE, SECURE, COMPATIBLE WITH YOUR INTEGRATION, OR AVAILABLE IN ANY LOCATION, OR THAT API DATA OR OUTPUT WILL BE ACCURATE, COMPLETE, OR SUITABLE FOR ANY PARTICULAR PURPOSE.

18. LIMITATION OF LIABILITY

TO THE MAXIMUM EXTENT PERMITTED BY LAW, MOMENCE AND ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, LICENSORS, SUPPLIERS, AND SERVICE PROVIDERS WILL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY, ENHANCED, OR PUNITIVE DAMAGES, OR FOR ANY LOSS OF PROFITS, REVENUE, BUSINESS, GOODWILL, USE, OR DATA, BUSINESS INTERRUPTION, COST OF SUBSTITUTE SERVICES, OR SECURITY OR DATA-RECOVERY COSTS, ARISING OUT OF OR RELATING TO THE MOMENCE APIs OR THESE API TERMS, REGARDLESS OF THE THEORY OF LIABILITY AND EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE AGGREGATE LIABILITY OF MOMENCE AND THE OTHER MOMENCE PARTIES ARISING OUT OF OR RELATING TO THE MOMENCE APIs OR THESE API TERMS WILL NOT EXCEED THE GREATER OF: (A) THE FEES PAID OR PAYABLE BY YOU SPECIFICALLY FOR USE OF THE MOMENCE APIs DURING THE THREE (3) MONTHS BEFORE THE EVENT GIVING RISE TO LIABILITY; OR (B) FIVE HUNDRED U.S. DOLLARS (US \$500). THE FOREGOING LIMITATIONS APPLY EVEN IF A REMEDY FAILS OF ITS ESSENTIAL PURPOSE. NOTHING IN THESE API TERMS EXCLUDES LIABILITY THAT CANNOT BE EXCLUDED BY LAW.

19. INDEMNIFICATION

You will defend, indemnify, and hold harmless Momence and its affiliates, officers, directors, employees, agents, licensors, suppliers, service providers, Subscribers, and partners from and against all third-party claims, demands, actions, investigations, liabilities, damages, judgments, settlements, penalties, fines, losses,

costs, and expenses, including reasonable attorneys' fees, arising out of or relating to: (a) your Integration or your use of the Momence APIs; (b) your breach of these API Terms or the Momence Agreement; (c) your or your service providers' violation of law or third-party rights; (d) data, content, instructions, or communications submitted, processed, or transmitted by you; (e) a Security Incident involving systems under your control; (f) your failure to obtain or honor required authorization or consent; or (g) claims that your Integration infringes, misappropriates, or violates third-party rights. Momence may assume control of the defense of any matter subject to indemnification, and you will cooperate. You may not settle any claim in a manner that admits fault by, imposes obligations on, or restricts Momence without Momence's prior written consent.

20. EXPORT, SANCTIONS, AND ANTI-CORRUPTION

You must comply with all applicable export-control, import, sanctions, and anti-boycott laws. You represent that you are not located in, organized under the laws of, or ordinarily resident in a comprehensively sanctioned jurisdiction and are not a restricted or blocked person. You may not use the Momence APIs for prohibited end uses or provide access to prohibited persons. You must comply with applicable anti-bribery and anti-corruption laws and may not offer anything of value to improperly influence any person in connection with the Momence APIs.

21. GENERAL PROVISIONS

21.1 Relationship of the Parties.

The parties are independent contractors. These API Terms do not create a partnership, franchise, joint venture, agency, fiduciary, employment, or exclusive relationship. Neither party may bind the other.

21.2 Assignment.

You may not assign, delegate, or transfer these API Terms or any rights or obligations, whether by operation of law, merger, change of control, or otherwise, without Momence's prior written consent. Momence may assign these API Terms to an affiliate or in connection with a merger, reorganization, financing, sale of assets, or similar transaction. Any prohibited assignment is void.

21.3 Notices.

Notices will be provided in the manner specified in the Momence Agreement. If the Momence Agreement does not specify notice procedures, Momence may provide notice through your account, the API Documentation, email to your registered contact, or another reasonable electronic method. Legal notices to Momence must be sent to [LEGAL NOTICE EMAIL] and [LEGAL NOTICE ADDRESS].

21.4 Governing Law and Venue.

The governing law, dispute-resolution process, and venue specified in the Momence Agreement apply to these API Terms. If the Momence Agreement does not contain those provisions, these API Terms will be governed by the laws of [STATE/COUNTRY], excluding conflict-of-laws principles, and the state and federal courts located in [COUNTY, STATE/COUNTRY] will have exclusive jurisdiction.

21.5 Force Majeure.

Momence is not liable for delay or failure caused by events beyond its reasonable control, including natural disasters, epidemics, war, terrorism, civil unrest, labor disputes, governmental action, utility or telecommunications failures, internet or cloud-provider outages, cyberattacks, denial-of-service attacks, and failures of third-party networks or service providers.

21.6 Changes to These API Terms.

Momence may update these API Terms from time to time. Material changes will become effective on the date stated in the updated terms or after notice through a reasonable channel. Continued use after the effective date constitutes acceptance, except where applicable law or the Momence Agreement requires affirmative agreement.

21.7 Entire Agreement and Order of Precedence.

These API Terms, the Momence Agreement, the API Documentation, and any applicable written addenda constitute the complete agreement concerning the Momence APIs and supersede prior discussions or terms on that subject. Any purchase-order terms or other unilateral terms submitted by you are rejected and void unless expressly accepted in a signed writing by Momence.

21.8 Waiver; Severability.

A waiver must be in writing and signed by the waiving party. Failure to enforce a provision is not a waiver. If any provision is unenforceable, it will be modified to the minimum extent necessary to make it enforceable, and the remaining provisions will remain in effect.

21.9 No Third-Party Beneficiaries.

Except for the Momence parties entitled to indemnification and liability protections, these API Terms do not create third-party beneficiary rights.

21.10 Interpretation.

Headings are for convenience only. “Including” means “including without limitation.” References to laws include amendments and successor provisions. Electronic acceptance and electronic records have the same force as originals and signatures to the extent permitted by law.