Foodsoft AS
Gaustadalléen 21, 0349 Oslo
Norway
VAT NR: NO 918 859 810 MVA

Last updated 25.10.2025

Welcome to MyFoodOffice!

Thanks for using MyFoodOffice modules and services ("**Service**"). The Services are provided by Foodsoft AS, located at Gaustadalléen 21, 0349 Oslo, Norway ("**Provider**", "**MyFoodOffice**"). Here are our terms and conditions for using our Service.

1. Introduction and Acceptance

1.1. **Parties.** These Terms of Service (the "Terms") form a legal agreement between **Foodsoft AS ("MyFoodOffice", the "Provider")** and the **Customer**, which means **(i)** any *business or organization* that registers for or uses the Service, **or (ii)** any *individual acting in a business capacity* (including a sole trader or freelancer) who registers for or uses the Service. Capitalized terms used but not defined in this Section 1 have the meanings set out in Section 2 (Definitions).

1.2. **Acceptance.** By (i) creating or being provisioned with a Customer Account, (ii) clicking "I agree" (or similar), or (iii) accessing or using the Service, the Customer accepts these Terms and represents that the individual accepting has authority to bind the Customer. If the Customer is a business or organization, the individual accepting represents they have authority to bind that Customer. If the Customer is an individual acting as a sole trader/freelancer, the individual accepts these Terms on their own behalf. If the Customer does not agree, the Customer must not access or use the Service.

1.3. **Business Use Only.** The Service is intended for use by businesses and organizations. By creating a Customer Account, the Customer represents it is acting in a business capacity. It is not for consumers acting outside a trade, business, or profession. If you are an individual Customer, you confirm you are acting solely for business purposes and consumer-protection laws applicable to purely personal/household use do not apply.

1.4. **Affiliates and Incorporation by Reference.** The Service may be provided by the Provider and, where applicable, its affiliates. These Terms incorporate the Documentation, the Privacy Policy, the DPA (Annex A) for processing of Customer Personal Data, and any Order or SOW. In the event of conflict, the order of precedence in Interpretation and Order of Precedence applies.

1.5. **Contact.** Questions about these Terms may be sent to support@myfoodoffice.com.

1.6. **Language.** These Terms are provided in English. If translated, the English version controls unless expressly stated otherwise in the applicable Order.

1.7. **Effective Date.** These Terms take effect on the date shown on the cover page or, if none, when the Customer first accesses the Service.

2. Definitions

Provider	Foodsoft AS (MyFoodOffice).
Customer	the legal entity that owns a Customer Account and enters into the Agreement with the Provider.
Parties; Party	“Parties” means the Provider and the Customer together, and “Party” means either of them individually.
Agreement	these Terms, the DPA, any applicable Order or SOW, and the Documentation and referenced policies to the extent incorporated by reference and not in conflict with Section 3 (Order of Precedence).
Service	the MyFoodOffice cloud service, including ERP, B2B ordering, APIs, and integrations made available by the Provider.
Master Customer	means the Customer that signs the Order on its own behalf and, if applicable, on behalf of Participating Affiliates.
Participating Affiliate	means a legal entity that is expressly listed in the applicable Order as participating in a Group Order for consolidated commercial terms.
Order	*an ordering document (including an email, order form, contract, quote, proposal, or online checkout confirmation) that specifies the Customer’s offered subscription, and that is accepted by the Parties (including via electronic acceptance or signature). An Order may reference and incorporate these Terms and any statement of work.*
Group Order	means an Order that lists a Master Customer together with one or more Participating Affiliates for consolidated commercial terms
Module	functional component of the Service that can be licensed separately (for example, *Food Declaration*, *Food Labels*, *Food Costing*, *Stocktake*).
Tier	a version of a Module with a defined feature set or capacity (for example, *Standard* or *Pro*).
Scope Level	the organizational unit for which a license applies.
Statement of Work (SOW)	a document (including an email, order form, contract, quote, proposal, or online checkout confirmation) confirmed by both Parties describing Professional Services (scope, deliverables, timeline, fees, assumptions) to be performed by Provider.
Customer Account	the Customer’s dedicated tenant/instance in the Service.
Customer Admin	a user designated by the Customer with administrative rights to the Customer Account.

End User	any user authorized by the Customer to access the Customer Account.
Buyer (role)	the party that places an order or initiates an order change in a Transaction.
Seller (role)	the party that receives an order or order change and is responsible for fulfillment in a Transaction.
Ordering Account	a limited-function Customer Account created or provisioned when an invited counterparty onboards to place orders with the inviting Customer. An Ordering Account is a Customer under these Terms but has only those capabilities the inviting Customer enables.
Trading Partner	another Customer Account or external entity that sends or receives order, delivery, invoice, or related transactional data with the Customer through the Service, including via supported networks or third-party integrations, whether acting as buyer, seller, or another role in such transactions.
Transaction	a business message flow (e.g., sales catalogues, order, order change, order confirmation, delivery, despatch advice, invoice, credit note, return, claims, product data) between a Customer and a Trading Partner.
Cross-Context Behavioral Advertising	targeting an individual or device across businesses, websites, apps, or services other than the Service, based on personal data obtained from their activity across such contexts.
In-Service Campaigns	promotions and informational messages configured by a Trading Partner and displayed within the Service to End Users of targeted company segments of another Trading Partner
Food Data Provider (FDP)	a Customer that shares ingredient or product data for use in the Global Product Library under the Food Data Provider Addendum.
Food Data Provider Addendum	the addendum that governs standards, data quality, update frequency, licenses, and related terms when a Customer acts as a Food Data Provider.
Global Product Library	the shared repository of ingredient and product data made available in the Service, populated by Food Data Providers and Customers pursuant to these Terms and the Food Data Provider Addendum.
External System	any third-party system or service (including a Customer's webshop, POS, ERP, payment gateway, middleware, or network access point) that connects to or exchanges data with the Service.
Designated Third-Party	the specific external system(s), vendor(s), product(s), and version(s) identified for a Standard Integration in the Documentation or expressly in an Order/SOW.

MyFoodOffice Connect	a collective reference to the Provider's standardized, generalized API endpoints and related developer resources provided by the Provider for third-party data exchange.
Designated Endpoint	a Provider-maintained, purpose-built API surface documented by the Provider for a specific purpose or Designated Third-Party
Provider Integration	an integration offered by the Provider as part of the Service (e.g., Accounting Connect, Webshop Connect), whether designated as Standard or delivered as Custom under an Order/SOW.
Third-Party-Built Integration	any integration with the Service that is designed, built, configured, or maintained by a third party other than the Provider (including Customer, Customer's vendors, or independent integrators).
Standard Integration	a Provider Integration that the Provider markets as part of the Service and designates as "Standard" for specific named third-party system(s) and version(s). A Standard Integration is not a universal plugin.
Custom Integration	any integration, mapping, transformation, connector, message profile, or workflow that (a) is developed or configured specifically for the Customer, or (b) goes beyond the documented or agreed scope of a Standard Integration, or (c) requires customer-specific code, mappings, or translations.
Documentation	user guides, policies, and technical specifications made available by the Provider.
Customer Data	all data, content, and information (including text, files, images, recipes, orders, transactions, and configurations) that the Customer or its End Users upload to, store in, or otherwise make available through the Service, including Customer Personal Data as a subset.
Customer Personal Data	the portion of Customer Data processed within the Customer Account on behalf of the Customer, that constitutes personal data as defined by applicable Data Protection Laws. For clarity, Customer Personal Data in the ToS corresponds to Controller Personal Data in the DPA
Operational Data	personal data Provider process as controller (admin users, billing, telemetry, website/marketing, support).
Privacy Policy	the notice describing controller-side processing of Operational Data.
Data Protection Laws	GDPR and applicable implementing laws.
DPA	the Data Processing Agreement attached as **Annex A**.
Integration	a connection between the Service and an External System.
Emergency Changes	changes to address a security vulnerability, service integrity/stability/availability risk, abuse/fraud, or a change required by

	law or a third-party platform/provider that necessitates immediate action
Provider Marks	the Provider's names, logos, trademarks, service marks, trade dress, domain names, and other brand features, whether registered or unregistered, together with all associated goodwill.
Service Level	a measurable performance target for the Service (for example, Availability/Uptime, Support response and resolution times, and data recovery objectives) as described in the Documentation.
SLA Credits	service credits that become available to the Customer if a Service Level is not met in a given period, calculated and applied as described in the Documentation.
Professional Services	work that is billable at then-current rates under a Statement of Work approved by both Parties.

3. Interpretation and Order of Precedence

3.1. **Interpretation**. Capitalized terms have the meanings above. "Including" means "including without limitation". Headings are for convenience only.

3.2. **Order of Precedence**. In case of conflict: (1) the DPA (solely for personal-data matters), (2) any signed statement of work or purchase/implementation agreement, (3) Privacy Policy (controller-side Operational Data matters), (4) these Terms of Service, and (5) Documentation and referenced policies.

3.3. **Food Data Provider Addendum.** If the Customer (or a separate legal entity) participates as a Food Data Provider, the **Food Data Provider Addendum** applies to that activity. In case of conflict solely regarding FDP activity: (1) the DPA (for personal-data matters), (2) Privacy Policy (controller-side Operational Data matters), (3) the Food Data Provider Addendum, (4) these Terms, then (5) Documentation/policies. If there is a conflict regarding Food Data ownership, distribution, integrity, or commercialization, the FDPA prevails.

4. Accounts, Access and Use

4.1. **Account**. Each Customer Account establishes a direct contractual relationship between the Customer and the Provider.

4.2. **Admin & Users**. The Customer controls user provisioning and is responsible for its End Users' compliance with the Agreement. The Customer must maintain current account information and reasonable access controls.

4.3. **Acceptable Use**. The Customer will not: (i) violate law, third-party rights, or the Service's technical limits; (ii) attempt unauthorized access, security testing, scraping, or reverse engineering; (iii) transmit malware or abusive content; (iv) overload, interfere with, or circumvent rate limits. The Provider may suspend access for suspected violations.

4.4. **Organizational Accounts.** Customer Accounts are organizational. By creating or being provisioned with a Customer Account, the individual who accepts these Terms represents and warrants that they have authority to bind the Customer to the Agreement. The Provider is not liable for an unauthorized individual purporting to bind the Customer unless the Provider knew or should reasonably have known the individual lacked authority.

4.5. **Role-based terms.** A Customer may act in different capacities under these Terms (e.g., as a standard Customer, as a Food Data Provider, or both). When acting as a Food Data Provider, the Food Data Provider Addendum applies in addition to these Terms and will govern any conflict for FDP activities.

4.6. **Customer Admin Rights.** The first user registered for a Customer Account is assigned Customer Admin rights (unless otherwise designated by the Customer). The Customer is responsible for appointing additional Customer Admins, managing End Users and their permissions, and promptly revoking access for any user who no longer acts on the Customer's behalf.

4.7. **Local User Administration.** Customer Admins may create, modify, and disable End User accounts and set role-based permissions within the Customer Account. The Customer is solely responsible for ensuring such users are duly authorized and for promptly suspending or removing access when required. The Provider is not liable for unauthorized access arising from the Customer's user-administration decisions, except to the extent caused by the Provider's gross negligence or willful misconduct.

4.8. **Duty to Update & Transfer.** The Customer must keep account, billing, and contact information complete and up-to-date, and must promptly transfer or reassign Customer Admin rights when roles change.

4.9. **Information Accuracy; Limited Access Pre-validation.** The Customer will provide accurate information (e.g., company name, business ID, address, contact details, and business activity). The Provider may offer limited access until required information is verified and may suspend or terminate accounts that remain incomplete or inaccurate.

4.10. **Proof of Authority; No Circumvention.** The Provider may request reasonable documentation demonstrating a user's authority to act for the Customer. Without the Provider's written consent, the Customer must not register (or attempt to register) a new account to replace an account previously terminated for cause.

4.11. **Responsibility for Users; Indemnity.** The Customer is responsible for all actions taken under its Customer Account (including by Customer Admins and End Users), except to the extent caused by the Provider's gross negligence or willful misconduct. The Customer will indemnify and hold the Provider harmless from third-party claims arising from access granted by the Customer to individuals who lacked authority or whose access the Customer failed to revoke in a timely manner.

4.12. **Safeguarding.** The Customer must keep all authentication factors (e.g., passwords, API keys, certificates, tokens) confidential, not share them between individuals, and follow the Documentation for secure setup and rotation.

4.13. **Compromise Notification.** The Customer must promptly (and in any event without undue delay) notify the Provider at support@myfoodoffice.com upon learning of any suspected or actual unauthorized access, compromise of credentials, or other security incident affecting the Customer Account. The Provider may suspend access reasonably necessary to protect the Service and data and will restore access once the issue is resolved.

4.14. **Administrator Suspension on Customer Request.** Upon a verified request from the Customer, the Provider will use reasonable efforts to suspend specified Customer Admin credentials without undue delay during support hours. The Provider may require identity and authority verification before acting. Suspension timing is not guaranteed, and the Provider is not liable for any access or actions occurring before the suspension is processed or arising from delays attributable to the Customer, except to the extent caused by the Provider's gross negligence or willful misconduct. The Customer remains responsible for promptly revoking access within the Customer Account where possible and for notifying the Provider of any suspected compromise.

4.15. **Liability Allocation.** See Sections 12 Customer Responsibility and 22 Limitation of Liability for consequences of failing to safeguard access.

4.16. **Prohibited Practices.** The Customer shall not share passwords between users, hard-code credentials in publicly accessible repositories, or circumvent access controls or rate limits. The Provider does not store passwords in plaintext and will never request a password by email.

5. Description of the Service

5.1. **Scope.** The Service is a cloud platform for professional food companies that supports: (i) product data and compliance workflows (e.g., recipes, declarations, costing, labeling); (ii) business operations (e.g., ordering, production, packing, warehousing, route planning); (iii) shop analytics and demand forecasting; and (iv) data exchange with external systems and trading networks. Modules are organized across these pillars and may be enabled per the Customer's subscription plan.

5.2. **Modules & Evolution.** The Provider may add, modify, or deprecate features or modules over time. Where a change would materially reduce core functionality of the Customer's subscribed plan, the Provider will give notice under Section 23 Changes to the Service or Terms.

5.3. **Ordering & Operations.** The Service can expose a B2B webshop and support order capture, production planning, packing, delivery documentation, route summaries, and related reports/analytics. Availability and specifics may vary by plan, configuration, and jurisdiction.

5.4. **Shops & Forecasting.** The Service may provide shop-level insights and demand prediction features to support ordering efficiency and waste reduction. Outputs depend on Customer Data and configuration and are further governed by Section 22 Limitation of Liability.

5.5. **Regulatory & Labeling Tools.** The Service offers decision-support tools for food declarations, ingredient/allergen management, nutrition calculation, label templates and costing ("Regulatory & Labeling Tools"). These tools depend on Customer Data, configuration choices, and any third-party or supplier-provided data the Customer elects to use. The Service does not constitute legal advice and cannot ensure compliance with all jurisdiction-specific rules, interpretations or enforcement practices.

5.6. **Global Product Library.** The Service may expose shared product and ingredient libraries to authorized users. Where such data originates from a Food Data Provider, the provider's obligations on standards, data quality, frequency of updates, and change notices are set out in the Food Data Provider Addendum.

5.7. **Ingredient & Supplier Data**. The Service may expose ingredient records provided by third parties, including Food Data Providers. Such records are made available "as provided" by the source. The Provider does not audit, warrant, or guarantee the accuracy, completeness,

conformance, or timeliness of third-party/supplier data, and may display it “as provided”. The Customer is solely responsible for evaluating suitability, configuring rules, and validating outputs for its regulatory and commercial purposes.

5.8. **Food Data Provider Records.** Rights to display and distribute FDP Data, integrity obligations (no substantive alteration), and license survival for existing copies are governed by the Food Data Provider Addendum (Annex B, §§7–10). See also §3.3 (Order of Precedence for FDP activity).

5.9. **Nutrition Calculations & Rounding.** Nutrition and allergen outputs are computed from inputs and rules configured by the Customer (e.g., formulations, yields, cooking factors, density, rounding/presentation rules). Outputs may differ from laboratory analyses. The Customer is responsible for validating outputs and selecting the correct jurisdictional rounding/presentation rules.

5.10. **Jurisdictions & Templates.** Label templates and regulatory checks, where available, are provided for convenience and may not reflect all applicable requirements, jurisdiction-specific rules or interpretations. The Customer is responsible for selecting the correct template, language variants, and mandatory statements for each market.

5.11. **Allergen & Cross-Contact.** Allergen flags and warnings are generated from data entered or enabled by the Customer. Cross-contact (“may contain”) and other precautionary statements require the Customer’s risk assessment and policy; the Service does not determine or recommend such statements. Outputs are provided for convenience and do not guarantee that allergen lists or warnings are complete, accurate, or fit for the requirements of any particular jurisdiction or market (including without limitation local language, formatting, emphasis, priority rules, or enforcement practices). The Customer is solely responsible for verifying compliance and selecting the correct statements for each market.

5.12. **Claims & Marketing Content.** Any nutrition, health, origin, sustainability or marketing claims placed on labels or listings are determined by the Customer. The Service does not validate claim substantiation or local claim restrictions.

5.13. **Labels & Certifications.** Where available and enabled, the Service provides decision-support tools and templates for certain labeling schemes and certifications, including without limitation The Norwegian Bread Scale label and the Nordic Key Hole.

a) These tools (i) rely on Customer inputs, configurations, and any third-party/supplier data the Customer elects to use; (ii) are provided for convenience; and (iii) do not constitute legal advice or a determination of eligibility. The Provider is not a certifying authority and does not guarantee that any label, mark, claim, or certification produced or supported by the Service is complete, accurate, or fit for the requirements of any jurisdiction or market.

b) The Customer is solely responsible for: (i) verifying scheme eligibility and ongoing conformity against the then-current criteria/rules, guidance, and enforcement practices; (ii) obtaining and maintaining any required licenses/permissions to use scheme names, logos, or marks and complying with brand/use guidelines; (iii) performing and documenting any required analyses, calculations, testing, and record-keeping; (iv) ensuring correct language, formatting, emphasis, and priority on labels; and (v) promptly updating or withdrawing labels/claims when formulations, suppliers, or applicable rules change. Scheme criteria and interpretations may change at any time; the Provider may update related checks/templates, but does not warrant timeliness or coverage of such updates.

c) If a competent authority or scheme owner notifies the Provider of non-compliance or misuse, the Provider may (without liability) disable or adjust the relevant template or flag until the issue is resolved. All scheme names and logos are the trademarks of their respective owners.

5.14. **Barcodes & Identifiers.** Where the Service helps generate barcodes/identifiers (e.g., GS1), it does so based on inputs supplied by the Customer. The Customer is responsible for GS1 membership, allocation rules, symbol quality/printing and retailer-specific requirements.

5.15. **Change History & Traceability.** The Service can maintain version and event logs (who/what/when) for traceability. Availability and retention of logs may vary by module, plan, and configuration as described in the Documentation.

5.16. **Integrations (overview).** The Service may interoperate with External Systems via (i) Provider Integrations (Section 10), and (ii) Third-Party-Built Integrations (Section 11). Common Integration Terms apply to all (§10.1). Compatibility is limited to Designated Third-Parties named in the Documentation or Order/SOW. No specific integration is guaranteed unless expressly agreed. For generalized API endpoints, see MyFoodOffice Connect (Section 9).

5.17. **Group / Multi-site.** For eligible plans, the Service may support multi-entity and centralized management features to coordinate shared data and order flows across locations.

5.18. **Documentation Controls.** Functional details, supported message types/versions, rate limits, and configuration requirements are described in the Documentation and may be updated from time to time.

5.19. **Beta/Preview.** Beta or preview features are provided AS IS, may be changed or withdrawn at any time, and are excluded from SLAs and warranties.

6. Interaction between Trading Partners

6.1. **Ordering Account Invitation.** When a counterparty is invited by a supplier to order via the Service, that counterparty creates an Ordering Account. Legally, that counterparty becomes a Customer under these Terms. In each order it acts in the Buyer role, and the supplier acts in the Seller role. The supplier controls what the Buyer can see and order in its storefront.

6.2. **Creation & Contracting.** When a Customer invites a counterparty to place orders via the Service, that counterparty may create (or be provisioned with) its own Customer Account (an Ordering Account). Each Ordering Account forms a direct agreement with the Provider under these Terms, independent of the inviting Customer.

6.3. **Scope of Use (Ordering Accounts).** Ordering Accounts may access those parts of the Service that the inviting Customer enables (e.g., catalog discovery, order placement and modification, confirmations, and related messaging). Ordering Accounts have no administrative rights in the inviting party's Customer Account.

6.4. **Configuration & Controls (Seller responsibility).** The inviting Customer controls Buyer onboarding, catalog visibility, prices, order windows/cut-offs, minimums, permitted change/cancellation rules, and channel-specific constraints, and is responsible for ensuring invited users are duly authorized to act for the Buyer.

6.5. **Relationship Between Trading Partners (No Privity).** Commercial terms (pricing, delivery/Incoterms, taxes, payment, cancellations/returns, service levels) are solely between Buyer and Seller. The Provider is not a party to those commercial contracts and does not control acceptance or fulfillment.

6.6. Roles and Data Protection.

a) **Controller/Processor.** Each Customer (including Ordering Accounts acting in the Buyer role and Sellers) is the data controller for personal data in its own Customer Account; the Provider acts as processor under the DPA (Annex A) and processes/transmits business messages strictly on the Customer's documented instructions.

b) **Independent Controllers on Receipt.** Upon exchange, the receiving Trading Partner acts as an independent data controller for the data it receives.

c) **No Joint Controllership.** The Trading Partners (Buyer and Seller) do not jointly determine purposes and means for these exchanges and therefore are not joint controllers under GDPR Art. 26. For clarity, the Provider acts as a processor and is not a joint controller with any Customer.

d) **Lawful Basis & Transparency.** Each Trading Partner remains responsible for having a lawful basis and required transparency for any personal data it discloses or receives in these exchanges (see the DPA).

e) **Data Minimization & Logs.** Only information necessary for ordering/fulfillment is exchanged. The Service may expose event/version logs (who/what/when) to involved Trading Partners for traceability.

f) **Campaign Analytics.** Provider may disclose to the originating Seller that the Buyer viewed or engaged with a Seller-configured campaign as part of the trade relationship between Buyer and Seller. The Seller receives this information as an independent controller. The Provider does not sell or rent Customer Data or Customer Personal Data to third parties and does not use such data for cross-context behavioral advertising. For clarity, the disclosure described in this subsection concerns in-Service, first-party campaigns and is subject to §14.6 Processing of any personal data in connection with in-Service campaigns is subject to the DPA (processor) and the recipients act as independent controllers upon receipt (see DPA §4.7).

g) **Shared Ingredient Library (if applicable).** When the Customer imports or uses ingredient data made available by a third party in the Service, the Customer authorizes the Provider to notify that third party of such use for traceability and data-quality purposes.

6.7. **Operational Communications.** Operational notifications (e.g., order confirmations/updates) generated by the Service are sent on the Customer's instructions. The Customer is responsible for the content, frequency, and lawfulness of such communications to its Trading Partners and contacts.

6.8. **Corrections, Changes, Cancellations.** Where technically feasible, the Provider will transmit Customer-initiated corrections/changes/cancellations without undue delay. If the Trading Partner has begun fulfillment (e.g., accepted, picked/produced, dispatched), further changes may be governed by that Trading Partner's terms; the Provider does not guarantee acceptance.

6.9. **Product Data.** When Trading Partners exchange product/ingredient information, the receiving party is responsible for validating and using it appropriately; the Provider does not verify such information and has no responsibility for Trading Partner decisions based on it.

6.10. **Support Boundaries.** The Provider offers technical support for access and use of the Service. Trade, pricing, fulfillment, quality, and invoice disputes are handled between Buyer and Seller. Support for External Systems used by either party is excluded from included support (see Section 7 Support and Maintenance and Section 8 Hardware Boundaries).

6.11. Suspension & Revocation.

a) The Provider may suspend any Customer Account (including an Ordering Account) for §4.3. Acceptable Use violations, security risk, legal requirement, overdue amounts, or use that materially degrades Service performance.

b) The inviting Customer may revoke an Ordering Account's access to its catalogs/pricing/ordering channels without deleting that Ordering Account.

c) Suspension or revocation does not relieve either Trading Partner of pre-existing commercial obligations between them.

6.12. Fees. Except where expressly stated in an applicable plan, Order, or public pricing, Ordering Accounts do not incur license fees; module fees and transaction-related charges (if any) are billed to the Customer that enabled the relevant channel or module. Any Ordering-Account-specific fees will be disclosed in the applicable plan or ordering document.

6.13. Upgrades & Conversion. An Ordering Account may upgrade to a broader paid plan by entering into an order with the Provider. The Provider may migrate legacy ordering experiences to newer flows on notice (see Section 23 Changes to the Service or Terms).

6.14. Branding. A B2B storefront may display the inviting Customer's branding; however, the Service is operated by the Provider and governed by these Terms and the DPA regardless of branding.

7. Support and Maintenance

7.1. Scope. This Section describes what is included in the subscription license and what is chargeable as Professional Services. If later updates to these Terms change this Section, the Section 23 Changes to the Service or Terms controls.

7.2. Service Levels by Plan. Support scope, response times, and availability may vary by subscription plan or Service tier. Higher tiers may include enhanced response commitments, dedicated customer-success or account-management resources, or other service levels as described in the applicable plan, Order, or Documentation. Unless expressly stated for the Customer's plan, no minimum response or resolution time is guaranteed, and access to live support or a dedicated contact is not included.

7.3. Changes to Service Levels. The Provider may update plan-specific service levels from time to time in accordance with Section 23 Changes to the Service or Terms; such updates do not constitute a Material Change unless they materially reduce the overall support level of the Customer's current paid plan.

7.4. Excluded from Support. Included Support does not cover: (i) third-party software, hardware, or the Customer's technical environment (computers, operating systems, networks); (ii) performing operational tasks on the Customer's behalf (e.g., bulk data entry, data export/import, content setup); or (iii) on-site work. These items may be provided as Professional Services at then-current rates.

7.5. Troubleshooting & Bug Fixes. Provider will triage and address software defects based on severity and business impact. Issues caused by user error, misconfiguration, or deficient internal routines are outside Included Support but may be assisted through Professional Services.

7.6. **Hosting**. The Service is delivered as a cloud service. Production data is currently hosted on Provider-controlled cloud infrastructure. Hosting locations and Sub-processors may change in accordance with the DPA; no data-residency commitment applies unless expressly agreed in an Order.

7.7. **Backups & Continuity.** Regular backups of Customer Data stored in the Service are performed, and restore procedures are tested at reasonable intervals. Program targets are not service-level guarantees. Return/deletion of Customer Personal Data is governed by the DPA.

7.8. **Maintenance Windows.** Scheduled maintenance may occur with reasonable prior notice; emergency maintenance may occur without notice. Service-level remedies (if any) exclude downtime caused by third-party networks, cloud-provider incidents, or Emergency Changes required to preserve security/availability.

7.9. **Browser & Platform Compatibility.** The codebase is maintained for compatibility with modern, supported browsers and technologies. End-of-life browsers or environments are not supported.

7.10. **Versions & Updates.** New versions and improvements are released on a regular cadence (typically around monthly) and are included in the ongoing subscription. Features may be added, modified, or deprecated per Section 23 Changes to the Service or Terms.

7.11. **Integrations support.** Support scope and responsibilities for integrations are set out in Section 9 (MyFoodOffice Connect), Section 10 (Provider Integrations & API Terms), and Section 11 (External Systems & Third-Party-Built Integrations).

7.12. **Hardware Boundary.** Provider's responsibility ends at the Service and its documented interfaces. Assistance with devices beyond the Service interfaces is outside Included Support and may be provided as Professional Services. See also Section 8 Hardware Boundaries for module-specific responsibilities and what is included versus billable.

7.13. **Professional Services.** The following are examples (non-exhaustive) of Professional Services that are chargeable at then-current rates: performing operational tasks for the Customer (e.g. data entry, bulk data preparation or import/export, quality review, consultancy, custom reports or mappings), integration development or re-mapping, on-site work, extended training, and support for the Customer's technical environment (including but not limited to OS, network, printers, scales, third-party software and apps). For clarity, issues attributable to External Systems or Third-Party-Built Integrations are outside Included Support and Service Levels; see §11.5.

8. Hardware Boundaries

8.1. **General.** The Service may interact with Customer-owned devices (for example, printers, label printers, scales, or other peripherals). These devices and their operating environments remain under the Customer's control. The Provider's responsibility is limited to the correct operation of the Service and any connector software supplied by the Provider. All other work may be performed as Professional Services

8.2. **No Service-Level Commitment for External Devices.** The Provider does not guarantee performance or uptime of the Service where disruption arises from Customer-managed devices, drivers, firmware, OS/browser policies, or network connectivity.

8.3. **Fair-Use Triage.** The Provider may perform brief remote triage to determine whether an issue originates in the Service or the Customer environment (device/driver/OS/network). When external, further assistance is billable as Professional Services.

8.4. **OEM Terms.** The Provider is not responsible for hardware warranties, replacements, or original equipment manufacturer or hardware supplier's terms (OEM terms).

8.5. **Food Labels Module**

a) **Scope.** The Food Labels module enables users to design and issue print jobs to Customer-managed label printers.

b) **Customer Responsibilities.** The Customer is responsible for: (i) installing and configuring the printer, drivers, print queues, firmware, and label media; (ii) ensuring the printer is accessible from the operating system and web browser used for the Service; and (iii) managing printer settings such as label dimensions, gaps, margins, print darkness, and physical alignment.

c) **Included Support.** The Provider will: (i) assist with template creation and confirm that print jobs are dispatched from the Service to the browser, (ii) verify that a compatible printer can receive a test print job when available to the browser.

d) **Excluded Support (Billable).** The following are outside Included Support and may be billed as Professional Services; (i) printer, driver, or firmware installation and calibration, (ii) OS/browser permission or security policy issues, (iii) Network, USB, Bluetooth, or serial-port connectivity, (iv) Printer configuration like label margin/gap calibration or media tuning, (v) Troubleshooting third-party label tools or OEM utilities.

e) **Disclaimer.** Due to differences between printers, drivers, and browsers, the Provider does not warrant identical print output, layout fidelity, color accuracy, or edge-to-edge printing.

8.6. **MyFoodOffice Link (Local Connector)**

a) **Purpose.** MyFoodOffice Link is a locally installed connector that transmits data from Customer-owned scales to the Service. MyFoodOffice Link license includes the software and updates but excludes any hardware or third-party tools.

b) **Customer Responsibilities.** The Customer is responsible for: (i) maintaining compatible devices, drivers, and cabling; (ii) ensuring network connectivity, OS permissions, and security configurations; and (iii) keeping MyFoodOffice Link and required dependencies up to date.

c) **Included Support.** (i) Access to installation instructions; (ii) remote verification that MyFoodOffice Link runs and communicates with the Service, (iii) Fixes for confirmed Provider-side defects in MyFoodOffice Link.

d) **Excluded Support (Billable).** (i) Hardware setup, network configuration, proxy/firewall tuning, serial-port mapping; (ii) OS, security, or policy adjustments; (iii) recurring issues caused by Customer environment changes; (iv) On-site work or travel.

e) **Connectivity & Legal Metrology Disclaimer.** MyFoodOffice Link depends on Customer-managed environments (device drivers, COM/USB ports, network/firewall, OS updates, power, and physical cabling). The Provider does not warrant uninterrupted device connectivity or compatibility with future OS, driver, or firmware changes. The Customer is solely responsible for (i) device calibration, verification, and maintenance; (ii) any weights-and-measures or legal-metrology approvals, seals, and records required by law; and

(iii) ensuring that any scale model and configuration are fit for the Customer's intended commercial use. Where a loss of connectivity or data capture is caused by Customer-side environments or third-party components, remediation beyond reasonable triage is Professional Services.

f) **Data Capture During Interruptions.** If connectivity is interrupted, readings may be delayed, queued, or unavailable. The Service does not guarantee real-time capture or backfill of missed readings. The Customer must validate critical entries and re-weigh as needed.

g) **OEM Warranty & Limits.** Any hardware warranties are solely from the device manufacturer or reseller. The Provider is not responsible for OEM defects or RMA processes and will not repair or replace third-party devices.

9. MyFoodOffice Connect

9.1. **Scope.** MyFoodOffice Connect consists of standardized, generalized API endpoints documented by the Provider. MyFoodOffice Connect is not built for a specific third-party system, endpoint, message profile, or use-case and does not imply support for any Designated Third-Party. For clarity, MyFoodOffice Connect is distinct from Designated Endpoints, which are documented purpose-built Provider API surfaces as defined in Section 2.

9.2. **Formats & versioning.** For MyFoodOffice Connect, the Provider determines supported formats and schemas and may add, modify, or deprecate endpoints per Section 23, without any guarantee of backward compatibility, with reasonable deprecation windows where feasible.

9.3. **Support boundaries.** MyFoodOffice Connect does not include Customer-specific mappings or third-party remediations; such work is out of scope and is delivered as Professional Services at then-current rates.

9.4. **Third-Party involvement.** Integrations built by third parties using MyFoodOffice Connect are Third-Party-Built Integrations and are outside included support and service levels, in accordance with Section 11. Use of MyFoodOffice Connect by third parties does not expand support scope beyond Provider-side endpoint behavior as documented.

10. Provider Integrations & API Terms

10.1. **Common Integration Terms (apply to all integrations).**

a) **Credentials & Security.** Each Party secures its own systems. The Customer must safeguard any third-party credentials and API keys used with the Service.

b) **Identifiers & Authentication.** The Customer must maintain accurate Trading-Partner identifiers (e.g., Peppol participant IDs, GLNs, VAT numbers) and keep credentials/certificates/API keys secure. The Provider may suspend exchange upon suspected misuse or invalid credentials.

c) **Traffic Quality.** The Provider may reject/quarantine malformed or non-conformant messages and expose error details via logs.

d) **Fair Use & Rate Limits.** Customer shall not exceed documented rate limits or circumvent controls; abusive traffic may be throttled or suspended.

e) **API Data Handling.** Customer shall not persist or cache Customer Personal Data retrieved via the API beyond what is necessary for the documented purpose and will secure any stored data appropriately. Processing of personal data via integrations is governed by the DPA.

f) **External Systems**. External system availability, performance, data quality, or conformance are outside the Provider's control. Service Levels and remedies exclude downtime or issues caused by them. (see Section 11).

g) **Customer Responsibilities (integrations).** The Customer will (i) procure and maintain required third-party accounts, credentials, permissions, and certificates; (ii) avoid unauthorized changes that break agreed mappings or profiles; (iii) provide timely test data and acceptance during integration work; (iv) promptly notify the Provider of material External System changes (e.g., authentication, endpoints, or mandatory fields) that may affect an integration; and (v) maintain a suitable non-production test environment with representative (minimised) data for acceptance and regression testing.

h) **Processing & routing on Customer instructions.** The Customer instructs the Provider to process, route, transmit, receive, validate, and store messages and data exchanged with Trading Partners through the Service, including via External Systems and supported networks.

i) **No Monitoring of External Roadmaps.** Provider has no obligation to monitor, track, or provide advance notice of upcoming changes to any External System, third-party API, message profile, or network. The Customer remains responsible for awareness of and compliance with such changes.

10.2. **Scope.** The Service supports Provider Integrations which may be designated as Standard or delivered as Custom under an Order/SOW. Compatibility is limited to Designated Third-Parties and does not imply universal plugins or open-ended mapping coverage. Where a Provider Integration connects with a Designated Endpoint, AS-IS upkeep covers the Provider side of that endpoint as documented; significant third-party changes remain out of scope under §10.4.

10.3. **Standard Integrations (AS-IS upkeep).** For Standard Integrations with Designated Third-Parties, the Provider will keep the integration working as documented (AS-IS) within the supported scope. Routine break/fix, minor version bumps, and adjustments reasonably required to maintain documented behavior are included in the subscription.

10.4. **Significant changes (out-of-scope).** If a Designated Third-Party makes a material/breaking change, deprecates endpoints, or introduces new mandatory flows or authentication that require significant re-work, the Provider may (i) deliver an update at its discretion under Section 23 Changes or (ii) offer a Statement of Work for out-of-scope effort. No timelines are guaranteed unless agreed in writing. Any Customer-specific mapping, connector changes, or third-party remediation required as a result are outside Included Support and delivered as Professional Services.

10.5. **Custom Integrations (billable).** Any development, re-mapping, transformation, message-profile change, regression testing, environment setup, or other work on a Custom Integration — including when triggered by Customer requirement changes, Provider endpoint changes or third-party changes — is outside Included Support and is delivered as Professional Services.

10.6. **Designation & scope control.** The status of an integration (Standard vs Custom), its Designated Third-Parties, supported versions, message types, and enabled options must be stated in the Documentation or expressly designated in the Order/SOW. Anything not designated is out of scope.

10.7. **No universal plugins.** Marketing names such as Accounting Connect or Webshop Connect describe families of Standard Integrations that are limited to Designated Third-Parties and agreed scope; they are not generic connectors for all vendors in a category.

10.8. **Testing & acceptance for Custom work.** Custom Integration deliverables follow the acceptance procedure in the Order/SOW. If none is stated: acceptance occurs upon the earlier of (i) signed acceptance, or (ii) 10 business days after delivery without a material, written rejection specifying defects.

10.9. **Deprecation & version windows.** The Provider may deprecate support for specific versions or flows of a Designated Third-Party in accordance with Section 23 Changes. Where feasible, notice will identify a version window and any required Customer actions.

10.10. **IP and data.** Unless otherwise agreed in the Order/SOW, mappings, transforms, and integration code for Provider Integrations are part of the Service IP; the Customer owns its data.

11. External Systems & Third-Party-Built Integrations

11.1. **External Systems.** The Service may interoperate with external systems operated by third parties. The Provider does not control such systems and does not guarantee their availability, performance, data quality, or conformance. This Chapter is subject to §10.1 (Common Integration Terms).

11.2. **Third-Party-Built Integrations.** Any integration with the Service that is built, configured, or maintained by a third party (including by the Customer or Customer's vendors) is a Third-Party-Built Integration. Such integrations are outside Included Support and outside Service Levels. For the avoidance of doubt, where a Third-Party-Built Integration connects to a Designated Endpoint, the Provider's responsibility is limited to the correct operation of that Designated Endpoint as documented; the third party's connector remains outside Included Support/Service Levels.

11.3. **Changes by Third Parties.** Third-party changes (including API, authentication, data models, or endpoints) that affect a Third-Party-Built Integration are outside the Provider's responsibility. The Provider has no obligation to modify the Service to accommodate such changes.

11.4. **Customer Responsibilities.** The Customer is responsible for (a) vetting third parties; (b) their compliance with these Terms and applicable law; (c) security of any credentials they use; and (d) ensuring that Third-Party-Built Integrations do not degrade or harm the Service.

11.5. **No Liability for External Systems; Service Levels.** Any unavailability, degradation, data loss, non-conformance, or security incident attributable to External Systems or to Third-Party-Built Integrations (each, an "External Cause") is not the Provider's responsibility and (a) does not count toward support time commitments (initial response or resolution targets), (b) does not count toward uptime/availability commitments ("Service Levels"), and (c) does not entitle the Customer to any remedies, fee reductions, or service credits ("SLA Credits"). Examples include: changes to External Systems or networks, and format/version or

endpoint changes outside the Service that require re-testing or re-mapping. Remediation of External Causes may be delivered as Professional Services at then-current rates.

12. Customer Responsibility

12.1. **Scope.** This Section provides a non-exhaustive list of customer responsibilities. Unless otherwise stated, the Customer remains solely responsible for compliance, adhering to industry standards and practice, the managing and use of the system, and decisions made on the basis of the Service.

12.2. **Accounts & users.** Appointing Customer Admins, authorizing End Users, managing permissions, and promptly revoking access.

12.3. **Safeguards & Notice.** Customer must protect credentials, API keys, and tokens and promptly notify Provider of any suspected compromise (see §4.13 Compromise Notification).

12.4. **Configurations & use.** Selecting modules/features, configuring workflows and rules, testing changes before production, and validating outputs generated by the Service. Any information, recommendations, forecasts, optimizations, costings, calculations, reports, or other outputs generated by the Service are for guidance only and must be validated by the Customer before use; accuracy and completeness depend on Customer Data, configurations, and (where applicable) External Systems or third-party data.

12.5. **Data input & quality.** Ensuring accuracy, completeness, and timeliness of data it enters or imports; having and maintaining all necessary rights in such data.

12.6. **Regulatory compliance.** Ensuring its product information, labels, claims, packaging, marketing, and communications comply with applicable law, industry standards and practice (including food, labeling, and consumer rules).

12.7. **External Systems.** Selecting, contracting, configuring, securing, and operating any External Systems (e.g., webshop, POS, ERP, payment, iPaaS, networks) that connect to the Service (see Section 11 and §10.1).

12.8. **Trading Partner relationships.** All commercial terms and communications with Trading Partners (pricing, delivery, taxes, cancellations/returns, service levels) and the content/frequency/lawfulness of operational notices sent on Customer's instructions.

12.9. **Lawful basis & transparency.** Having a lawful basis and required transparency for any personal data it provides or instructs the Service to process, and performing any required DPIA/assessments (see the DPA).

12.10. **Data categories.** Not instructing processing of prohibited/special categories unless expressly agreed in writing in accordance with the DPA.

12.11. **Exports & retention choices.** Exporting data needed for its records and configuring retention/deletion options available in the Service.

12.12. **Fees & taxes.** Paying fees and applicable taxes per the Agreement.

13. Group Customers & Participating Affiliates

13.1. **Eligibility & Listing.** Group discounts and consolidated terms apply only to Participating Affiliates expressly identified in the applicable Order. The Provider may request reasonable evidence of affiliation.

13.2. **Authority & Responsibility.** The Master Customer represents and warrants it has authority to bind each Participating Affiliate listed in the Group Order. The Master Customer is jointly and severally liable for all fees and obligations of Participating Affiliates under the Group Order, and the Provider may invoice the Master Customer for any Participating Affiliate's unpaid amounts.

13.3. **Separate Customers; No Privity Among Them.** Except as expressly set out in this Section, each Participating Affiliate remains a separate Customer under these Terms. The Provider is not a party to commercial arrangements between group members.

13.4. **Group Discounts;** Changes. Group discounts (if any) are determined in the Group Order and recalculated at renewal based on: (i) the Participating Affiliates then in scope, and (ii) the modules then licensed. Mid-term additions/removals normally take discount effect at the next renewal. Discounts may be adjusted if group structure or license counts were misstated or materially change.

13.5. **Termination or Dissolution Events.** If a Participating Affiliate ceases to qualify (e.g., loss of affiliation) or is removed from the Group Order, its access continues through the current term (unless terminated under the Agreement) and renews separately on then-current terms unless otherwise agreed. Any no-longer-applicable group discount will be removed at renewal.

13.6. **Aggregated Liability Cap (Group).** Where a valid Group Order applies, the aggregate liability of the Provider to the Master Customer and all Participating Affiliates together arising out of or related to the Agreement and the DPA (whether in contract, tort, or otherwise) shall not exceed the lesser of: (i) NOK 100,000 (excluding VAT); or (ii) the aggregate fees paid or payable under the Group Order for the Services in the twelve (12) months immediately preceding the first event giving rise to liability. All claims by any group member count toward, and share, this single cap. The exclusions and disclaimers in Section 22 Limitation of Liability continue to apply. For Customers not under a Group Order, the standard per-Customer cap applies.

13.7. **Data Protection Pointer.** For DPA purposes, each Participating Affiliate listed in a Group Order acts as a separate controller for its own Customer Account. The Parties are not joint controllers. Nothing in this Section alters the roles or obligations set out in the DPA.

14. Data Protection

14.1. **Roles.** Within the Customer Account, the Customer is the data controller and the Provider the data processor. The Parties' obligations are set out in the **DPA (Annex A)**.

14.2. **Operational Data (controller).** Provider acts as data controller for Operational Data as described in the Privacy Policy. For any conflict between this Section and the Privacy Policy regarding Operational Data, the Privacy Policy controls.

14.3. **Membership Verification & Third-Party Contact.** The Customer authorizes the Provider to contact third parties to: (a) verify membership status for benefits; and/or (b) enable or disable

features that depend on third-party consent or setup, in each case on the Customer's instruction and for the Customer's purposes.

14.4. **Sub-processors.** Provider may use sub-processors to deliver the Service, as described in DPA Section 7. The detailed sub-processor roster is not public and is available to Customers upon request under confidentiality. Provider will give advance notice of intended changes and Customers may object as set out in the DPA.

14.5. **Data Protection.** Data-subject requests relating to Operational Data (where Provider is controller) are handled in accordance with the Privacy Policy and may be sent to support@myfoodoffice.com. Requests relating to Customer Personal Data (processed on Customer's behalf) are handled under the DPA and will be redirected to the Customer as controller.

14.6. **No Sale or Cross-Context Ads.** Provider does not sell or rent Customer Data or Customer Personal Data to third parties and does not use such data for cross-context behavioral advertising (i.e., targeting across businesses, websites, apps, or services other than the Service). Provider processes Customer Data solely to deliver the Service and support per the Agreement and DPA. For clarity, §19.6 (Aggregated/De-identified Data; Derived Data) remains permitted, provided no Customer or data subject is identifiable. In-Service Campaigns configured by Trading Partners (see §6.6) and related company-level analytics do not constitute cross-context behavioral advertising.

15. Security, Backup and Continuity

15.1. **Security Program.** The Provider maintains administrative, technical, and physical safeguards appropriate to the Service.

15.2. **Backups.** The Provider performs regular backups of Customer Data stored in the Service and tests restoration procedures at reasonable intervals. Backup retention and restore testing cadence are described in the Documentation.

15.3. **Incidents.** Security incidents involving Customer Personal Data will be handled per the DPA.

15.4. **Security Monitoring & Enforcement.** Provider may monitor Service usage, network traffic, and logs to maintain security, prevent fraud/abuse, enforce these Terms, and protect Service integrity, and may investigate suspected violations and suspend or block access that poses a risk or violates these Terms. Provider will access Customer Data only as reasonably necessary to provide support, investigate security/availability incidents, or comply with law. Processing of Customer Personal Data in this context is governed by the DPA; telemetry and logs are processed as Operational Data under the Privacy Policy. Nothing in this Section creates a duty to monitor Customer activity or content.

16. Subscription Plans, Trials, and Plan Changes

16.1. **Plan Structure; Modular Licensing.** The Service is licensed on a modular, scope-based model. Access to specific features is determined by (i) the Modules the Customer licenses, (ii) the Tier of each Module (e.g., Standard or Pro), and (iii) the Scope Level(s) at which each Module is activated (Group, Production, and/or Store), as stated in the applicable Order or on the Provider's pricing page. If there is a conflict, the Order prevails.

16.2. **Scope Levels and Counting Rules.** The following scope levels apply;

a) **Group.** The Group Scope Level provides shared master data and chain-level controls across Participating Affiliates and/or sites.

b) **Production.** A “Production” license applies per (i) legal entity engaged in food production and sales, or (ii) distinct production site that functions as a separate economic unit of material scale. The predominant number of customers are B2B or own Stores.

c) **Store.** A “Store” license applies per owned or controlled retail outlet selling predominantly to consumers.

16.3. **Tiers.** Each Module may be offered in one or more Tiers, such as Standard and Pro, with the features described in the Documentation. The Tier for a Module at a given Scope Level is shown on the Order.

16.4. **Term Options; Co-Terming.** Plans may be offered on monthly or annual terms (or as otherwise stated).

16.5. **Upgrades and Add-Ons (Co-Term).** The Customer may add Modules, increase Scope Levels (e.g., add Stores or Production sites), or upgrade Tiers at any time. Additional fees are charged pro-rata for the remainder of the then-current billing period, and the change co-terms with the existing subscription.

16.6. **Downgrades and Reductions.** Plan downgrades (including Tier reductions or removal of Modules or Scope Levels) take effect at the next renewal. Features removed by a downgrade remain available until the effective date and will be disabled after that date. The Customer is responsible for exporting data and adjusting configurations that rely on downgraded features before the effective date. For clarity, §17.6 No Refunds applies.

16.7. **Participating Affiliates.** Participating Affiliates may use licensed Modules solely within the Scope Levels and Tiers specified on the Order. The Provider may require that certain Modules at the Group Scope Level be licensed by the Customer entity that administers the shared tenant.

16.8. **Role Transitions (FDP ↔ Customer).** If an entity that has signed the Food Data Provider Addendum later upgrades or adds other modules, it becomes a Customer under these Terms for those modules; the Food Data Provider Addendum continues to govern (i) previously contributed provider data and (ii) any new provider contributions. Conversely, a Customer that begins contributing data to the Global Product Library becomes a Food Data Provider for that activity and the Food Data Provider Addendum applies in addition to these Terms. Termination of a subscription does not by itself revoke licenses already granted for contributed provider data, except as expressly stated in the Food Data Provider Addendum.

16.9. **Pricing and Plan Updates (on Renewal).** The Provider may update plan structures or fees effective upon renewal and will provide at least 30 days’ prior notice. If the Customer does not agree to the updated plan or fees, it may select a different plan available at renewal or elect not to renew.

16.10. **Non-Itemized Pricing; Feature Changes.** Unless the Order itemizes a Module or Scope Level as a separate priced line, the subscription is bundled and non-itemized. Suspension, restriction, or disabling of any single feature, workflow, or integration under the Agreement (including the DPA) does not entitle the Customer to a price reduction, refund, or credit.

16.11. **Trials.** If the Service is provided on a trial basis, the trial duration is shown at sign-up. At the end of the trial, the Customer must convert to a paid plan to continue full access; otherwise, access may be limited or disabled. Trial data may be deleted after a reasonable period if not

converted, subject to the data-export and deletion principles described under §18.9 Effect of Termination; Data Handling.

16.12. **Documentation and Support Scope.** General information about plans is available on the Provider's pricing page, and support scope is described under Section 7 Support and Maintenance, and Section 8 Hardware Boundaries. Nothing in this Section limits clauses in Section 17, Fees, Billing and Taxes, Section 18 Term, Renewal, Suspension and Termination, or suspension provisions elsewhere in these Terms.

17. Fees, Billing and Taxes

17.1. **Fees.** Fees may include recurring license fees (modules and Standard Integrations) and time-and-materials for Professional Services (including Custom Integrations and any out-of-scope re-work under Section 11).

17.2. **Designated Endpoint License.** Certain Designated Endpoints may require a recurring license for operation, monitoring, and AS-IS upkeep on the Provider side, as described in the Documentation or applicable Order. This fee is separate from any Professional Services for connector development or re-mapping.

17.3. **Invoicing & Payment.** Invoices are due 10 days from invoice date.

17.4. **Late Payment Interest and Costs.** Any overdue amount accrues interest from the due date until paid, at the statutory rate pursuant to the Norwegian Act relating to Interest on Overdue Payments (Forsinkelsesrenteloven). Provider may suspend the Service for non-payment under §18.2 and the Customer must reimburse Provider's reasonable costs of collection.

17.5. **Taxes.** Fees exclude taxes; the Customer is responsible for applicable VAT/sales taxes.

17.6. **No Refunds.** Paid fees are non-refundable unless required by law. For bundled, non-itemized plans, fees are not reduced or credited if any single feature is unavailable, suspended, or disabled under the Agreement (including for legal or data-protection reasons). This includes, without limitation, outcomes under the DPA's Section 7 Sub-processor objection process and any disabling of Affected Processing (as defined in DPA Section 2) for legal or data-protection reasons.

17.7. **No Set-Off.** Amounts due under the Agreement must be paid without set-off or counterclaim.

17.8. **Acceleration on Breach.** Upon the Customer's material breach (including material non-payment), all fees for the remainder of the then-current subscription term become immediately due and payable.

18. Term, Renewal, Suspension and Termination

18.1. **Term & Renewal.** Subscriptions renew automatically for successive periods equal to the initial term unless either Party gives 30 days' notice prior to the end of the then-current term.

18.2. **Suspension.** The Provider may suspend the Service for (i) overdue amounts; (ii) security risk (including suspected credential compromise); (iii) violation of §4.3 Acceptable Use or law; (iv) legal requirement; or (v) use that materially degrades Service performance for others.

18.3. **Insolvency.** Either Party may terminate the Agreement immediately by notice if the other Party (i) ceases business, (ii) becomes insolvent or admits inability to pay debts as they fall

due, (iii) makes an assignment for the benefit of creditors, or (iv) becomes subject to the control of a trustee, receiver, administrator, or similar authority, to the extent permitted by applicable law.

18.4. **Termination for Cause.** Either Party may terminate the affected subscription(s) for material breach not cured within 30 days after written notice describing the breach in reasonable detail. If the material breach is not reasonably curable within 30 days, the breaching Party must begin cure within that period and diligently pursue it to completion within a commercially reasonable time. Termination for cause applies only to the affected subscription(s)/Module(s) unless the material breach renders the Agreement as a whole untenable.

18.5. **Immediate Termination by Provider.** The Provider may terminate immediately (or suspend pending termination) for: (i) repeated or material §4.3 Acceptable Use violations; (ii) unauthorized access, sharing, or resale of the Service; (iii) IP infringement, reverse engineering, or circumvention of technical controls; (iv) confidentiality breaches; (v) export-control/sanctions violations; or (vi) use that materially degrades Service performance or poses a security/availability risk.

18.6. **Repeated Breach.** Two or more substantially similar breaches within 6 months constitute a material breach not subject to further cure.

18.7. **Non-Payment as Cause.** In addition to any suspension rights, the Provider may terminate the Agreement for non-payment if fees remain unpaid 15 days after written notice of late payment.

18.8. **Effect on Fees and Refunds (Termination for Cause).** The consequences below exclusively govern fees, credits, and refunds when termination for cause occurs, and apply subject to §17.6 (No Refunds) where specified.

a) If the Customer terminates for the Provider's uncured material breach, the Provider will issue a pro-rata refund credit of prepaid license fees for the unused portion of the current subscription term of the affected subscription(s). The credit will be applied to future invoices; no cash refund. Credits exclude professional-services fees, usage/transaction charges, taxes, and pass-through costs, and constitute Customer's sole monetary remedy for the uncured material breach, subject to the Section 22 Limitation of Liability.

b) If the Provider terminates for the Customer's uncured material breach (including material non-payment), all unpaid fees for the remainder of the then-current subscription term of the affected subscription(s) become immediately due and payable.

c) §17.6 No Refunds provision applies in all other cases.

18.9. **Effect of Termination; Data Handling.**

a) Return/export and deletion of Customer Personal Data are governed exclusively by the DPA (Annex A, "Return and Deletion"), which is incorporated by reference.

b) De-identified/aggregated data and Derived Data may be retained and used as permitted under these Terms. Operational Data (controller-side) retention is governed by the Privacy Policy.

c) Data exports or preparation beyond any in-product self-service tools are Professional Services.

d) FDP Data. For contributed FDP Data, FDPA §16 governs go-forward cessation, historical retention, and consuming customers' local copies.

18.10. **Survival.** Provisions that by their nature should survive (including Confidentiality, Intellectual Property; Feedback, License/Restrictions, Data Protection/DPA, Limitations of Liability, Indemnities/Intellectual Property Claims, Fees and Taxes (for amounts accrued and owing), and 18.9 Effect of Termination; Data Handling) will continue after termination or expiry.

19. Intellectual Property; Feedback

19.1. **Ownership.** The Provider and its licensors own all rights, title, and interest in and to the Service and Documentation.

19.2. **Proprietary Notices.** The Customer must not remove, obscure, or alter any copyright, trademark, or other proprietary notices appearing in the Service, the Documentation, or in any exports or downloads generated by the Service.

19.3. **Customer Data.** The Customer owns its data. The Customer grants the Provider a limited, non-exclusive license to process Customer Data for the purpose of providing the Service and related support. For clarity, when the Customer acts as an FDP, licenses for FDP Data are governed by the Food Data Provider Addendum.

19.4. **Aggregated/De-identified Data** means data that has been **irreversibly de-identified** so that neither a **Customer** nor any **data subject** is identifiable (taking account of reasonable means likely to be used), including statistical or summary data across multiple customers.

19.5. **Derived Data** means data, insights, and learnings generated by the Provider through processing of the Service's data (e.g., metrics, benchmarks, trends, model weights/embeddings, feature importances, and other outputs), excluding Customer Data in an identifiable form.

19.6. **Aggregated Insights; Derived Data.** Provider may create, use, copy, modify, analyze, combine with other datasets, publish, distribute, and commercialize Aggregated/De-identified Data and Derived Data for any lawful purpose, including benchmarking, industry reports, capacity planning, product/service improvement, and training/tuning of algorithms and machine-learning models, provided that no Customer or data subject is identified and no Customer Confidential Information is disclosed in identifiable form. Provider owns all right, title, and interest in Aggregated/De-identified Data and Derived Data and any outputs thereof. Provider will not attempt to re-identify such data and will maintain reasonable technical and organizational measures to prevent re-identification.

19.7. **Relationship to other terms.** Use of personal data to produce Aggregated/De-identified Data is subject to the DPA; any third-party content licenses (including the Food Data Provider Addendum) continue to apply and are not expanded by this clause.

19.8. **Feedback.** The Customer grants the Provider a royalty-free, worldwide, irrevocable license to use suggestions or feedback to improve the Service, without identifying the Customer as the source.

19.9. **License to Use the Service and Documentation.** Subject to these Terms and timely payment of fees, the Provider grants the Customer a limited, revocable, non-exclusive, non-transferable (except as permitted under "Assignment"), and non-sublicensable license to access and use the Service and Documentation for the Customer's internal business purposes during the subscription term.

19.10. **Restrictions.** Except as expressly permitted in these Terms or by law, the Customer must not: (i) resell, rent, lease, lend, or operate the Service for or on behalf of third parties

(including as a service bureau or time-sharing); (ii) sublicense or assign rights in the Service; (iii) copy, modify, create derivative works of, or frame the Service or Documentation; (iv) publish benchmarks or performance tests without the Provider's prior written consent; or (v) use the Service to build a competing product or service. The §4.3 Acceptable Use obligations also apply.

19.11. **Open-Source Components.** Certain components may be offered under open-source licenses; where applicable, those licenses govern the use of those components.

19.12. **Trademarks.** The Customer may not use Provider Marks except to factually identify itself as a customer (and then only in accordance with reasonable brand-use guidelines provided by the Provider). All goodwill arising from use of Provider Marks accrues to the Provider. The Provider's use of the Customer's name/logo is governed by marketing references.

19.13. **Reservation of Rights; Termination of License.** The Provider reserves all rights not expressly granted. The license above automatically terminates upon expiration or termination of the subscription.

20. Confidentiality

20.1. **Definition.** "**Confidential Information**" means non-public information disclosed by one Party ("**Disclosing Party**") to the other ("**Receiving Party**") that is marked or otherwise identified as confidential or that should reasonably be understood to be confidential given the nature of the information and the circumstances of disclosure, including business, technical, security, pricing, and product information. Confidential Information does not include information that (i) is or becomes public through no breach of the Agreement; (ii) was known to the Receiving Party without duty of confidentiality before disclosure; (iii) is independently developed without use of the Disclosing Party's information; or (iv) is rightfully received from a third party without duty of confidentiality.

20.2. **Use and Care.** The Receiving Party will use Confidential Information only to perform under the Agreement, protect it with at least reasonable care, and limit access to its employees, contractors, professional advisers, and permitted subcontractors who have a need to know and are bound by confidentiality obligations no less protective than this Section. The Receiving Party remains responsible for their compliance.

20.3. **Non-Disclosure.** The Receiving Party will not disclose Confidential Information to any other third party without the Disclosing Party's prior written consent.

20.4. **Compelled Disclosure.** If the Receiving Party is legally required to disclose Confidential Information, it will (where lawful) promptly notify the Disclosing Party and reasonably cooperate to seek protective treatment. Only the portion legally required may be disclosed.

20.5. **Return/Destruction.** Upon written request or upon termination, the Receiving Party will return or destroy Confidential Information (and confirm destruction in writing), except that the Receiving Party may retain (i) copies in routine backups that are not readily accessible and will be destroyed on the normal retention cycle, and (ii) copies required for legal or compliance purposes. Retained copies remain subject to this Section.

20.6. **Duration.** These confidentiality obligations apply during the term and for three (3) years after termination; trade secrets are protected for as long as they remain trade secrets under applicable law.

20.7. **Customer Personal Data.** For Customer Personal Data, the DPA (Annex A) governs. In case of conflict between this Section and the DPA regarding Customer Personal Data, the DPA controls.

21. Indemnification

21.1. **Intellectual Property Claims (targeted to the Service).** The Provider will defend the Customer against any third-party claim alleging that the Service, when used as permitted and in accordance with the Documentation, infringes a patent, copyright, or trademark, and will pay amounts finally awarded (or agreed in settlement).

21.2. **Provider Remedy.** If such a claim arises, Provider may, at its option and expense: (i) modify the Service to be non-infringing while substantially preserving functionality; or (ii) replace the impacted functionality with a non-infringing equivalent. If Provider cannot achieve (i) or (ii) within 30 days after Customer's written notice of the claim (the "Cure Period"), Provider may terminate the affected subscription(s) and issue a pro-rata credit of prepaid license fees for the unused portion of the affected subscription term. The credit will be applied to future invoices; no cash refund. Credits exclude professional-services fees, usage/transaction charges, taxes, and pass-through costs, and constitute Customer's sole monetary remedy for the covered IP claim, subject to the Section 22 Limitation of Liability.

21.3. **Excluded claims.** The Provider has no obligation for claims to the extent arising from: (i) Customer Data (including product information, labels, recipes, images, and messaging content); (ii) combinations with External Systems or items not provided by the Provider (including Customer-managed webshops, POS, ERP, iPaaS, or networks); (iii) unauthorized modifications by the Customer; or (iv) use of other than a current version the Provider makes available.

21.4. **Limited liability. Customer responsibility.** This Section states the Customer's exclusive remedy for third-party IP infringement claims relating to the Service and is subject to Section 22 Limitation of Liability. As a condition of the foregoing obligations, the Customer will promptly implement any modifications, replacements, or workarounds provided by the Provider.

21.5. **Customer Indemnity.** The Customer will indemnify and hold harmless the Provider and its affiliates, officers, and personnel from and against third-party claims, damages, fines, and reasonable costs (including legal fees) to the extent arising from: (i) Customer Data (including product information, labels, recipes, images, and messaging content); (ii) the Customer's use of the Service in violation of these Terms or applicable law; (iii) use or combinations with External Systems or items not provided by the Provider; or (iv) Trading Partner or other commercial disputes between the Customer and third parties, or (v) Customer's use or republication of third-party/supplier data (including FDP data) without adequate validation or where required notices are omitted. This indemnity does not apply to the extent the claim is caused by the Provider's breach of these Terms.

21.6. **Procedures.** The indemnified Party must promptly notify the indemnifying Party of the claim, grant the indemnifying Party sole control of the defense and settlement, and reasonably cooperate (at the indemnifying Party's expense). The indemnifying Party will not settle a claim that imposes non-monetary obligations on, or admits fault of, the indemnified Party without its prior written consent (not unreasonably withheld).

22. Limitation of Liability

22.1. **Service AS IS.** To the maximum extent permitted by law and except as expressly stated, the Service is provided “AS IS” and “AS AVAILABLE”. The Provider makes no warranties, whether express, implied, or statutory, including any warranties of merchantability, fitness for a particular purpose, or non-infringement. The Provider does not warrant that the Service will be uninterrupted, timely, secure, error-free, or that results will be accurate or complete.

22.2. **Guidance Only (Decision-Support Outputs).** Any information, recommendations, forecasts, optimizations, costings, calculations, reports, or other decision-support outputs generated by the Service are for guidance only. Such outputs depend on Customer Data and configurations and, where applicable, data received from External Systems or other third-party sources. The Provider does not warrant the accuracy, completeness, or suitability of any output where underlying inputs, mappings, configurations, models, or third-party data are incomplete, inaccurate, unavailable, stale, or changed. The Customer remains solely responsible for reviewing and validating outputs before use in operations, commercial decisions, or compliance workflows.

22.3. **Local Law**. Provider makes no representation that the Service complies with local laws. Customer is solely responsible for determining the Service’s suitability for its legal and regulatory obligations in the jurisdictions where it operates. If the Service is not a fit, Customer should not sign up or should obtain a written addendum that explicitly addresses those requirements.

22.4. **Unauthorized Access Caused by Customer.** To the extent permitted by law, Provider is not liable for losses arising from unauthorized use of Customer’s Account resulting from Customer’s failure to safeguard credentials or to give timely notice under §4.13 Compromise Notification. Customer is responsible for reasonable, direct costs attributable to such failure (e.g., re-provisioning, usage charges), except where Provider’s gross negligence or willful misconduct was the proximate cause.

22.5. **Allocation**. Without limiting the foregoing, the Provider will not be liable for losses arising from the Customer’s failure to perform its obligations.

22.6. **Third-party data.** To the extent permitted by law, the Provider has no liability arising out of or relating to (i) third-party or supplier-provided data (including FDP data) made available through the Service, or (ii) Customer’s reliance on such data, except where the Provider’s gross negligence or willful misconduct is the proximate cause.

22.7. **Applicability.** The limitations and exclusions in this Section apply in the aggregate across the entire Agreement and any incorporated documents, including the DPA, and govern all claims arising out of or relating to processing of Customer Personal Data, to the maximum extent permitted by law.

22.8. **Single global cap.** To the maximum extent permitted by law, the aggregate liability of the Provider and its Affiliates arising out of or related to the Agreement and DPA (including data-protection claims and personal-data breaches), whether in contract, tort, or otherwise, shall not exceed the lesser of (i) NOK 100,000 (excluding VAT), or (ii) the fees paid or payable by the Customer for the Service in the twelve (12) months immediately preceding the first event giving rise to liability. Where a Group Order applies, the ‘Aggregated Liability Cap (Group)’ in Group Customers & Participating Affiliates governs and replaces the per-Customer cap for the Master Customer and its Participating Affiliates.

22.9. **Claims Period.** Any claim must be brought within twelve (12) months after the cause of action accrues, or it is permanently barred.

22.10. **Regulatory fines.** Provider is not liable for fines imposed on Customer by a supervisory authority, except to the extent such liability cannot be limited under mandatory law.

22.11. **Exclusions.** To the fullest extent permitted by law, neither the Provider nor its affiliates, licensors, or service providers will be liable for any indirect, incidental, special, consequential, punitive, or exemplary damages, or for any loss of profits, revenue, goodwill, or data, arising out of or relating to the Agreement or the Service, even if advised of the possibility of such damages. Without limiting the foregoing, the Provider does not warrant uninterrupted or error-free operation and will not be liable for outages or failures of the public internet, access networks, or third-party hosting or access-point providers, or other events outside the Provider's reasonable control.

23. Changes to the Service or Terms

23.1. **Changes.** The Provider may improve or modify the Service. It may also update these Terms. For Material Changes, the Provider will provide 30 days' notice using the methods described under §26.8 Delivery Methods. Non-Material Updates (clarifications, administrative edits, security, performance, or legally required updates) that do not materially disadvantage Customer may take effect on posting without advance notice.

23.2. **Acceptance by Continued Use.** Continued use of the Service after the effective date stated in the notice under §23.1 constitutes acceptance of the applicable change.

23.3. **Objection to a Material Change.** If the Customer objects to a Material Change (as defined in §23.4) that materially and adversely affects the Customer, the Customer may terminate the affected subscription(s) only by giving written notice before the change takes effect, using the delivery methods in §26.8. For clarity, Emergency Changes (§23.4) and Sub-processor/vendor changes (§23.5) are not Material Changes and do not give rise to this termination right.

23.4. **Material Change.**

a) A "**Service Material Change**" is a service change that permanently removes or substantially degrades a core capability of the Customer's subscribed plan as a whole without a functionally equivalent alternative available in the same plan tier. For clarity, the following are *not* Service Material Changes: (i) changes to infrastructure or subcontractors (including Sub-processors) without net loss of security or compliance posture; (ii) security, stability, or performance improvements; (iii) deprecation of beta/preview features; (iv) changes required by law or by a third-party platform/provider; and (v) disabling only the Affected Processing under the DPA Section 7 in response to the Customer's Sub-processor objection.

b) A "**Terms Material Change**" means a change to these Terms that (i) reduces a Customer's contractual rights or remedies in a non-trivial way, (ii) imposes new material obligations, or (iii) expands Provider's rights to Customer Data beyond what was previously permitted. Administrative, clarifying, or legally required updates that do not materially disadvantage Customer are not Terms Material Changes.

23.5. **Emergency Changes.** Notwithstanding §23.1 to §23.3, Provider may implement emergency changes to address a security vulnerability, service integrity/stability/availability risk, abuse/fraud, or a change required by law or a third-party platform/provider that necessitates immediate action ("**Emergency Changes**"). Emergency Changes may be deployed without

prior notice; Provider will give post-implementation notice via the §26.8 Delivery Methods where commercially reasonable. An Emergency Change is not a Material Change.

23.6. **Sub-processors and other vendors.** Provider may appoint, replace, or remove sub-processors and other third-party vendors. For Controller Personal Data, the DPA (Annex A) governs notice and objections; a change of sub-processor is not a Material Change to the Service and Customer's sole remedies are those in the DPA. For Operational Data (controller-side) and for vendors processing non-personal data, Provider may change vendors at any time; such changes are not Material Changes and do not give rise to termination, refunds, or credits.

24. Marketing References

24.1. **Marketing References.** Unless Customer notifies Provider otherwise, Customer grants Provider a limited, non-exclusive, royalty-free, revocable license to use Customer's name and logo solely to identify Customer as a user of the Service in Provider's websites, slide decks, and similar customer lists. No further rights are granted; use will follow any reasonable brand-use guidelines provided by Customer. Customer may opt out at any time by written notice, and Provider will cease new uses and remove reasonable online references within 30 days of receipt (archival materials excluded).

25. Governing Law and Venue

25.1. **Governing Law.** This Agreement is governed by the laws of Norway, without regard to conflict-of-law rules.

25.2. **Venue.** Any dispute arising out of or in connection with this Agreement shall be brought before the Oslo District Court (Oslo tingrett), Norway.

26. Miscellaneous

26.1. **Force Majeure.** Neither Party is liable for delays or failures caused by events beyond its reasonable control.

26.2. **Assignment.** Either Party may assign the Agreement in connection with a merger, acquisition, or sale of substantially all assets, with notice; otherwise, assignment requires the other Party's consent (not unreasonably withheld).

26.3. **Relationship of the Parties.** The Parties are independent contractors. Nothing in these Terms creates a partnership, joint venture, franchise, agency, fiduciary, single-employer or joint-employer relationship. Neither Party has authority to bind the other or incur obligations on the other's behalf. No exclusive relationship is created by these Terms.

26.4. **Subcontractors.** The Provider may use subcontractors; for personal-data processing, sub-processors are governed by the DPA.

26.5. **Electronic Signatures.** Creating or being provisioned with a Customer Account, clicking "I agree" (or similar), or using the Service constitutes the Customer's **electronic signature** and agreement to these Terms. Electronic signatures and records satisfy "in writing" and signature requirements.

26.6. **Records and Logs.** The Provider's system logs, billing records, and usage data constitute prima facie evidence of use and charges unless disproved by credible evidence.

26.7. **Cookies and Similar Technologies.** Provider uses cookies and similar technologies. Non-essential cookies are used based on consent; details are in the cookie notice referenced by the Privacy Policy.

26.8. **Delivery Methods.** The Provider may deliver notices by: (i) email to the contacts on file; (ii) in-product messages or dashboard banners; (iii) postings on the Provider's website/Documentation; or (iv) physical mail to the Customer's address on file. SMS/text may be used for account/security verification and critical alerts; standard carrier charges may apply.

26.9. **Deemed Receipt.** Notices are deemed received 24 hours after posting or emailing, or upon delivery confirmation for physical mail, unless a bounce-back or similar error indicates non-delivery.

26.10. **Requirements.** The Customer needs internet access and a modern browser to receive electronic notices.

26.11. **Withdrawal.** Electronic delivery is integral to the Service. A Customer that does not agree to electronic notices must terminate the Customer Account.

26.12. **Third-Party Links.** The Service and Documentation may reference or link to third-party sites or materials. The Provider does not control and is not responsible for such third-party content; access is at the Customer's own risk and does not imply endorsement.

26.13. **Export Controls and Sanctions.** The Customer will not use, export, re-export, or transfer the Service in violation of applicable export control or sanctions laws. The Customer represents it is not listed on, or owned/controlled by a party listed on, any applicable sanctions list and will not permit access to the Service from embargoed territories in breach of law.

26.14. **Severability; Waiver.** If a provision is unenforceable, it will be modified to the minimum extent necessary; others remain in effect. Failure to enforce any provision is not a waiver. Any waiver must be in writing and signed by the waiving Party and is effective only for the specific instance and purpose given.

26.15. **Entire Agreement.** The Agreement (these Terms, the DPA, and any Order or SOW) is the Parties' entire agreement and supersedes prior terms on the same subject.

Annex A — Data Processing Agreement (DPA)

This DPA forms part of the Agreement between **Foodsoft AS (MyFoodOffice)** ("**Processor**") and the **Customer** identified in the applicable Order or ToS ("**Controller**").

1. Scope, duration, and roles

1.1. **Applicable Law.** This Data Processing Agreement is intended to meet the requirements of Article 28 of Regulation (EU) 2016/679 (the “GDPR”), as implemented in Norway through the Personal Data Act of 15 June 2018 (Personopplysningsloven) and the EEA Agreement (together, “Data Protection Laws”). Where relevant to the Processing and expressly agreed by the Parties in a signed addendum, references to GDPR include the UK GDPR and/or the Swiss Federal Act on Data Protection (FADP).

1.2. **No other regimes.** Except as expressly agreed in a signed addendum, the Processor does not undertake to comply with any other local or sector-specific privacy regimes, certification frameworks, or data-residency mandates. The Controller remains solely responsible for determining the Service’s suitability for its own legal and regulatory obligations in the jurisdictions where it operates. Nothing herein limits either Party’s compliance with mandatory law that applies to it.

1.3. **Data Scope.** This DPA applies only to Controller Personal Data that Processor processes on Controller’s documented instructions under the Agreement. It does not apply to e.g. Customer Non-Personal Data or Operational Data processed by Provider as controller which are governed by the Agreement and Privacy Policy.

1.4. **Subject matter**. Processor processes Controller Personal Data to provide the cloud Services described in the Agreement (e.g., ordering flows, ERP features, regulatory/labeling tools, integrations).

1.5. **Duration**. This DPA applies for the Term of the Agreement and any wind-down period described herein.

1.6. **Roles**. Controller is the controller and Processor is the processor for the Processing of Controller Personal Data under this DPA. For clarity, the Parties do not act as joint controllers under GDPR Article 26 for the Processing under this DPA.

1.7. **Master Customer and Participating Affiliates.** Where an Order names multiple controllers (Master Customer and Participating Affiliates), Processor acts for each named controller with respect to its own Customer Account; Parties are not joint controllers.

2. Definitions

Personal Data	any information relating to an identified or identifiable natural person (“data subject”). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
Controller Personal Data	Personal Data processed by Processor on Controller’s documented instructions.
Non-Personal Data	means data that is not personal data, including without limitation product and ingredient records, recipes/formulations, SKUs, BOMs, labels and artwork, pricing, catalog content, operational settings, production/route plans, and other business records uploaded or configured by Customer.

Sub-processor	a processor engaged by Processor to carry out specific Processing activities.
Sub-processor Roster	the non-public list of third-party processors engaged by the Processor, available from the Processor upon request under a duty of confidentiality.
Change Notice	a written notice of an intended addition or replacement of a Sub-processor, including name, role, processing location(s), and the nature of processing.
Affected Processing	the specific Processing operations performed by the Provider (and, where applicable, its Sub-processors) on Controller Personal Data that must be suspended, modified, or discontinued as a **direct** result of: (i) Customer's substantiated objection to a Sub-processor under DPA Section 7; (ii) a binding legal or regulatory restriction; (iii) the Provider's incident response to a security incident; or (iv) an Emergency Change needed for security, stability, or availability—**and only to the minimum extent necessary** to address the triggering event. For clarity, Affected Processing does **not** include: (a) unrelated Processing activities; (b) ancillary services such as support, billing, or account administration; or (c) Processing that can reasonably continue through alternative technical or organizational measures.

3. Interpretation; Order of Precedence; Updates

3.1. **Interpretation**. Capitalized terms have the meanings above. Capitalized terms not defined here have the meanings given in the Agreement or, if not defined there, in GDPR. "Including" means "including without limitation". Headings are for convenience only.

3.2. **Precedence.** In case of conflict, this DPA controls over the Agreement **solely** for personal-data Processing; otherwise, the Agreement prevails.

3.3. **Updates.** Processor may update this DPA to reflect legal or operational changes necessary for compliance. Material changes will be notified via the methods in the Agreement and become effective as stated there.

4. Processing on documented instructions

4.1. **Sources of instructions (limited).** Processor will process Controller Personal Data **only** on Controller's documented instructions, which are limited to: (i) the Agreement and this DPA; (ii) configurations and selections made by Controller within the Service; and (iii) written directions that Processor **expressly accepts in writing**.

4.2. **Permitted operational processing.** Processing also includes what is necessary for Processor to (a) provide and support the Services, (b) maintain security and availability, and (c) comply with applicable law.

4.3. **Inconsistencies; order of precedence.** If any Controller instruction conflicts with the Agreement or this DPA, the order of precedence in §3.2 applies. Service configurations under

§4.1(ii) control over ad-hoc written directions under §4.1(iii) unless Processor agrees otherwise in writing.

4.4. **Lawfulness and feasibility.** Where an instruction is **unlawful**, **infeasible**, or would create a security/integrity risk or disproportionate burden, Processor may decline or suspend the instruction (unless prohibited by law) and will notify Controller where reasonably practicable.

4.5. **Custom changes and costs.** Processor has **no obligation** to create custom configurations, disable sub-features, modify workflows, or implement workarounds to follow an instruction. Any such change, if Processor elects to do it, requires mutual written agreement and is chargeable on a time-and-materials basis in accordance with the **Costs & Payments** Section.

4.6. **Controller responsibilities.** Controller is solely responsible for the **lawfulness** of its instructions (including having a valid legal basis and transparency toward data subjects) and for the accuracy of configurations and data it provides. Processor may rely on Controller's configurations and accepted written directions as the complete and final instructions.

4.7. **Trading Partners; transmissions.** Controller instructs Processor to transmit, route, and make available Controller Personal Data to Trading Partners and other recipients designated by Controller via the Services (including through supported networks and integrations). Processor acts solely as Processor for these transmissions. Upon receipt, each Trading Partner acts as an independent controller for the data it receives; Processor is not a joint controller with Controller or any Trading Partner. Controller is solely responsible for (i) identifying and authorizing recipients, (ii) having a lawful basis and required transparency for disclosures to them, and (iii) any contractual or statutory obligations between Controller and its Trading Partners.

4.8. **Remote Access by Customer Users.** Customer may permit End Users outside the EEA to remotely access data hosted in the EEA. Such access occurs under Customer's control and constitutes Customer's own cross-border disclosure. Customer-initiated remote access or disclosures are Controller's own transfers, and Controller is responsible for related notices, assessments, and lawful bases. This does not make Processor a data exporter for those Customer-initiated disclosures.

4.9. **No duty to monitor.** Processor is not required to monitor Controller's compliance with Data Protection Laws or to detect unlawful instructions; Processor's role is limited to executing documented instructions per this Section 4.

4.10. **Legal compulsion and emergencies.** Processor may process Controller Personal Data as reasonably necessary to comply with a binding legal obligation or to address an urgent security/availability incident affecting the Service; Processor will limit such processing to what is necessary and notify Controller where legally permitted.

4.11. **Documentation.** Processor may maintain logs or tickets evidencing instructions received and actions taken under this Section 4 and may use such records to demonstrate compliance with Article 28(3)(a) GDPR.

5. Confidentiality

5.1. **Confidentiality**. Processor ensures persons authorized to process Controller Personal Data are bound by confidentiality and receive appropriate privacy/security training.

6. Security

6.1. Processor will implement appropriate technical and organizational measures as required by GDPR Article 32, considering the state of the art, costs, and risks.

6.2. The Processor has deployed a set of security measures, including (non-exhaustive); Access control & authentication, Data in transit & at rest, Logging & monitoring, Vulnerability & patch management, Incident response, Business continuity & backups, Change management, Personnel security & training, Physical & cloud security (rely on cloud provider controls; data segregation & tenancy (logical isolation between customers), Supplier/Sub-processor security.

6.3. Processor may update the measures from time to time to reflect improvements or changed risks, provided the overall security level is not, in Processor's reasonable judgment, materially degraded.

7. Sub-processors (general authorization; limited remedies)

7.1. **General authorization.** The Controller grants the Processor a general authorisation to engage Sub-processors in connection with the Services, subject to this DPA Section 7.

7.2. **Flow-down & responsibility.** Processor will impose Article 28(3) obligations on Sub-processors and remains responsible for their performance as required by Article 28(4).

7.3. **Non-public roster.** The Processor maintains a Sub-processor Roster. The Processor will provide the Roster to the Controller upon request, and the Controller must treat it as Confidential Information.

7.4. **Change Notice.** The Processor will provide a Change Notice for any intended addition or replacement of a Sub-processor at least 30 calendar days before the change takes effect (urgent security or continuity needs excepted per §7.8). Change Notices will be sent via email notice to Controller's admin contact(s).

7.5. **Objections.** Controller may object only with a specific, documented data-protection risk (not commercial, performance, or location preferences) by written notice within ten (10) days of the date notice is given. Non-specific objections are deemed withdrawn. For clarity, commercial preferences, performance considerations, or data-location preferences are not reasonable grounds for objection.

7.6. **No configuration obligation.** Processor has no obligation to create custom configurations, disable sub-features, or implement workarounds in response to a Controller's objection where doing so would introduce disproportionate burden, security or integrity risk, or material technical complexity.

7.7. **Remedy.** If Controller validly objects under DPA Section 7 and no reasonable alternative is available, Controller's **sole and exclusive remedy** is:

(a) Separable item: where the affected Processing is expressly identified as a separate, itemized service in the applicable Order, to give written notice to terminate that specific item only.

(b) Non-separable bundle: where the affected Processing forms part of a bundled, non-itemized plan, the Service is not separable and no partial termination or fee adjustment is

available. Controller may cease using the affected functionality, but the plan and fees remain unchanged for the Term.

7.8. **Emergency engagement.** Where an urgent engagement/replacement is necessary to preserve security or service continuity, the Processor may appoint a Sub-processor without prior notice, provided it gives the Controller a Change Notice without undue delay and offers the objection/termination options in §§7.5–7.7 (and §7.9 for timing/fees).

7.9. **Timing and fees.** Any permitted termination under this Section is effective on the earlier of (i) the end of the then-current billing period for the affected item, or (ii) the date specified by Processor (not earlier than 30 days after notice), in all cases without refunds, credits, or damages. Controller remains liable for all fees accrued through the effective date. Any notice of termination under this Section must be given within the same ten (10) day objection window unless Processor agrees in writing to extend for documented regulatory reasons.

7.10. **Pricing Consequence.** Where the Affected Processing is part of a bundled, non-itemized plan, disabling Affected Processing does not change plan fees and does not entitle Controller to refunds, credits, offsets, or early termination rights under the Agreement.

7.11. **Provider option.** Where technically feasible and at its discretion, Processor may recommend a configuration to avoid the affected Processing. Acceptance is optional; declining does not expand Controller's remedies. Any optional configuration or migration actions that Processor elects to perform in connection with a Controller objection are chargeable in accordance with Section 16, and may require reasonable downtime windows.

7.12. **No broader termination.** For clarity, no change of Sub-processor entitles Controller to terminate the Agreement or any non-affected Services.

8. Third-Party Processing; Responsibility Boundaries

8.1. **Customer-managed processors & services.** Where Controller elects to connect the Services to any External System or engages its own processors (e.g., iPaaS, ERP, POS, networks), Controller is solely responsible for (i) selecting, contracting with, and supervising such third parties; (ii) ensuring an Article 28-compliant DPA is in place with them; and (iii) their security, availability, data quality, and compliance. Processor is not responsible for any act/omission of such third parties and is not their sub-processor.

8.2. **Trading Partners as independent controllers.** Personal data disclosed or made available by Controller to Trading Partners via the Services is received by those Trading Partners as independent controllers. Processor is not a joint controller with Controller or any Trading Partner and has no obligations toward them under this DPA. Controller is solely responsible for lawful basis, transparency, and any contract terms with Trading Partners.

8.3. **Customer-initiated disclosures & remote access.** Disclosures initiated or authorized by Controller (including remote access by users outside the EEA/UK/CH, or by Trading Partners) occur under Controller's control and constitute Controller's own transfer/disclosure. Processor is not the exporter for those disclosures and has no obligation to assess or implement transfer tools for them.

8.4. **No back-to-back obligations.** Except for Processor's own Sub-processors under DPA Section 7, Processor has no obligation to "flow down" this DPA to, or audit, third parties contracted by Controller, nor to implement configurations or workarounds to meet third-party preferences (location, formats, bespoke security), unless separately agreed in writing (Professional Service).

8.5. **Data ingress from third parties.** Where data is imported from third parties at Controller's direction (including supplier/FDP data), Controller is responsible for the lawfulness of the source, accuracy, and any notices required. Processor processes such data as Controller's Processor and does not verify third-party content.

8.6. **No duty to monitor third parties.** Processor has no duty to monitor Controller's or any third party's compliance. Processor's obligations are limited to the Services and its Sub-processors.

8.7. **Cooperation scope.** Any assistance Processor provides in relation to Controller's third parties is out of scope and chargeable under Section 16 (Costs & Payments).

9. Assistance to Controller

9.1. **Data subject requests.** Taking into account the nature of Processing, Processor will assist Controller with appropriate technical and organizational measures, insofar as possible, to respond to requests under Chapter III GDPR.

9.2. **Security; DPIA.** Processor will provide information reasonably necessary for Controller's security obligations and DPIA/consultation duties (Articles 32–36), limited to Processor's Processing.

9.3. **Litigation/regulatory support.** Upon Controller's written request, Processor will reasonably assist with preservation, search, review, export, or production of Controller Personal Data needed for disputes or regulatory proceedings.

9.4. **Costs.** Assistance is chargeable, in accordance with Section 16 (Costs & Payments).

10. Personal Data Breaches

10.1. **Definition.** "Personal data breach" has the meaning in GDPR Article 4(12).

10.2. **Notice to Controller.** Processor will notify Controller after becoming aware of a personal data breach affecting Controller Personal Data. Initial notice may be followed by updates as information becomes available.

10.3. **Content of notice.** Processor will share information reasonably available to it to support Controller's Articles 33–34 obligations, which may include: a summary of the incident, known scope and likely effects, measures taken or proposed, and a contact point.

10.4. **Scope exclusions.** This Section does not apply to incidents in systems owned or controlled by Controller or in External Systems.

10.5. **Cooperation & costs.** Assistance beyond initial notice and factual information reasonably available to Processor (e.g., Controller-specific notification drafting, regulatory liaison at Controller's request, call-center/credit-monitoring arrangements) is chargeable in accordance with Section 16.

10.6. **No admission; coordinated communications.** Any breach notifications or disclosures by Processor are not an admission of fault or liability. Public statements referencing Processor's systems must be coordinated with Processor where reasonably practicable.

10.7. **Records.** Processor will document personal data breaches as required by GDPR Article 33(5).

11. International transfers

11.1. **Processing locations.** Processor may process Controller Personal Data in any country where Processor or its Sub-processors maintain facilities, subject to this Section 11.

11.2. **No data-residency commitment.** Unless required by mandatory law, Processor does not commit to store, host, or process Controller Personal Data in any particular country or region. Processor may transfer, route, or replicate Controller Personal Data (including backups, logs, and support artifacts) across locations where Processor or its Sub-processors operate, subject to this Section 11. Preferences regarding data location do not constitute a valid objection under §7.5.

11.3. **Transfer mechanisms.** For transfers of Controller Personal Data outside the EEA/UK/Switzerland, Processor will ensure an appropriate transfer mechanism applies (e.g., EU Standard Contractual Clauses (SCCs), UK IDTA/Addendum, or other valid tool).

11.4. **Regionalization.** Where commercially and technically feasible, Processor will prefer EU regions for hosting primary data stores for the production environment of the Services. This is not a data-residency commitment and does not restrict support operations, redundancy, or processing by Sub-processors per §11.2–11.3

11.5. **Standard tools only.** Processor has no obligation to execute Controller-drafted transfer clauses or bespoke supplemental measures. Processor's standard transfer tools and documentation apply.

11.6. **Precedence.** To the extent of conflict between this DPA and the applicable SCCs/IDTA, the SCCs/IDTA prevail (including governing law and jurisdiction).

11.7. **Notification.** Processor may select, switch, and update the applicable transfer tool (including SCCs Modules) in its discretion to address legal or operational changes, without prior notice unless required by law or the transfer tool itself.

11.8. **Agency for execution.** Processor is authorized to execute, as agent for Controller solely for this purpose, SCCs/IDTA (and ancillary documents) with Sub-processors as needed to support the Services.

11.9. **Documentation & supplemental measures.** Processor will provide standard transfer-impact assessment materials and documentation as part of its compliance materials. Any Controller-specific assessments, bespoke questionnaires, workshops, or supplemental measures beyond Processor's standard approach are subject to availability and billed time-and-materials under Section 16, with commercially reasonable timelines and no service-level commitments.

11.10. **Changes in law.** Processor may update the chosen transfer mechanism or implement supplementary measures to reflect legal changes without this constituting a material change to the Services or giving rise to refunds, credits, or additional termination rights.

11.11. **Refunds.** Selection or update of a transfer tool, or changes to Sub-processor locations, do not create termination, refund, credit, offset, or fee-adjustment rights, except as expressly set out in DPA Section 7.

11.12. **Records.** Processor will keep records of executed transfer tools and make high-level evidence available through its Compliance Materials; Processor is not obliged to provide copies of underlying Sub-processor agreements.

11.13. **Trading-Partner access/exports.** Cross-border disclosures by Controller to its Trading Partners (or remote access by them) occur under Controller's control and constitute Controller's own transfer; Processor is not the exporter for those disclosures. Controller remains responsible for any transfer assessments and notices vis-à-vis its Trading Partners.

12. Return and Deletion

12.1. **Export window.** Upon expiry or termination of the applicable Services, and on Controller's written request made within 30 days, Processor will make available an export of Controller Personal Data within a commercially reasonable period.

12.2. **Format (Processor-determined).** Exports will be provided in a commonly used, machine-readable format supported by the Service and determined by Processor (such as CSV and/or JSON with reasonable field descriptions). Processor is not obliged to create custom exports, mappings, or transformations; any non-standard assistance is available on a time-and-materials basis.

12.3. **Secure delivery.** Exports will be delivered via a secure transfer method designated by Processor (e.g., authenticated download or SFTP). Any third-party secure-transfer or storage fees are pass-through in accordance with Section 16.

12.4. **Deletion timeline.** After the 30-day export window—or earlier at Controller's written instruction—Processor will delete or irreversibly anonymize Controller Personal Data from active systems, aligned with the data-deletion timelines in the Agreement, subject to:

a) **Backups/archival.** Data in backup media will be overwritten on the regular rotation. Processor is not required to restore or delete individual records from backups except when restoring for disaster recovery; and

b) **Legal hold/claims.** To the extent retention is required by law or reasonably necessary for the establishment, exercise, or defense of legal claims. Retained copies remain subject to this DPA.

12.5. **Scope/exclusions.** This Section applies to Controller Personal Data stored in the Service. It excludes Processor's system logs, security/audit logs, derived or aggregated metrics, and de-identified data, which Processor may retain and use per the Agreement.

12.6. **Confirmation (on request).** Upon completion of actions under §12.4, Processor will, on Controller's written request, provide a brief written confirmation that deletion/anonymization of active systems has been completed in accordance with this Section.

12.7. **Controller choice & silence.** Controller may choose return and/or deletion. If Controller does not submit a request under §12.1 within 30 days, Processor may proceed with deletion under §12.4 and is not obliged to retain data beyond its standard schedules.

13. Information and audits

13.1. **Reports-first compliance.** Upon Controller's request, Processor will make available information reasonably necessary to demonstrate compliance with Article 28(3)(h) GDPR,

primarily via: (i) security and privacy summaries; (ii) responses to industry-standard security questionnaires; (iii) third-party assurance reports and/or certifications (if any); (iv) data-protection "evidence pack" (together, the "**Compliance Materials**").

13.2. **On-site audits excluded.** On-site audits or inspections are not permitted, unless an addendum signed by both Parties explicitly approve so. Audits are limited to review of the Compliance Materials and a reasonable remote Q&A session.

13.3. **Last-resort trigger (where on-site is pre-approved).** Where an on-site audit right exists, an on-site visit may occur only if the Compliance Materials and remote Q&A are objectively insufficient to verify Processor's compliance for Controller's Processing and the Parties have attempted in good faith to resolve the gaps remotely.

13.4. **Frequency & notice.**

a) **Remote review:** at most once in any rolling twenty-four (24) month period with 60 days' prior written notice and a written audit plan.

b) **On-site (if pre-approved):** at most once in any rolling thirty-six (36) month period, with 60 days' prior written notice, limited to one business day on site.

c) **Regulatory/urgent exception:** Shorter notice is permitted only if required by a competent supervisory authority's written demand specifically naming Controller's data at Processor, or in case of a suspected material breach affecting Controller Personal Data that Processor has not addressed after written notice.

13.5. **Scope limitations.** All audits (remote or on-site):

a) cover only Processor's controls relevant to the Processing of Controller Personal Data under the Agreement;

b) do not grant direct access to Processor's underlying shared/multi-tenant infrastructure or configurations in a way that could expose other customers' environments; instead, Processor will provide tenant-scoped or redacted evidence (e.g., screenshots, config exports, tickets, policies/procedures, and sampled logs) sufficient to verify applicable controls;

c) exclude other customers' data, trade secrets, source code, cryptographic material (e.g., private keys), cloud-provider premises, raw vulnerability scan outputs, and pricing or non-security commercial information;

d) use sampling and read-only evidence review (no production data exfiltration);

e) occur during normal business hours, without undue disruption, and follow Processor's site/security rules;

f) exclude active testing (including penetration testing, vulnerability scanning, load/stress testing, social-engineering or phishing) unless separately agreed in writing by Processor;

g) produce findings that reference only Controller's context and avoid disclosure of Processor's confidential information unrelated to compliance.

13.6. **Pooled/independent audits.** Processor may satisfy audit requests via a pooled audit or independent third-party assessment covering substantially similar controls. If a pooled audit report addresses the audit plan's objectives, it fulfills Processor's audit obligation for that cycle.

13.7. **Auditor requirements.** The auditor must be (i) independent and appropriately qualified in information security and privacy, (ii) not a competitor of Processor or its affiliates, (iii) bound by a written NDA acceptable to Processor, and (iv) compliant with Processor's access, HSE, and confidentiality policies. Processor may reasonably object to an auditor who fails these criteria; Controller will nominate an alternative.

13.8. **Audit NDA.** Controller will execute Processor's audit/engagement NDA.

13.9. **Audit plan & conduct.** At least 30 days before any audit work begins, Controller will provide an audit plan describing objectives, scope, requested documents, and testing methods aligned to recognized frameworks. The Parties will refine the plan to minimize burden and protect confidentiality.

13.10. **Output & remediation.** The auditor will provide Processor with a copy of the draft findings. Final reports are Processor-confidential and may be used by Controller solely to meet its GDPR obligations. Where the audit identifies a material non-conformity with this DPA, the Parties will agree a timely and proportionate remediation plan. This clause does not create any service-credit or refund entitlement.

13.11. **No duplication.** If substantially the same controls were audited in the preceding 12 months (remote) or 36 months (on-site) and no material changes have occurred, Processor may satisfy the request by re-providing the most recent applicable report plus an attestation of no material adverse change.

13.12. **Reservation of rights.** Nothing in this Section requires Processor to disclose information that would: (i) compromise the security or privacy of other customers or the Service; (ii) breach law or third-party confidentiality; or (iii) reveal trade secrets or highly sensitive internal details where a summary or redacted form would suffice.

13.13. **Costs.** Audit costs, retainers, pass-throughs, and payment terms are governed by Section 16.

14. Data categories and restrictions

14.1. **Typical data subjects & categories.** Unless the Parties expressly agree otherwise in writing, Controller Personal Data processed under this DPA is limited to business-context data relating to End Users and Trading-Partner personnel, including: names, roles, business contact details, account identifiers, authentication/authorization data, order/transaction metadata, usage and event logs, IP addresses and device/browser information necessary for security, performance monitoring, troubleshooting, and in-app guidance; plus ticket metadata and attachments reasonably required for support. (See also Annex 1.)

14.2. **Telemetry, SDKs, and in-app guidance.** Where the Service employs performance/security telemetry or in-app guidance SDKs, Processor will limit collection to what is necessary to operate those features (e.g., user ID or business email (or hash), device/browser, IP, timestamps, event/error data). Controller will not configure or use such tooling to capture payload content unless strictly necessary for troubleshooting a specific issue and proportionate to the risk.

14.3. **Support and tickets (minimization).** Controller must avoid including payload content or unnecessary personal data in tickets, chat, or email to support. Where reproducing an issue, Controller will (a) redact extraneous personal data, (b) provide minimal logs or screenshots sufficient to explain the problem, and (c) refrain from sharing any categories prohibited by §14.4

14.4. **Special categories / minors.** Controller will not instruct Processing of special categories of data (GDPR Art. 9), criminal conviction/offence data (GDPR Art. 10), data relating to children, payment card primary account numbers (PANs) or full magnetic-stripe/CSC data, precise geolocation (fine-grained location enabling tracking of individuals), unless expressly agreed in a signed addendum specifying scope, safeguards, and lawful basis; otherwise such Processing is prohibited. Any contrary instructions are at Controller's risk to the maximum extent permitted by law.

14.5. **Minimization in common channels.** Controller will not include Prohibited Categories (§14.4) in (a) print jobs or document-relay features, (b) emails/notifications sent via the Service or its Sub-processors, or (c) tickets/logs/screenshots shared for support. Controller will redact payload content and share only data strictly necessary to reproduce or resolve issues.

14.6. **Exception path.** If Controller requires Processing of a Prohibited Category, the Parties will first execute a signed addendum specifying scope, lawful basis, additional safeguards, retention, and any transfer tools required under Section 11. Processing may begin only after signature.

14.7. **Enforcement.** If Processor reasonably determines an instruction would breach this Section 14, it may suspend only the Affected Processing and will notify Controller where practicable; remedies follow Sections 7 and 18.

15. Requests from public authorities

15.1. **Notification.** Processor will promptly notify Controller of any binding request for disclosure of Controller Personal Data by a public authority (unless legally prohibited) and limit disclosure to what is legally required.

15.2. **Costs.** Cooperation beyond initial notice and factual information reasonably available to Processor is chargeable in accordance with Section 16.

16. Costs & Payments

16.1. **Chargeable activities.** Except for activities expressly included in the Service, Controller will pay Processor on a time-and-materials basis for any out-of-scope privacy/security assistance. Chargeable activities include, without limitation:

a) assistance with data-subject requests, DPIAs, and consultations beyond Processor's standard documentation (Section 9);

b) audit activities beyond the provision of Compliance Materials, including remote Q&A and any permitted on-site work (Section 13);

c) support for inquiries, investigations, subpoenas, or other legally binding demands from public authorities relating to Controller Personal Data; preservation, search, review, export, or production of Controller Personal Data for legal holds, litigation, eDiscovery or regulatory proceedings (Section 15)

d) international-transfer formalities specific to Controller, including transfer impact assessments and Controller-requested supplemental measures that exceed Processor's standard approach (Section 11);

e) configuration changes, workarounds, data migrations, or feature disablement that Processor elects to perform in connection with a Sub-processor objection (DPA Section 7);

f) any other Controller-requested Professional Services related to this DPA.

16.2. **Rates and pass-throughs.** Billable work is charged at Processor's then-current professional-services rates, in 0.5-hour increments, plus reasonable expenses and pass-through third-party fees (e.g., secure-transfer, storage, Sub-processor or cloud provider charges).

16.3. **Retainers for audits/extended engagements.** As a condition to any audit activity (including remote Q&A beyond Compliance Materials) or any single engagement Processor estimates will exceed 2 hours, Controller will prepay a non-refundable retainer equal to the greater of 2 hours of Professional Services or Processor's written estimate for the scope, at then-current rates. Participation is contingent on cleared funds 10 business days before the scheduled start;

16.4. **Billing.** Time is drawn against the retainer. Overages are invoiced weekly.

16.5. **Cancellations/reschedules** within 10 business days of the start incur a **25%** cancellation fee.

16.6. **Payment terms (override).** Notwithstanding the Agreement's general payment terms, amounts invoiced under this Section 16 are due net 10 days from invoice date.

16.7. Taxes; no set-off. Fees are exclusive of taxes. Controller is responsible for applicable taxes. Amounts due under this Section 16 must be paid without set-off or counterclaim (as per the Agreement).

17. Limited Liability

17.1. **Liability.** The Section 22 Limitation of Liability in the Terms of Service applies to this DPA and to all Processing under it as if set out in full. Nothing in this DPA increases either Party's liability beyond the Agreement or creates additional remedies. For clarity, this includes the Agreement's aggregate cap across the Agreement and DPA, exclusions of indirect damages, and claim-period limits, subject to mandatory law.

17.2. **Regulatory fines.** Processor is not liable for fines imposed on Controller by a supervisory authority, except to the extent such liability cannot be limited under mandatory law.

17.3. **Carve out.** The above does not limit Controller's payment obligations under this DPA or the Agreement, nor does it restrict liability that cannot be limited under mandatory law.

18. Termination rights under this DPA

18.1. **Termination rights.** Except as expressly provided in §7.7 Remedy, this DPA does not grant additional termination rights.

18.2. **Refunds.** Any termination is limited to the specific Affected Processing, and does not entitle Controller to refunds, credits, or damages.

19. Governing law and venue

19.1. **Governing Law.** This DPA is governed by the laws of Norway, without regard to conflict-of-law rules, and without prejudice to mandatory data-protection rights.

19.2. **Venue.** Any dispute arising out of or in connection with this DPA shall be brought before the Oslo District Court (Oslo tingrett), Norway.

Annex A-1 — Details of Processing

A. **Subject matter and purpose.** Provision of the Services (ERP, B2B ordering, integrations, labeling tools, shared libraries, and related support/maintenance/security).

B. **Nature of Processing.** Collection, hosting, storage, retrieval, transmission, display, deletion, and other operations necessary to provide the Services and their integrations.

C. **Categories of data subjects.** Employees and representatives of Controller and its Trading Partners; end users authorized by Controller; recipients/contacts in order flows.

D. **Categories of personal data.** Identification and business contact data (name, role, email, phone, address); account identifiers; authentication/authorization data; transactional/order metadata; usage and event logs; optional message content required for order fulfillment; support tickets. *(No special categories unless expressly agreed.)*

E. **Sensitive data.** Not intended. Prohibited unless agreed per §14.4.

F. **Frequency.** Continuous for the Term.

G. **Retention.** As required for the Services and as configured by Controller; deletions per DPA Section 12.

H. **Controller obligations and rights.** As set out in the Agreement and this DPA, including providing lawful instructions and maintaining transparency/lawful basis with data subjects.

I. **Sub-processors.** General authorization; list available on request (DPA Section 7).

Annex B — Food Data Provider Addendum

1. **Scope.** This Addendum applies when a Customer acts as a Food Data Provider (“FDP”) and shares ingredient/product data (“FDP Data”) to the Service’s shared/global library for use by other Customers.

2. **Standards & Format.** The Provider may specify data standards and transport methods (e.g., GS1-aligned schemas, API/file layouts). The Provider will give at least **60 days’** notice before a materially changed standard takes effect, unless a shorter period is required by law or urgent security/fraud concerns.

3. **No Provider Warranty; “As Provided.”** FDP Data is published to the library **as provided by the FDP**. The Provider does not verify, audit, warrant, or guarantee the accuracy, completeness, conformance, or timeliness of FDP Data, and disclaims all warranties to consuming Customers regarding FDP Data to the maximum extent permitted by law.

4. **FDP Responsibilities (no Provider warranty).**
   (a) **Authority to Share.** FDP represents only that it has the right to supply FDP Data to the Provider for the purposes contemplated here and that doing so does not knowingly infringe third-party intellectual property rights or violate applicable law.
   (b) **Data Quality Goal (non-warranty).** FDP will use reasonable efforts to supply accurate and up-to-date data consistent with the applicable standard and its legal obligations. **This is not a warranty to the Provider or to other Customers.**
   (c) **Updates.** FDP will update FDP Data as needed to correct errors or changes. The Provider may flag, suspend, or remove FDP Data that is manifestly inaccurate, non-conformant, or subject to complaint.

5. **Frequency Guidance.** FDP should update at a frequency sufficient to maintain good data quality (e.g., monthly as a guideline). High-volume or frequently changing assortments should use automated/API updates.

6. **Ownership and License.** FDP retains all right, title, and interest in and to FDP Data. FDP grants Provider a non-exclusive, worldwide, royalty-free license (including the right to sublicense to Customers, Trading Partners, and approved ecosystem channels made available through the Service, such as APIs and marketplaces) to host, store, reproduce, index, format, display, transmit, and distribute FDP Data via the Service and the Global Product Library for value-chain use cases contemplated by this Agreement. Nothing herein assigns ownership of FDP Data to Provider.

7. **Provider Rights.** Provider may (a) annotate non-substantive metadata (e.g., timestamps, status, provenance, unique IDs), (b) perform non-substantive technical transformations (e.g., file/encoding changes, exact unit conversions, schema mappings that preserve meaning), and (c) suspend or remove FDP Data that is non-conformant, unlawful, or reasonably disputed.

8. **Verbatim Distribution; Integrity.** Except for the non-substantive actions in Section 2, Provider will not alter the substantive content of FDP Data and will maintain source attribution and version history. Provider may publish, display, distribute, transmit, syndicate, and otherwise make available FDP Data as provided (verbatim, unaggregated) to users of the Service, Trading Partners, and ecosystem channels permitted under Section 1.

9. **License Survival for Existing Copies.** Upon termination of this Addendum or cessation of FDP activity, the foregoing license continues solely as necessary for (i) historical records,

audit/traceability, and legal compliance, and (ii) Customers' continued use of FDP Data already accessed or embedded in their regulatory/labeling records before termination, subject to the Customers' obligations under the Terms.

10. **No Duty to Monitor.** Except where required by law, the Provider has no duty to monitor, verify, or correct FDP Data and may rely on FDP submissions and change notices.

11. **Downstream Use & Disclaimers.** Consuming Customers are solely responsible for assessing suitability and complying with labeling/regulatory requirements. FDP Data is a reference input and does not replace legal, regulatory, or scientific validation.

12. **Indemnity by FDP (targeted).** FDP will defend and indemnify the Provider against third-party claims to the extent arising from (i) FDP's lack of authority to supply FDP Data, or (ii) alleged IP infringement by FDP Data as supplied, in each case excluding claims caused by the Provider's modification beyond format/transmission, or by the Provider's willful misconduct. **This clause does not create any warranty to consuming Customers.**

13. **Liability Limits.** Subject to willful misconduct or liability that cannot be limited by law, the Provider's aggregate liability to FDP under this Addendum is capped at the lesser of (i) the fees paid by FDP to the Provider in the 12 months preceding the event or (ii) NOK 100,000; the Provider disclaims indirect, consequential, and special damages.

14. **Privacy & Confidentiality.** FDP Data is generally product information intended for public/regulated disclosure. Where FDP Data incidentally contains personal data (e.g., named contacts on specifications), the FDP is controller for that disclosure. Provider's role is as described in the Privacy Policy (Operational Data) and DPA (processor)

15. **Order of Precedence.** For FDP activities, this Addendum controls over conflicting terms in the main ToS. All other provisions of the ToS remain in force.

16. **Termination Effects.** Upon Addendum termination or FDP role cessation, the Provider will cease further distribution of FDP Data in the shared library on a go-forward basis. Existing consuming Customers may retain local copies previously accessed; the Provider may retain historical records as required for audit, traceability, and lawful purposes.