API Terms of Service
Kabal

1. General Terms

1.1. These API (Application Programming Interface) Terms of Service (the "API Terms") govern access to and use of the application programming interfaces, software development kits and related documentation and materials made available by Kabal AS ("Kabal") (the "APIs"). By accessing or using the APIs, the relevant customer entity (the "Customer") agrees to be bound by these API Terms, which apply as a technical extension of the agreement between Kabal and the Customer for Kabal`s software solution (the "Services") (the "Main Agreement"). TThese API Terms are designed to protect the integrity of Kabal`s production environment, ensure a reliable experience for all users, define the technical boundaries of Kabal`s service, and ensure that personal data made available through the APIs is protected.

The Customer must use the APIs only in accordance with these API Terms and the Kabal API documentation, as updated from time to time (the "Documentation").

In the event of any conflict between these API Terms and the Main Agreement, these API Terms prevail as regards access to and use of the APIs.

1.2. Subject to compliance with these API Terms and the Main Agreement, Kabal grants the Customer a non-exclusive, worldwide, non-transferable, revocable license to access the APIs only as necessary to develop, test, use, and support an application that interfaces with the Services (the "Application"). The Customer may not sell, rent, lease, sublicense, redistribute, or syndicate access to any of the APIs. Deployment of any API production environment requires mandatory written review and approval by Kabal.

The Customer's written request for such approval shall state the purpose of the API access, the APIs or modules concerned, the countries from which data made available through the APIs ("API Data") will be accessed and in which it will be stored, the location of any webhook endpoints to which API Data will be sent, and any third parties (including the Customer`s processors and integrators) that will access API Data on the Customer's behalf, together with their location. The Customer is responsible for the accuracy and completeness of its request and shall obtain Kabal's prior written approval before any change to it. Kabal's approval may be given in writing, including by e-mail, and the request as approved constitutes the "Approved API Scope". The Customer shall not access or store API Data in any country other than those stated in the Approved API Scope without Kabal's prior written approval.

1.3. The API is a shared resource. Access is subject to "Fair Use" to ensure system stability. One user's misuse can degrade the service for everyone else. Therefore, these API Terms are built on the principle of fair use.

Access is subject to strict rate limiting based on the Customer`s API subscription level (e.g. Basic/Standard/Enterprise), as set out in the Main Agreement or, where not specified there, in Kabal`s applicable price list. The Customer is fully responsible for adhering to the following hard limits and data handling requirements, applying to specific interfaces:

- Mandatory Pagination: For any API endpoint that returns a list of data, the Customer

must use the provided pagination parameters (e.g., limit, offset, or cursor-based methods). Requesting all available data in a single, unpaginated call is prohibited.

- Filtering: The Customer must utilize available filtering parameters (e.g., date range, status, id) to narrow down its request's server-side. Fetching an entire dataset only to filter it client-side is prohibited.
- Conditional Requests (Caching): To reduce redundant data transfer, the Customer should support ETag headers. Use the If-None-Match request header so Kabal`s server can respond with a 304 Not Modified status if data has not changed.
- Webhooks: Customer shall strive to minimize unnecessary traffic and shall use webhooks where available as the primary method for updates instead of high-frequency polling.
- API Interface for KPIs: Access to this specific interface is strictly limited to a maximum of once every 30 seconds per API key.
- Web Embedded Interface: Any automated refresh or polling within the Web Embedded Interface must not be configured to occur more frequently than once every 30 seconds.

Handling Rate Limits:

- HTTP 429 Status: Kabal uses the HTTP 429 Too Many Requests response code when the Customer exceeds its limit. The Customer must monitor its API calls for this status code.
- Exponential Backoff: If the Customer receives a 429 error or a 5xx server error, the Customer`s application must implement an exponential backoff strategy (waiting for a progressively longer period before retrying).

1.4. Kabal will issue unique API Keys for authentication. All calls must be authenticated; unauthenticated requests will be rejected.

- Confidentiality of Keys
  Customer is solely responsible for the security of the API keys, unless such breach results solely from a proven a security failure attributable directly to Kabal`s gross negligence, and must not share them publicly or commit them to public repositories. Customer must keep all API keys, passwords, and other access credentials ("Credentials") strictly confidential. Customer shall not sell, lease, share, transfer, or sub-license Credentials to any third party without Kabal's prior written consent.

- Responsibility for Usage
  Customer is solely responsible for any and all access to and use of the API that occurs under Customer's Credentials, whether such use is authorized by Customer or not.

- Breach by Third Parties
  Any act or omission by a third-party using Customer's Credentials that would constitute a breach of these API Terms if taken by the Customer shall be deemed a material breach by the Customer.

- Notification
  Customer must notify Kabal immediately of any unauthorized use of Credentials or any other known or suspected breach of security.

- Identification
  All API requests must be identified by a user agent string pre-communicated to Kabal.

1.5. Customer shall not, and shall not permit others to:

a. access the APIs in violation of any law or regulation or for fraudulent purpose;

b. access the APIs in any manner that

   i. compromises, breaks or circumvents any of Kabal`s technical processes, security measures, authentication system or usage limit associated with the Services,

   ii. poses a security vulnerability to customers or users of the Services

   iii. tests the vulnerability of Kabal`s systems or networks, unless expressly authorized under a Kabal security testing or bug bounty program, or

   iv. undermines the Services` access controls, such as by exposing private channel data to a user without access;

c. access the APIs in order to replicate or compete with the Kabal Services;

d. attempt to reverse engineer or otherwise derive source code, trade secrets, or know-how of the APIs or Services;

e. attempt to use the APIs in a manner that exceeds rate limits or constitutes excessive or abusive usage;

f. transmit viruses, worms or other malicious code;

g. implement an uncontrolled automated retry mechanism for failing API requests; or

h. access the APIs from, or provide access to, any person or entity located in a territory subject to UN or EU sanctions;

1.6. The APIs are the exclusive property of Kabal. No ownership interest is transferred to the Customer. Any configurations, improvements, or developments related to the APIs made by the Customer shall automatically be transferred to Kabal. Any feedback, suggestions, or modifications proposed by the Customer regarding the APIs shall be deemed the sole property of Kabal upon creation.

1.7. Kabal reserves the right to audit and monitor the Customer`s usage, Application and technical implementation to ensure compliance with these API Terms, including Personal Data Terms and the handling of API Data. The Customer shall cooperate with inquiries related to any such an audit and provide Kabal with reasonable evidence that its Application complies with Kabal`s terms and policies.

1.8. Customer acknowledges that integration performance may depend on external systems and networks outside Kabal`s control and that Kabal may take immediate technical measures (including throttling or temporarily suspending a specific API key, client, endpoint, or operation) where Kabal deems such action necessary to protect the stability, security, or availability of the Services, or to prevent unauthorized access or system degradation. Kabal may also, with immediate effect, restrict, suspend or revoke API access or amend the Approved API Scope where Kabal considers this necessary to comply with applicable data protection law, or where the Customer breaches the Personal Data Terms or the Approved API Scope. These protective measures are operational safeguards to ensure system integrity and do not constitute a formal suspension or termination of the Main Agreement. Kabal shall have no liability for any loss of data, business interruption or any direct, indirect or consequential losses incurred by Customer as a result of such good-faith protective measures.

No service credits or other compensation shall be payable for any unavailability or degradation of the APIs caused by:

A. Protective measures under this Article 1.8,

B. The Customer`s code, configurations or non-adherence to these API Terms or the Documentation, or

C. Systems or networks outside Kabal`s control.

Kabal will notify the Customer as soon as reasonably practicable following such action and will, where applicable, provide information regarding the reason for the action. Any permanent suspension or termination of API access remains subject to the provisions of the Main Agreement, except where revocation of API access is necessary to comply with applicable data protection law or results from the Customer's breach of the Personal Data Terms or the Approved API Scope. To the extent practicable, Kabal will strive to limit such protective actions to the specific credentials or operations causing the issue, provided that

such limitation does not compromise the effectiveness of the protective measure or the security of other customers.

2. Personal Data

2.1. This Article 2 and Article 3 (together the "Personal Data Terms") govern the Customer`s retrieval and handling of API Data.

2.2. The Customer shall retrieve only the API Data necessary for the purpose stated in the Approved API Scope. Special categories of personal data, including health and medical data processed in Kabal Personnel, are excluded from the Approved API Scope unless Kabal has expressly agreed otherwise in writing, subject to such additional safeguards as Kabal may require.

2.3. As controller of the API Data, the Customer shall:

A. implement appropriate technical and organisational measures to protect API Data against unauthorised access, loss and disclosure;

B. retain API Data only for as long as necessary for the stated purpose, securely delete it when no longer necessary or when API access ends, and confirm such deletion in writing on Kabal's request;

C. not disclose or transfer API Data to any third party, except to its own processors identifies in and approved under the Approved API Scope and bound by written obligations no less protective than the Personal Data Terms, or where required by law, and in each case only where permitted under Applicable Data Protection law and subject to appropriate transfer safeguards; and

D. comply with the data protection laws applicable to it, including any notification or authorisation requirement in its jurisdiction concerning access to data held outside that jurisdiction.

3. API Access from Third Countries

3.1. This Article 3 applies where API Data is accessed from, or stored in, a country outside the European Economic Area (EEA), unless the recipient is covered by an adequacy decision of the European Commission ("Third-Country Access"). Third-Country Access shall only be permitted where it is included in the Approved API Scope and permitted under Applicable Data Protection Law and the Personal Data Terms. Where Third-Country Access constitutes a transfer of Personal Data under Applicable Data Protection Law, the transfer mechanism set out in the Data Processing Agreement between Kabal and the Customer shall apply.

3.2. Where Third-Country Access is permitted under this Clause, the Customer shall:

A. notify Kabal promptly, where legally permitted, of any legally binding request by a public authority for disclosure of API Data, or of any direct access by a public authority to API Data of which it becomes aware;

B. where prohibited from notifying, use its best efforts to obtain a waiver of the prohibition;

C. review the legality of any such request and challenge it where, after careful assessment, there are reasonable grounds to consider it unlawful;

D. disclose only the minimum API Data permissible under a reasonable interpretation of the request; and

E. document such requests and its response and make the documentation available to Kabal on request, to the extent permitted by law.

3.3. The Customer shall notify Kabal promptly if it has reason to believe that it can no longer comply with this Article 3, including following a change in the laws or practices of the relevant country.

3.4. Third-Country Access to data in the Datalake API module requires Kabal's prior written approval, which Kabal may grant subject to additional safeguards or a restricted scope, or refuse at its discretion.

4. API Use and Change Management

4.1. Kabal may update the technical controls described in Article 1.3, including rate limits, pagination and filtering, as needed to maintain service integrity.

4.2. Kabal may modify, improve, or deprecate API endpoints as part of normal product evolution. Where reasonably practicable, Kabal will provide 30 days advance notice for material structural changes to existing API endpoints. Minor updates, enhancements, or non-material changes may be implemented with shorter notice, typically via standard release notes. Furthermore, the notice period shall not apply where action is required to address critical security vulnerabilities, legal compliance, or to sustain platform availability.

4.3. Issues originating from Kabal's systems that materially affect the API will be handled through Kabal's standard support channels.

4.4. The APIs are intended for use by businesses and organizations and not for consumer purposes. To the maximum extent permitted by law, the Customer hereby acknowledges and agrees that consumer laws do not apply. If however any consumer laws (e.g., in Australia, the Competition and Consumer Act 2010 (Cth)) do apply and cannot otherwise be lawfully excluded, nothing in these API Terms will restrict, exclude or modify any statutory

warranties, guarantees, rights or remedies the Customer has, and Kabal`s liability is limited (at Kabal`s option) to the replacement or repair of the APIs.

5. Datalake API Module - Special Conditions

5.1. For customers subscribing to Kabal's Datalake API module, the following special terms apply:

A. The Datalake module is provided for extraction of archive data to a secondary source for reporting and backup purposes.

B. The data of Datalake is being restored daily and is at least 24 hours old, and the Datalake service will be unavailable during the data restoration process.

C. The content, structure and set of supported endpoints provided reflects the underlying data structure of the Kabal solution and is subject to change. Versioning is available for at least 6 months after a change has been made.

D. No end-user support is provided but technical implementation support/assistance can be arranged through the Customer's key account manager or otherwise agreed customer success representative at consultancy rates as stated in the applicable commercial agreement or price list between the Parties.

E. Kabal reserves the right to perform any tasks deemed necessary to maintain the security and availability of the Datalake without prior warning.

F. The content of the Datalake shall be used for internal purposes only (analysis, reporting, backup, etc.) and shall not be shared with third parties unless approved by Kabal.

6. Amendments, Termination and Governing Law

6.1. Kabal may amend these API Terms at any time.

6.2. The Customer's right to access the APIs ends automatically upon expiry or termination of the Main Agreement. Article 2 and Article 3 continue to apply for as long as the Customer retains any API Data.

6.3. These API Terms are governed by the law, and disputes shall be resolved in the manner and venue, agreed in the Main Agreement.