

DIGITAL POLICY ALERT

DPA API Terms

Version: 6 October 2026

PREAMBLE

These DPA API Terms ("API Terms") supplement the DPA Licensed Data – General Terms ("General Terms") for the DPA API delivery channel only. They apply only where the Subscriber's Order grants direct access to DPA API endpoints, credentials, or developer tools. They do not apply merely because SGEPT uses an API internally to operate the DPA MCP Server or another service. Capitalised terms not defined herein have the meaning given in the General Terms.

The General Terms govern all matters relating to the Licensed Data itself, including intellectual property, licence classes, usage restrictions, warranties, liability, and governing law. These API Terms address only the operational terms specific to direct API access. An API Subscription confers access to the Licensed Data through the API only; it grants no right of access through, and no right arising under the terms applicable to, any other delivery channel.

1. ADDITIONAL DEFINITIONS

- **'API'** means the programmatic interface provided by SGEPT for accessing the Licensed Data.
- **'API Subscription'** means a Subscription whose Order grants direct API access under these API Terms.
- **'API Key'** means the unique authentication credential issued to the Subscriber for API access.
- **'Endpoint'** means a specific URL path through which the API delivers data (e.g. Events, Data Counts, Mappings, Semantic Search).
- **'Rate Limit'** means the maximum number of API requests permitted per unit of time, as specified in the Order or in a versioned technical schedule incorporated by the Order.

2. API ACCESS AND CREDENTIALS

2.1 Authentication. The Subscriber shall access the API exclusively through the API Key issued by SGEPT. Each API Key is unique to the Subscriber, may be used only in applications and systems operated by or for the Subscriber's Organisation, and must not be shared with third parties or embedded in publicly accessible code repositories.

2.2 Credential Security. The Subscriber shall store API Keys securely, rotate them periodically or upon suspicion of compromise, and notify SGEPT immediately if an API Key is or may be compromised. SGEPT may revoke and reissue API Keys where a security risk is identified. API Keys are credentials of the Subscriber's Organisation; they do not define the licensed population, which is defined by the Order (General Terms Section 1, 'Authorised Users'), and must not be used to extend access beyond the Authorised Users so defined.

3. ENDPOINTS AND INTEGRATION

The API provides access to the Licensed Data through the Endpoints identified in the Order or SGEPT's versioned technical schedule, as updated from time to time. The Subscriber is responsible for its own systems and integration choices, including integrating with the API to receive updates. SGEPT

does not warrant that Endpoints will remain unchanged except as expressly stated in an incorporated Service Level Agreement or the Order; version management is addressed in Section 6.

4. USE RIGHTS

The Subscriber's permitted use of data accessed through the API is determined by the licence class selected in its Order under the General Terms, together with Permitted Citation. The same Internal Use, Derived Use, and Redistribution boundaries apply regardless of API delivery. Absent separately granted Redistribution rights under General Terms Section 4.5, raw data redistribution is not permitted; no such right is implied by an API Subscription. The Subscriber may load, store, and process API responses within its internal systems for the purposes permitted by its licence class, subject to General Terms Section 4.7 where a Service Provider is used.

5. TECHNICAL LIMITS AND ACCEPTABLE USE

In addition to the restrictions in the General Terms, the Subscriber shall not: exceed the Rate Limit or any query limit stated in the Order, or attempt to bypass rate-limiting mechanisms; use automated tools to systematically overload the API beyond reasonable operational use; attempt to reverse-engineer, decompile, or disassemble any part of the API; or use the API in any way that could impair its performance or interfere with other Subscribers' use. Reasonable caching to operate the Subscriber's permitted use is allowed; bulk extraction beyond the scope of the licence class, and systematic circumvention of technical limits, are not.

6. SECURITY AND SUSPENSION; VERSION MANAGEMENT

The Subscriber shall maintain reasonable safeguards for its API integration and give prompt notice of suspected compromise. SGEPT may proportionately suspend or throttle API access where continued access threatens security, service integrity, or availability, in accordance with General Terms Section 16.

The format and structure of the API may change over time. SGEPT will provide at least thirty (30) calendar days' written notice before implementing changes that affect the Subscriber's existing integration. Deprecated API versions will remain available for at least ninety (90) days following the introduction of a replacement version.

7. SERVICE LEVELS

A Service Level Agreement applies to the DPA API only where, and as, expressly incorporated in the Subscriber's Order. These API Terms do not themselves promise availability levels or remedies. Where no Service Level Agreement is incorporated, the API is provided in accordance with the General Terms without separate service-level commitments.

8. INCORPORATION

The General Terms govern all legal terms applicable to the Subscriber's use of the API, including without limitation intellectual property (Section 3), licence and restrictions (Section 4), attribution (Section 5), data security (Section 7), warranties and disclaimers (Sections 11–12), limitation of liability (Section

13), indemnification (Section 14), term, suspension, and termination (Section 16), modification (Section 17), precedence (Section 18), and governing law (Section 21), in each case of the General Terms.