

Data Processing Addendum

How we Handle Data

Introduction

This Data Processing Addendum ("**Addendum**", "**DPA**") is supplementary to, and forms part of, the terms of use available at haveibeenpwned.com/TermsOfUse, as updated from time to time (the "**Agreement**") between **Superlative Enterprises Pty Ltd** (ABN 62 085 442 020) of Level 11, 2 Corporate Court, Bundall, Queensland, Australia ("**Superlative**", "**we**" or "**us**") and the entity or person(s) subscribing to our services ("**Customer**"). This Addendum applies where and to the extent that Superlative is acting as a Processor or service provider (as applicable) of Personal Data on behalf of Customer under the Agreement. In the event of any conflict between this Addendum and the Agreement, this Addendum shall prevail to the extent of such conflict.

DPA

1. **Definitions and Interpretation**

In this Addendum, the following terms shall have the following meanings:

- (a) "**Applicable Privacy Laws**" means any worldwide data protection and privacy laws and regulations applicable to the Personal Data in question including, where applicable: (i) European Union Regulation 2016/679 General Data Protection Regulation

("GDPR"); (ii) the United Kingdom Data Protection Act 2018 ("UKDPA"); (iii) the revised Swiss Federal Data Protection Act (the "revFADP"); and (iv) the Australian Privacy Act 1988 (Cth); in each case as amended, repealed, consolidated, superseded or replaced from time to time.

- (b) "**Data Subject**" means an identified or identifiable individual whose Personal Data is processed.
- (c) "**Personal Data**" means any information relating to an identified or identifiable individual or any other information defined as 'personal data' or 'personal information' under Applicable Privacy Laws.
- (d) "**Restricted Transfer**" means (i) where the EU GDPR applies, a transfer of Personal Data from the EEA to a country outside the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data from the UK to any other country which is not based on adequacy regulations pursuant to Section 17A of the UK GDPR; and (iii) where the RevFADP applies, a transfer of Personal Data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.
- (e) "**SCCs**" means the [standard contractual clauses annexed to the Commission implementing decision \(EU\) 2021/914](#), as may be amended, superseded or replaced from time to time.
- (f) "**UK Addendum**" means [the International Data Transfer Addendum \(version B.0, in force 21 March 2022\)](#) issued by the Information Commissioner's Office under s.119(A) of the UKDPA, as may be amended, superseded or replaced from time to time.
- (g) The terms "**Controller**", "**Processor**", "**Data Subject**" and "**processing**" have the meanings given to them in Applicable Privacy Laws or, if not defined therein, the

GDPR (and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly)

- (h) Any capitalised terms used but not defined in this Addendum shall have the meanings given to them under the Agreement.

2. **Processing of Personal Data**

2.1 *Relationship of the parties:* The Customer is a Controller of the Personal Data described in **Annex 1.B** (the "**Data**") and Superlative shall process the Data solely as a Processor or Service Provider (as applicable) on behalf of the Customer. Superlative and the Customer shall each comply with their respective obligations under Applicable Privacy Laws. Where the concepts of Controller and Processor are not expressly contemplated by Applicable Privacy Laws, the parties' obligations in connection with this Addendum shall be interpreted under those Applicable Privacy Laws to align as closely as possible with the scope of those roles while still complying fully with those Applicable Privacy Laws.

2.2 *Purpose limitation:* Superlative shall process the Data as necessary to perform its obligations under the Agreement and strictly in accordance with the documented instructions of Customer (the "**Permitted Purpose**"). Superlative must only: (i) retain, use, disclose or otherwise process the Data for the Permitted Purpose (including for its own commercial purpose), except where otherwise required by any law applicable to Superlative; and (ii) must not "sell" the Data within the meaning of the Applicable Privacy Laws. Superlative shall immediately inform Customer if it becomes aware that Customer's processing instructions infringe Applicable Privacy Laws but without obligation to actively monitor Customer's compliance with Applicable Privacy Laws. The parties acknowledge that Customer's transfer of Data to Superlative is not a "sale" of Personal Data within the meaning of Applicable Privacy Laws and Superlative provides no monetary or other valuable consideration to Customer in exchange for the Data.

2.3 *International transfers:* To the extent that Superlative transfers the Data (or permits the Data to be transferred) to a country other than the country in which the Data was first collected, it shall first take such measures as are necessary to ensure that the transfer is made in compliance with Applicable Privacy Laws. Such measures may include (without limitation) transferring the Data to a recipient that has executed standard contractual clauses adopted by the European Commission, UK Secretary of State or Information Commissioner's Office (as applicable) or transferring the Data to a recipient that has executed a contract with Superlative that ensures the Data will be protected to the standard required by Applicable Privacy Laws. Superlative will also protect the Data in a way that overall provides comparable safeguards to the country in which the Data was first collected.

2.4 *Standard contractual clauses:* To the extent that the transfer of Data from Customer to Superlative involves a Restricted Transfer, the SCCs shall be incorporated by reference and form an integral part of this Addendum with Customer as "data exporter" and Superlative as "data importer". For the purposes of the SCCs: (i) the module two (controller to processor) terms shall apply and the module one, three and four terms shall be deleted in their entirety; (ii) in Clause 9, Option 2 shall apply; (iii) in Clause 11, the optional language shall be deleted; (iv) in Clause 17, Option 1 shall apply and the SCCs shall be governed by Irish law; (v) in Clause 18(b), disputes shall be resolved before the courts of Ireland; (vi) the Annexes of the SCCs shall be populated with the information set out in the Annexes to this DPA; and (vii) if and to the extent the SCCs conflict with any provision of the Agreement (including this DPA), the SCCs shall prevail to the extent of such conflict.

2.4.1 *UK transfers:* In relation to Data that is protected by the UK GDPR, the SCCs as incorporated under Section 2.4 shall apply with the following modifications: (i) the SCCs shall be amended as specified by the UK Addendum, which shall be

incorporated by reference; (ii) Tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed using the information contained in the Annexes of this DPA; (iii) Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "importer"; and (iv) any conflict between the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

2.4.2 *Swiss transfers*: In relation to Data that is protected by the RevFADP, the SCCs as incorporated under Section 2.4 shall apply with the following modifications: (i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the RevFADP; (ii) references to "EU," "Union," and "Member State" shall be replaced with "Switzerland"; (iv) references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the "Swiss Federal Data Protection and Information Commissioner" and the "competent Swiss courts"; and (v) the SCCs shall be governed by the laws of Switzerland and disputes shall be resolved before the competent Swiss courts.

2.5 *Confidentiality of processing*: Superlative shall ensure that any person that it authorises to process the Data (including Superlative's staff, agents and subcontractors) (an "**Authorised Person**") shall be subject to appropriate responsibilities of confidentiality. Superlative shall ensure that all Authorised Persons process the Data only as necessary for the Permitted Purpose.

2.6 *Security*: Superlative shall implement appropriate technical and organisational measures to protect the Data from the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, access to the Data (a "**Security Incident**"). At a minimum, such measures shall include the measures identified at the url haveibeenpwned.com/Privacy. Customer

acknowledges that Superlative may update or modify the security measures from time to time by publishing these at the url haveibeenpwned.com/Privacy, provided that such updates and modifications do not result in a degradation to the overall level of security.

2.7 *Sub-processing*: Customer authorises Superlative to engage third party Processors ("**Sub-processors**") to process the Data for the Permitted Purpose provided that:

2.7.1 Superlative provides reasonable prior notice at least 14 days before the proposed addition or replacement of any Sub-processor, in order to allow Customer to raise any reasonable objections on grounds of data protection;

2.7.2 Superlative imposes data protection terms on any Sub-processor it engages that ensure substantially the same standard of protection provided under this Addendum and Superlative remains fully liable for any breach of this Addendum caused by an act, error or omission or the performance of its Sub-processors.

Superlative's current Sub-processors are identified at Annexure 3. For the purposes of Clause 9(c) of the SCCs, Customer acknowledges that Superlative may be restricted from disclosing Sub-processor agreements to Customer due to confidentiality obligations. Where Superlative cannot disclose a Sub-processor agreement to Customer, Customer shall provide all information (on a confidential basis) it reasonably can in connection with such agreement.

2.8 *Cooperation and Data Subjects' rights*: Superlative shall provide all reasonable and timely assistance to Customer to enable Customer to respond to: (i) any request from a Data Subject to exercise any of their rights under Applicable Privacy Laws; and (ii) any other correspondence, enquiry or complaint received from a Data Subject, data protection authority, regulator or other third party in connection with Superlative's processing of the Data. In the event any such request, correspondence, enquiry or complaint is made directly

to Superlative, Superlative shall promptly inform Customer providing full details of the same.

- 2.9 *Data Protection Impact Assessment:* Superlative shall provide Customer with all such reasonable and timely assistance as Customer may require in order to comply with its obligation under Applicable Privacy Laws to conduct data protection impact assessments and, if necessary, to consult with its relevant data protection authority.
- 2.10 *Security Incidents:* Upon becoming aware of a Security Incident, Superlative shall inform Customer without undue delay and shall provide all such timely information and reasonable cooperation as Customer may reasonably require in order for Customer to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Privacy Laws. Superlative shall further take all such measures and actions as are reasonably necessary to remedy or mitigate the effects of the Security Incident and keep Customer informed of all material developments in connection with the Security Incident. Customer will not communicate or publish any notice or admission of liability concerning any Security Incident which directly or indirectly identifies Superlative (including in any legal proceeding or in any notification to regulatory authorities or affected Data Subjects) without Superlative's prior approval, unless Customer is compelled to do so under applicable law. In any event, Customer shall provide Superlative with reasonable prior written notice of any such communication or publication.
- 2.11 *Deletion or return of Data:* Upon termination or expiry of the Agreement, Superlative shall (at Customer's election) destroy or return to Customer all Data (including all copies of the Data) in its possession or control. This requirement shall not apply to the extent that Superlative is required by any law to retain some or all of the Data, in which event Superlative shall isolate and protect the Data from any further

processing except to the extent required by such law until deletion is possible.

ANNEXES

ANNEX I. A. LIST OF PARTIES

Data exporter(s):

Name: The entity identified as the "Customer" on the Order Form or the name specified in Customer's account.

Address: The Customer's Billing Address specified on the Order Form or the address specified in Customer's account.

Contact person's name, position and contact details: The Primary Contact Name, Primary Contact Position and Primary Contact Email specified on the Order Form or the contact information specified in a Customer's account.

Activities relevant to the data transferred under these Clauses: The data exporter is a customer of the data importer and utilising the data importer's services on haveibeenpwned.com.

Role (controller/processor): Controller

Data importer(s):

Name: The Superlative entity identified on the Order Form.

Address: The Superlative entity's address specified on the Order Form.

Representative contact details: Contact person's name, position and contact details: Troy Hunt, Founder and CEO support.haveibeenpwned.com

Activities relevant to the data transferred under these Clauses: The data importer operates a website used as a resource to determine if the data of individuals or organisations has been compromised in a known data breach.

Role (controller/processor): Processor

Annex 1.B. DESCRIPTION OF TRANSFER

Categories of data subjects: Licensed Users of the Service pursuant to the Agreement between Superlative and the Customer, which may include Customer's employees, contractors or agents.

Categories of personal data: The categories of personal data are determined and controlled by Customer in its sole discretion.

Sensitive data transferred (if applicable) and applied restrictions or safeguards: We do not collect sensitive information. See Annex 2 for applied restrictions and safeguards.

Frequency of the transfer: Ad hoc.

Nature of the processing: Processing of the Customer's and Licensed Users' usernames, passwords and contact details in order to access and manage the Services.

Purpose(s) of the data transfer and further processing: Provision of the Service pursuant to the Agreement.

Period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: The personal data will be retained until termination or expiry of the Agreement, in accordance with Section 2.11 of this Addendum.

Annex 1.C. COMPETENT SUPERVISORY AUTHORITY

The supervisory authority of the EEA Member State in which Customer is established or, if Customer is not established in the EEA, the EEA Member State in which Customer's representative is established or in which Customer's End Users are predominantly located.

ANNEX 2 - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Technical and organisational measures to ensure the security of the data include:

- (a) all data transmitted over the internet is transmitted over Hypertext Transfer Protocol Secure (HTTPS);
- (b) Cloudflare is used extensively to block potentially malicious requests;
- (c) rate limits on APIs are implemented at both the code level and via Cloudflare;
- (d) regular security scans are performed to identify code or configuration vulnerabilities;
- (e) firewalls are employed to limit access to services running on Microsoft Azure;
- (f) disclosure of any security vulnerabilities are encouraged via [the security.txt file](#); and
- (g) Third party components are kept well-maintained.

ANNEX 3 – LIST OF SUB-PROCESSORS

The Customer has authorised the use of the following sub-processors.

Provider	Description of processing	Privacy contact
Cloudflare	Security services	privacyquestions@cloudflare
Microsoft Corporation	Data storage through Microsoft Azure platform	microsoft.com/en-au/concern/privacy

Provider	Description of processing	Privacy contact
SendGrid	Transactional and marketing communications	privacy@twilio.com
Stripe	Online payment processing	privacy@stripe.com
Zendesk	Customer support services	privacy@zendesk.com

Check if your email has been compromised in a data breach

[🔍 Check my email](#)

Services

[Email Search](#)

[Domain Search](#)

[Who's Been Pwned](#)

[Passwords](#)

[Notify Me](#)

[API](#)

[Pricing](#)

[Opt Out](#)

[Dashboard](#)

[Partners](#)

Information

[Demos](#)

[Who, What & Why](#)

[FAQ](#)

[Privacy Policy](#)

[Terms of Use](#)

[DPA](#)

[Suggest a Feature](#)

[Donate](#)

[Merch](#)

Connect With Us



© 2026 Have I Been Pwned. All rights reserved.