



## DATA PROCESSING AGREEMENT (DPA)

### PARTIES

<b>DN</b>	<b>The Do Nation Enterprise</b> (company number 8688899) with registered office at 5 High Green, Great Shelford, Cambridge, England, CB22 5EG; and
<b>Client</b>	

(each a **Party**)

### BACKGROUND

Under an agreement (**Agreement**) DN provides a web-based online pledge platform (**Platform**) service to Client. See <https://www.wereadonation.com/organisations/> for general information about DN's platform.

Each party is a separate controller for the name, business contact details and related personal data it processes about the other's personnel in order to perform the Agreement and to manage the relationship between the parties; with the exception of that relationship-management personal data, DN is a processor for all Client users' personal data entered into the Platform by each user (each a **Client User**) when making their pledges (**Pledges**) on the Platform (**Client User Data**).

### AGREEMENT

For the purposes of the Agreement and the **DPA Terms** below:

<b>Details of the Client User Data (Article 28(3) GDPR information)</b>	
<i>Subject matter and duration of the processing</i>	The subject matter and duration of the processing are set out in the Agreement and this DPA.
<i>Nature and the purpose of the processing</i>	Processing activities (including but not limited to, access, use, store, transfer, receipt, collection and organisation of personal data) that are reasonably required to provide the Platform under the Agreement.
<i>Types of personal data</i>	Any types of personal selected or provided by Client Users. <ul style="list-style-type: none"><li>• Business contact details</li><li>• Personal details</li><li>• Lifestyle details (including relating to pledges on the Platform, etc)</li><li>• Employment/education status (including whether student, employed or retired, etc)</li></ul> To the extent voluntarily provided by a Client User when making a Pledge (which DN shall be entitled to treat as manifestly made public by the Client User), this may include special category personal data or sensitive personal data)
<i>Categories of data subjects</i>	Client Users

<i>Obligations and rights of Client</i>	The obligations and rights of Client are set out in the Agreement and the DPA Terms below.
---	--

<b>Transfers of personal data and details required by the Standard Contractual Clauses (if applicable)</b>			
DN and Client hereby agree that the <b>Standard Contractual Clauses</b> (controller - processor) at <a href="https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02010D0087-20161217">https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02010D0087-20161217</a> will be deemed to apply between the data exporter(s) and data importer(s) set out below, on the basis that the following references in the Standard Contractual Clauses have the following meanings:			
<i>Standard Contractual Clauses (SCCs) reference</i>	<i>Location in the SCCs</i>	<i>DN as importer</i>	<i>DN as exporter</i>
Data exporter(s)	Appendix 1	Client and its group companies in EEA that benefit from the Agreement	DN
Data importer(s)	Appendix 1	DN	Client and its group companies outside UK/EEA that benefit from the Agreement  Sub-processors outside the UK/EEA  (N/A to any sub-processor being governed by Binding Corporate Rules, in which case the BCRs shall be the legitimate transfer mechanic)
Recipients	Annex B	See <i>Sub-processors</i> in the table below	See <i>Sub-processors</i> in the table below
Description of technical and organisational measures	Appendix 2	See <i>Technical and Organisational Measures</i> in the table below	As published by Sub-processors from time to time
All other relevant references in the SCCs shall be construed with reference to the applicable part of the tables immediately above/below and the Agreement more widely, unless otherwise expressly specified in the Agreement.			

<b>Technical and Organisational Measures, sub-processors, and DN's contact details for privacy-related communications</b>	
<i>Technical and Organisational Measures</i>	<p>Do Nation is a small, cloud first, organisation. That means DN has no on-premises infrastructure other than laptops and mobiles provided by DN to staff. DN uses GSuite as its primary office environment, and a variety of other SaaS platforms to deliver the Platform.</p> <p>Do Nation has Cyber Essentials certification (number IASME-CE-008497). Verify this here: <a href="https://www.ncsc.gov.uk/cyberessentials/search">https://www.ncsc.gov.uk/cyberessentials/search</a></p> <p>DN uses published guidance from the UK's Information Commissioners Office (ICO) and the National Cyber Security Centre (NCSC) on required security outcomes to ensure adequate data protection. See: <a href="https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes">https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes</a></p> <p>DN has formal written information security and data protection policies.</p> <p>DN conducts due diligence on all our SaaS providers, ensuring they have appropriate security and compliance measures in place to meet GDPR requirements.</p>

	<p>DN enables all security features these platforms have available, such as two factor authentication, and provides password managers for all staff to ensure they have strong, unique passwords for each service.</p> <p>DN keeps all devices used for its business up-to-date and ensures they meet a minimum set of security requirements.</p> <p>DN provides training for staff on secure behaviours.</p> <p>The Platform has been subject to independent security testing.</p>
<i>Sub-processors</i>	<p>The providers of the following services:</p> <ul style="list-style-type: none"> <li>GSuite</li> <li>Heroku</li> <li>AWS</li> <li>SendGrid</li> <li>CloudAMQP</li> <li>MemCachier</li> <li>Rollbar</li> <li>Papertrail</li> <li>Heroku Database</li> <li>Active Campaign</li> <li>HelpScout</li> <li>Amplitude</li> <li>Mailchimp</li> </ul>
<i>Contact details for privacy-related communications</i>	<a href="mailto:privacy@wearedonation.com">privacy@wearedonation.com</a>

**SIGNATURES**

<b>Signed for and on behalf of THE DO NATION ENTERPRISE LIMITED</b>	<b>Signed for and on behalf of</b>
<p>.....</p> <p><b>Name:</b> <b>Position:</b> <b>Date:</b></p>	<p>.....</p> <p><b>Name:</b> <b>Position:</b> <b>Date:</b></p>

# DPA TERMS

## 1. DEFINITIONS AND INTERPRETATION

- 1.1 **Client User Data** means any information relating to an identified or identifiable natural person that is processed by DN as a result of, or in connection with, the provision of a Platform to Client Users under the Agreement; an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- 1.2 **GDPR** means: (a) the European Union General Data Protection Regulation (EU) 2016/679 on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA); (b) the GDPR as incorporated into United Kingdom (UK) law by the Data Protection Act 2018 (**DPA; UK GDPR**) and amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 (each as amended, superseded, or replaced); and (c) any other data protection laws or regulations modelled on GDPR under applicable laws and regulations.
- 1.3 **UK Data Protection Laws** means the UK GDPR, the DPA, the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) and any other United Kingdom law relating to personal data and/or any other extra-territorial laws applying in the United Kingdom relating to personal data applicable to processing of personal data.
- 1.4 **Data Protection Laws** means the UK Data Protection Laws, the relevant parts of the *UK-EU Trade and Cooperation Agreement*, and any other legislation relating to personal data and all other legislation and regulatory requirements in force from time to time which apply to a Party relating to the use of personal data.
- 1.5 The terms **controller, processor, data subject, personal data, processing, appropriate technical and organisational measures and personal data breach** are defined in the UK Data Protection Laws.
- 1.6 This DPA is subject to the terms of the Agreement and is incorporated into the Agreement. Interpretations and defined terms in the Agreement apply to the interpretation of this DPA.
- 1.7 In the case of conflict or ambiguity between: (a) any of the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA will prevail; and (b) any of the provisions of this DPA and any SCC, the provisions of the executed SCC will prevail.
- 1.8 In the DPA, the following rules of interpretation apply: (a) headings shall not affect the interpretation of the DPA; (b) a person includes a

natural person, corporate or unincorporated body (whether or not having separate legal personality); (c) a reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established; (d) a reference to a group of companies is in relation to a company, that company, any subsidiary or holding company from time to time of that company, and any subsidiary from time to time of a holding company of that company; (e) a reference to a holding company or a subsidiary means a holding company or a subsidiary (as the case may be) as defined in section 1159 of the Companies Act 2006; (f) a reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time; (g) a reference to a statute or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision; (h) unless the context otherwise requires, any reference to EU law that is directly applicable or directly effective in the UK at any time is a reference to it as it applies in England and Wales from time to time including as retained, amended, extended or re-enacted on or after 31 December 2019; (i) a reference to writing or written includes email (but not any other form of direct messaging such as WhatsApp or Slack); and (j) any words following the terms including, include, in particular, for example or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.

1.9 Any obligation on a Party not to do something includes an obligation not to allow that thing to be done.

## 2. CLIENT'S PROCESSING INFORMATION

2.1 The front sheet describes the subject matter and duration of the processing of the Client User Data, the nature and purpose of the processing, the types of personal data and categories of data subjects and the rights and obligations of the Client in connection with the Client User Data.

2.2 Client confirms: (a) its use of the Platform, and invitation to Client Users to use the Platform to make Pledges, complies with the Data Protection Laws applicable to Client (including having a lawful basis for processing under the GDPR); (b) Client has taken reasonable care to comply with Article 28(1) GDPR; and (c) the technical and organisational measures described on the front sheet are sufficient to meet the requirements of the GDPR and ensure the protection of the rights of Client Users.

## 3. DN'S PROCESSING OBLIGATIONS

3.1 DN may process Client User Data to fulfil the Business Purposes of the Agreement. **Business Purposes** means the services described in the

- Agreement or any other purpose recorded in writing between the Parties.
- 3.2 DN will only process Client User Data to the extent, and in such a manner, as is necessary for the Business Purposes.
- Client instructions*
- 3.3 DN will process the Client User Data only in accordance with the instructions of Client (including any instructions given by use of functionality of the Platform). DN will not process Client User Data for any other purpose or in a way that DN believes does not comply with this DPA or the UK Data Protection Laws. DN must promptly notify Client if, in its opinion, Client's instruction would not comply with the UK Data Protection Laws (unless applicable law would prevent DN from doing so).
- Employees and contractors*
- 3.4 DN will ensure that all employees and contractors are informed of the confidential nature of Client User Data and are bound by confidentiality obligations and use restrictions in respect of Client User Data. (Such restriction shall not apply to any aspect of the Platform which is publicly available or any Pledges which the Client User has made public.)
- Security of processing*
- 3.5 DN will implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of personal data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Client User Data.
- 3.6 DN will implement such measures as are reasonable to ensure a level of security appropriate to the risk involved, including as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of security measures.
- 3.7 DN will take reasonable steps to ensure the reliability, integrity and trustworthiness of all DN's employees with access to Client User Data.
- Sub-processing*
- 3.8 Client consents to DN appointing any third party processor of personal data as part of its common technology infrastructure for Platforms and providing its services generally (see the front sheet for an up to date list).
- 3.9 DN will inform Client of any additional or replacement sub-processors and Client shall raise any objection within 7 days of notification, giving reasons, to the email [privacy@wearedonation.com](mailto:privacy@wearedonation.com).
- 3.10 DN confirms that it has entered or (as the case may be) shall enter into agreements with any sub-processor in compliance with the UK Data Protection Laws.
- 3.11 As between Client and DN, DN shall remain responsible to Client for all acts or omissions of any third party processor appointed by it pursuant to this DPA.
- 3.12 Client acknowledges and agrees that the appointment of the sub-processors is subject to each sub-processors' standard terms data processing agreement terms (**Sub-processor DPA Terms**).
- 3.13 Any obligations of DN with respect to sub-processors are subject to the Sub-processor DPA Terms.
- Data subject assistance*
- 3.14 DN will assist Client by ensuring that there are such technical and organisational measures as may be reasonable to provide information to assist Client to comply with the rights of data subjects in connection with the Client User Data under the UK Data Protection Laws, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data.
- Supervisory authority assistance*
- 3.15 DN will (at Client's cost and expense) assist Client with its obligations to supervisory authorities relating to personal data breaches, data protection impact assessments, and consultations affecting Client User Data.
- 3.16 DN will, without undue delay, notify Client of any personal data breach affecting Client User Data. DN will also provide Client with the following information: (a) description of the nature of the personal data breach; (b) the likely consequences; and (c) description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects).
- 3.17 DN will promptly notify Client if it receives any notice from a supervisory authority that relates directly to the processing of Client User Data (unless requested by the supervisory authority not to).
- Deletion or return of Client User Data*
- 3.18 DN will (at Client's cost and expense) comply with any Client request or instruction requiring DN to delete or return Client User Data.
- Record keeping and audit*
- 3.19 DN will keep records regarding any processing of personal data it carries out for Client in accordance with UK Data Protection Laws (**Records**).
- 3.20 DN will ensure that the Records are sufficient to enable Client to verify DN's compliance with its obligations under this DPA and DN will provide Client with copies of the Records upon request (no more than once per calendar year).
- 3.21 On Client's written request to [privacy@wearedonation.com](mailto:privacy@wearedonation.com), DN will provide written evidence of its then-current accreditations (no more than once per calendar year).
- 3.22 Client's authorised representative, subject to

- confidentiality and conflict of interest clearances, may audit the Records upon 30 days written notice to [privacy@wearedonation.com](mailto:privacy@wearedonation.com) (no more than once per calendar year).
- 4. CROSS-BORDER TRANSFERS OF PERSONAL DATA**
- 4.1 DN shall ensure any cross-border transfers of Client User Data outside of the UK/EEA by DN are in compliance with the UK Data Protection Laws.
- 4.2 The SCCs referenced on the front sheet shall apply, as the context requires.
- 5. CCPA**
- 5.1 Solely for clause 5.1, **Commercial Purpose**, **Personal Information** and **Sell** are as defined in California Consumer Privacy Act 2018 (**CCPA**). If DN processes Personal Information subject to CCPA on behalf of Client, DN will not: (a) Sell Personal Information; (b) retain, use or disclose Personal Information for any purpose, including a Commercial Purpose, other than for the specific purpose of performing the Services; or (c) retain, use, or disclose Personal Data outside the direct business relationship between the Parties.
- 6. TERM AND TERMINATION**
- 6.1 This DPA will remain in full force and effect so long as: (a) the Agreement remains in effect; or (b) DN retains any Personal Data related to the Agreement in its possession or control as part of exit management under the Agreement (**DPA Term**).
- 6.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Agreement in order to protect Personal Data will remain in full force and effect.
- 6.3 If a change in any Data Protection Laws prevents either Party from fulfilling all or part of its Agreement obligations, the Parties will suspend the processing of personal data until that processing complies with the new requirements.
- 7. GENERAL & INTERPRETATION**
- 7.1 DN may assign, transfer, grant any security interest over or hold on trust any of its rights or obligations under the DPA or any interest in them, provided the assignee or transferee remains bound by this DPA (including meeting at least the same level as technical and organisational protection standards as DN).
- 7.2 Client shall not, without the written consent of DN (which shall not be unreasonably withheld or delayed) assign or transfer any of its rights or obligations under the DPA to any third party which is not in its group of companies.
- 7.3 Nothing in the DPA is intended to or shall operate to create a partnership or joint venture of any kind between the Parties. Neither Party shall have the authority to bind the other Party or to contract in the name of, or create a liability against, the other Party in any way or for any purpose.
- 7.4 Other than as set out in this clause, the Parties do not intend any third party to have the right to enforce any provision of the DPA under the Contracts (Rights of Third Parties) Act 1999 or otherwise.
- 7.5 The Agreement and DPA are the entire agreement between the Parties, and replaces all previous agreements and understandings between them, relating to its subject matter.
- 7.6 No variation of the DPA shall be effective unless it is in writing and signed by or on behalf of each Party.
- 7.7 No failure or delay by a Party to exercise any right or remedy provided under the DPA or by Data Protection Laws shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.
- 7.8 The rights and remedies expressly conferred by the DPA are cumulative and additional to any other rights or remedies a Party may have.
- 7.9 Unless a notice is expressly stated to be by email in the DPA, the notices provisions of the Agreement shall apply to any notice under the DPA.
- 7.10 If any provision or part-provision of the DPA is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of the DPA. If any provision or part-provision of the DPA is deemed deleted, DN may replace it with a provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.
- 7.11 The Parties shall ensure that a DN privacy manager, and an appropriate counterpart from Client, shall use their best efforts to negotiate in good faith and settle any dispute or difference that may arise out of the DPA. The escalation and dispute resolution provisions of the Agreement shall apply to the DPA.
- 7.12 The DPA and any non-contractual obligations arising in connection with it are governed by and construed in accordance with English law, and the courts of England and Wales shall have exclusive jurisdiction to determine any dispute arising in connection with the DPA, including disputes relating to any non-contractual obligations.

© The Do Nation Enterprise Ltd 2021  
Version 1.0 (June 2021)