Effective from 21st September 2022

This DPA is entered into between the Controller and the Processor and is incorporated into and governed by the terms of the Agreement.

1. Definitions

Any capitalised term not defined in this DPA shall have the meaning given to it in the Agreement.

"**Affiliates**"

means any entity that directly or indirectly controls, is controlled by, or is under common control of a party. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of a party;

"Agreement"

means the agreement between the Controller and the Processor for the provision of the Services;

"CCPA"

means the California Consumer Privacy Act of 2018, along with its regulations and as amended from time to time

"Controller"

means the Customer;

"Data Protection Law"

means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states and the United Kingdom, any amendments, replacements or renewals thereof, applicable to the processing of Personal Data, including where applicable the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020, the EU GDPR, the UK GDPR, the FDPA, the UK Data Protection Act 2018, the CCPA and any applicable national implementing laws, regulations and secondary legislation relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426;

"Data Subject"

shall have the same meaning as in Data Protection Law or means a "Consumer" as that term is defined in the CCPA;

"DPA"

means this data processing agreement together with Exhibits A, B and C;

"EEA"

means the European Economic Area;

“EU GDPR”

means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (General Data Protection Regulation);

“FDPA”

means the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1; FDPA) and as amended from time to time

“Personal Data”

shall have the same meaning as in Data Protection Law;

“Processor”

means the Company, including as applicable any “Service Provider” as that term is defined by the CCPA;

“Restricted Transfer”

means:

(i) where the EU GDPR applies, a transfer of Personal Data via the Services from the EEA either directly or via onward transfer, to any country or recipient outside of the EEA not subject to an adequacy determination by the European Commission; and

(ii) where the UK GDPR applies, a transfer of Personal Data via the Services from the United Kingdom either directly or via onward transfer, to any country or recipient outside of the UK not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and

(iii) a transfer of Personal Data via the Services from Switzerland either directly or via onward transfer, to any country or recipient outside of the EEA and/or Switzerland not subject to an adequacy determination by the European Commission;

“Security Policy”

means the Processor’s security document as updated from time to time, and shown in Exhibit B;

“Services”

means all services and software applications and solutions provided to the Controller by the Processor under and as described in the Agreement;

“SCCs”

means:

(i) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries published at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN/, ("**EU SCCs**"); and

(ii) where the UK GDPR applies standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR as set out in Exhibit C of this DPA, ("**UK SCCs**"); and

(iii) where Personal Data is transferred from Switzerland to outside of Switzerland or the EEA, the EU SCCs as amended in accordance with guidance from the Swiss Data Protection Authority; ("**Swiss SCCs**");

"Sub-Processor"

means any third party (including Processor Affiliates) engaged directly or indirectly by the Processor to process Personal Data under this DPA in the provision of the Services to the Controller;

"Supervisory Authority"

means a governmental or government chartered regulatory body having binding legal authority over a party;

"UK GDPR"

means the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

2. Purpose

2.1 The Processor has agreed to provide the Services to the Controller in accordance with the terms of the Agreement. In providing the Services, the Processor shall process Customer Data on behalf of the Controller. Customer Data may include Personal Data. The Processor will process and protect such Personal Data in accordance with the terms of this DPA.

3. Scope

3.1 In providing the Services to the Controller pursuant to the terms of the Agreement, the Processor shall process Personal Data only to the extent necessary to provide the Services in accordance with the terms of the Agreement, this DPA and the Controller's instructions documented in the Agreement and this DPA, as may be updated from time to time.

3.2 The Controller and Processor shall take steps to ensure that any natural person acting under the authority of the Controller or the Processor who has access to Personal Data does not process them except on the instructions from the Controller unless he or she is required to do so by any Data Protection Law.

4. Processor Obligations

4.1 The Processor may collect, process or use Personal Data only within the scope of this DPA.

4.2 The Processor confirms that it shall process Personal Data on behalf of the Controller in accordance with the documented instructions of the Controller.

4.3 The Processor shall promptly inform the Controller, if in the Processor's opinion, any of the instructions regarding the processing of Personal Data provided by the Controller, breach any Data Protection Law.

4.4 The Processor shall ensure that all employees, agents, officers and contractors involved in the handling of Personal Data: (i) are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential; (ii) have received appropriate training on their responsibilities as a data processor; and (iii) are bound by the terms of this DPA.

4.5 The Processor shall implement appropriate technical and organisational measures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

4.6 The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

4.7 The technical and organisational measures detailed in Exhibit B shall be at all times adhered to as a minimum security standard. The Controller accepts and agrees that the technical and organisational measures are subject to development and review and that the Processor may use alternative suitable measures to those detailed in the attachments to this DPA, provided such measures are at least equivalent to the technical and organisational measures set out in Exhibit B and appropriate pursuant to the Processor's obligations in clauses 4.5 and 4.6 above.

4.8 The Controller acknowledges and agrees that, in the course of providing the Services to the Controller, it may be necessary for the Processor to access the Personal Data to respond to any technical problems or Controller queries and to ensure the proper working of Services. All such access by the Processor will be limited to those purposes.

4.9 Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the Controller by having in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights and the Controller's compliance with the Controller's data protection obligations in respect of the processing of Personal Data.

4.10 The Processor confirms that it and/or its Affiliate(s) have appointed a data protection officer where such appointment is required by Data Protection Law. The appointed data protection officer may be reached at dpo@donorfy.com.

4.11 The Processor may not: (i) sell Personal Data; (ii) retain, use, or disclose Personal Data for commercial purposes other than providing the Services under the terms of the Agreement; or (iii) retain, use, or disclose Personal Data outside of the Agreement.

5. Controller Obligations

5.1 The Controller represents and warrants that: (i) it shall comply with the terms of this DPA and its obligations under Data Protection Law; (ii) it has obtained any and all necessary permissions and authorisations necessary to permit the Processor, its Affiliates and Sub-Processors, to execute their rights or perform their obligations under this DPA; and (iii) all Affiliates of the Controller who use the Services shall comply with the obligations of the Controller set out in this DPA

5.2 The Controller shall implement appropriate technical and organisational measures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

5.3 The Controller acknowledges and agrees that some instructions from the Controller, including destruction or return of data, the Processor, assisting with audits, inspections, DPIAs or providing any assistance under this DPA, may result in additional fees. In such case, the Processor shall be entitled to charge the Controller for its costs and expenses in providing any such assistance and will notify the Controller of its fees for providing such assistance in advance, unless otherwise agreed.

6. Sub-Processors

6.1 The Controller acknowledges and agrees that: (i) Affiliates of the Processor may be used as Sub-Processors; and (ii) the Processor and its Affiliates respectively may engage Sub-Processors in connection with the provision of the Services.

6.2 All Sub-Processors who process Personal Data in the provision of the Services to the Controller shall comply with the obligations of the Processor set out in this DPA.

6.3 The Controller authorises the Processor to use the Sub-Processors already included in the current list of Sub-processors to process the Personal Data. pub. During the term of this DPA, the Processor shall provide the Controller with 30 days prior notification, via email, of any changes to the list of Sub-Processors before authorising any new or replacement Sub-Processor to process Personal Data in connection with the provision of the Services.

6.4 The Controller may object to the use of a new or replacement Sub-Processor, by notifying the Processor promptly in writing within ten (10) Business Days after receipt of the Processor's notice. If the Controller objects to a new or replacement Sub-Processor, the Controller may terminate the Agreement with respect to those Services which cannot be provided by the Processor without the

use of the new or replacement Sub-Processor. The Processor will refund the Controller any prepaid fees covering the remainder of the term of the Agreement following the effective date of termination with respect to such terminated Services.

6.5 All Sub-Processors who process Personal Data shall comply with the obligations of the Processor set out in this DPA. The Processor shall prior to the relevant Sub-Processor carrying out any processing activities in respect of the Personal Data; (i) appoint each Sub-Processor under a written contract containing materially the same obligations to those of the Processor in this DPA enforceable by the Processor; and (ii) ensure each such Sub-Processor complies with all such obligations.

6.6 The Controller agrees that the Processor and its Sub-Processors may make Restricted Transfers of Personal Data for the purpose of providing the Services to the Controller in accordance with the Agreement. The Processor confirms that such Sub-Processors: (i) are located in a third country or territory recognised by the EU Commission or a Supervisory Authority, as applicable, to have an adequate level of protection; or (ii) have entered into the applicable SCCs with the Processor; or (iii) have other legally recognised appropriate safeguards in place.

7. Restricted Transfers

7.1 The parties agree that, when the transfer of Personal Data from the Controller to the Processor or from the Processor to a Sub-processor is a Restricted Transfer, it shall be subject to the applicable SCCs.

7.2 The parties agree that the EU SCCs shall apply to Restricted Transfers from the EEA. The EU SCCs shall be deemed entered into (and incorporated into this DPA by reference) and completed as follows:

(i) Module Two (Controller to Processor) shall apply where the Customer is a Controller of Customer Data and the Company is processing Customer Data;
(ii) Module Three (Processor to Processor) shall apply where the Company is a Processor of Customer Data and the Company uses a Sub-Processor to process the Customer Data;
(iii) In Clause 7 of the EU SCCs, the optional docking clause will not apply;
(iv) In Clause 9 of the EU SCCs Option 2 applies, and the time period for giving notice of Sub-Processor changes shall be 30 days;
(v) In Clause 11 of the EU SCCs, the optional language shall not apply;
(vi) In Clause 17 of the EU SCCs, Option 1 applies and the EU SCCs shall be governed by Irish law;
(vii) In Clause 18(b) of the EU SCCs, disputes shall be resolved by the courts of Ireland;
(viii) Annex I of the EU SCCs shall be deemed completed with the information set out in Exhibit A of this DPA;
(ix) Annex II of the EU SCCs shall be deemed completed with the information set out in Exhibit B of this DPA.

7.3 The parties agree that the EU SCCs as amended in clause 7.2 above, shall be adjusted as set out below where the FDPA applies to any Restricted Transfer:

(i) The Swiss Federal Data Protection and Information Commissioner (“FDPIC”) shall be the sole Supervisory Authority for Restricted Transfers exclusively subject to the FDPA;

(ii) Restricted Transfers subject to both the FDPA and the EU GDPR, shall be dealt with by the EU Supervisory Authority named in Exhibit A of this DPA;
(iii) The term 'member state' must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs;
(iv) Where Restricted Transfers are exclusively subject to the FDPA, all references to the GDPR in the EU SCCs are to be understood to be references to the FDPA;
(v) Where Restricted Transfers are subject to both the FDPA and the EU GDPR, all references to the GDPR in the EU SCCs are to be understood to be references to the FDPA insofar as the Restricted Transfers are subject to the FDPA;
(vi) The Swiss SCCs also protect the Personal Data of legal entities until the entry into force of the revised FDPA.

7.4 The parties agree that the UK SCCs shall apply to Restricted Transfers from the UK and the UK SCCs shall be deemed entered into (and incorporated into this DPA by reference), as set out in Exhibit C of this DPA.

7.5 In the event that any provision of this DPA contradicts directly or indirectly any SCCs, the provisions of the applicable SCCs shall prevail over the terms of the DPA.

8. Data Subject Access Requests

8.1 The Controller may require correction, deletion, blocking and/or making available the Personal Data during or after termination of the Agreement. The Controller acknowledges and agrees that the Processor will process the request to the extent it is lawful and will reasonably fulfil such request in accordance with its standard operational procedures to the extent possible.

8.2 In the event that the Processor receives a request from a Data Subject in relation to Personal Data, the Processor will refer the Data Subject to the Controller unless otherwise prohibited by law. The Controller shall reimburse the Processor for all costs incurred resulting from providing reasonable assistance in dealing with a Data Subject request. In the event that the Processor is legally required to respond to the Data Subject, the Controller will fully cooperate with the Processor as applicable.

9. Audit

9.1 The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections.

9.2 Any audit conducted under this DPA shall consist of examination of the most recent reports, certificates and/or extracts prepared by an independent auditor bound by confidentiality provisions similar to those set out in the Agreement. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Controller, the Controller may conduct a more extensive audit which will be: (i) at the Controller's expense; (ii) limited in scope to matters specific to the Controller and agreed in advance; (iii) carried out during the Processor's usual business hours and upon reasonable notice which shall be not less than 4 weeks unless an identifiable material issue has arisen; and (iv) conducted in a way which does not interfere with the Processor's day-to-day business.

9.3 This clause shall not modify or limit the rights of audit of the Controller, instead it is intended to clarify the procedures in respect of any audit undertaken pursuant thereto.

10. Personal Data Breach

10.1 The Processor shall notify the Controller without undue delay after becoming aware of (and in any event within 72 hours of discovering) any accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to any Personal Data ("**Personal Data Breach**").

9.2 The Processor will take all commercially reasonable measures to secure the Personal Data, to limit the effects of any Personal Data Breach, and to assist the Controller in meeting the Controller's obligations under applicable law.

11. Compliance, Cooperation and Response

11.1 The Processor will notify the Controller promptly of any request or complaint regarding the processing of Personal Data, which adversely impacts the Controller, unless such notification is not permitted under applicable law or a relevant court order.

11.2 The Processor may make copies of and/or retain Personal Data in compliance with any legal or regulatory requirement including, but not limited to, retention requirements.

11.3 The Processor shall reasonably assist the Controller in meeting the Controller's obligations to carry out data protection impact assessments (DPIAs), taking into account the nature of processing and the information available to the Processor.

11.4 The Controller shall notify the Processor within a reasonable time, of any changes to applicable data protection laws, codes or regulations which may affect the contractual duties of the Processor. The Processor shall respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organisational measures to maintain compliance. If the Processor is unable to accommodate the necessary changes, the Controller may terminate the part or parts of the Services which give rise to the non-compliance. To the extent that other parts of the Services provided are not affected by such changes, the provision of those Services shall remain unaffected.

11.5 The Controller and the Processor and, where applicable, their representatives, shall cooperate, on request, with a Supervisory Authority in the performance of their respective obligations under this DPA and Data Protection Law.

12. Liability

12.1 The limitations on liability set out in the Agreement apply to all claims made pursuant to any breach of the terms of this DPA.

12.2 The parties agree that the Processor shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Sub-Processors to the same extent the Processor would be liable if performing the services of each Sub-Processor directly under the terms of the DPA, subject to any limitations on liability set out in the terms of the Agreement.

12.3 The parties agree that the Controller shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Affiliates as if such acts, omissions or negligence had been committed by the Controller itself.

12.4 The Controller shall not be entitled to recover more than once in respect of the same loss.

13. Term and Termination

13.1 The Processor will only process Personal Data for the term of the DPA. The term of this DPA shall coincide with the commencement of the Agreement and this DPA shall terminate automatically together with termination or expiry of the Agreement.

14. Deletion and Return of Personal Data

14.1 The Processor shall at the choice of the Controller, upon receipt of a written request received within sixty (60) days the end of the provision of the Services, delete or return Personal Data to the Controller. The Processor shall in any event delete all copies of Personal Data in its systems within sixty (60) days of the effective date of termination of the Agreement unless: (i) applicable law or regulations require storage of the Personal Data after termination; or (ii) partial Personal Data of the Controller is stored in backups, then such Personal Data shall be deleted from backups up to one (1) year after the effective date of termination of the Agreement.

15. General

15.1 This DPA sets out the entire understanding of the parties with regards to the subject matter herein.

15.2 Should a provision of this DPA be invalid or become invalid then the legal effect of the other provisions shall be unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended commercially and shall replace the invalid provision. The same shall apply to any omissions.

15.3 Subject to any provision of the SCCs to the contrary this DPA shall be governed by the laws of England and Wales. The courts of England shall have exclusive jurisdiction for the settlement of all disputes arising under this DPA.

15.4 The parties agree that this DPA is incorporated into and governed by the terms of the Agreement.

Exhibit A - List of Parties, Description of Processing and Transfer of Personal Data, Competent Supervisory Authority

MODULE TWO: CONTROLLER TO PROCESSOR

A. LIST OF PARTIES

The Controller:

means the Customer.	
Address:	As set out for the Customer in the Agreement.
Contact person's name, position and contact details:	As provided by the Customer in its account and used for notification and invoicing purposes.
Activities relevant to the data transferred under the SCCs:	Use of the Services.
Signature and date:	By entering into the Agreement, the Controller is deemed to have signed the SCCs incorporated into this DPA and including their Annexes, as of the Effective Date of the Agreement.
Role:	Data Exporter.
Name of Representative (if applicable):	Any UK or EU representative named in the Controller's privacy policy.

The Processor:

means the Company: Donorfy Limited

Address:	Amelia House, Crescent Road, Worthing, BN11 1QR, England
Contact person's name, position and contact details:	Robin Fisk Chief Executive Officer Robin.fisk@donorfy.com
Activities relevant to the data transferred under the SCCs:	The provision of cloud computing solutions to the Controller under which the Processor processes Personal Data upon the instructions of the Controller in accordance with the terms of the Agreement.
Signature and date:	By entering into the Agreement, the Processor is deemed to have signed the SCCs, incorporated into this DPA, including their Annexes, as of the Effective Date of the Agreement.
Role:	Data Importer
Name of Representative (if applicable):	dpoeu@donorfy.com

B. DESCRIPTION OF PROCESSING AND TRANSFERS

Categories of Data Subjects:	• The Controller's constituents – including donors, supporters, volunteers, funders, customers, subscribers, members, beneficiaries, service users, advocates and other stakeholders. • Employees, freelancers and contractors of the Controller and other users added by the Controller from time to time. • Authorised users, Affiliates and other participants from time to time to whom the Controller has granted the right to access the Services in accordance with the terms of the Agreement. • Clients of the Controller and individuals with whom those end users communicate with by email and/or instant messaging. • Service providers of the Controller.

	• Other individuals to the extent identifiable in the content of emails or their attachments or in archiving content.
Categories of Personal Data:	The Controller may submit Personal Data to the Services, the extent of which is determined and controlled by the Controller. The Personal Data includes but is not limited to: • Personal details, names, user names, passwords, email addresses and telephone numbers of users and prospects. • Personal Data derived from user and prospect use of the Services such as records and business intelligence information. • Personal Data within email and messaging content which identifies or may reasonably be used to identify, data subjects. • Meta data including sent, to, from, date, time, subject, which may include Personal Data. • Financial data of users. • Data concerning education and profession. • Data revealing political opinions, image and sound recordings. • File attachments that may contain Personal Data. • Survey, feedback and assessment messages. • Information offered by users as part of support enquiries. • Financial contributions. • Prospect research data as researched and recorded by the Controller. • Other data added by the Controller from time to time.
Sensitive Data:	Personal Data transferred includes but is not limited to the following special categories of data: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Data concerning health
The frequency of the processing and transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous basis for the duration of the Agreement.
Nature of the processing:	Processing operations include but are not limited to: management of constituent data, donations, communications,

	collection of Gift Aid, and fundraising activities. These operations relate to all aspects of Personal Data processed.
Purpose(s) of the data transfer and further processing:	Personal Data is transferred to sub-contractors who need to process some of the Personal Data in order to provide their services to the Processor as part of the Services provided by the Processor to the Controller.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:	Unless agreed otherwise in writing, for the duration of the Agreement, subject to clause 14 of the DPA.
For transfers to (Sub-) processors, also specify subject matter, nature and duration of the processing:	The Sub-Processor list sets out the Personal Data processed by each Sub-Processor and the services provided by each Sub-processor.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies (e.g. in accordance with Clause 13 of the SCCs)	Where the EU GDPR applies, the Irish Data Protection Authority – The Data Protection Commission. Where the UK GDPR applies, the UK Information Commissioner's Office, (ICO). Where the FDPA applies, the Swiss Federal Data Protection and Information Commissioner, (FDPIC).

MODULE THREE: PROCESSOR TO PROCESSOR

A. LIST OF PARTIES

The Data Exporter: is the Company.

The Data Importers: are the Sub-Processors named in the Sub-Processor list which contains the name, address, contact details and activities relevant to the data transferred to each Data Importer.

B. DESCRIPTION OF PROCESSING AND TRANSFERS

The Sub-Processor list includes the information about the processing and transfers of the Personal Data, for each Data Importer:

- categories of Data Subjects
- categories of Personal Data
- the nature of the processing
- the purposes of the processing

Personal Data is processed by each Data Importer:

- on a continuous basis
- to the extent necessary to provide the Services in accordance with the Agreement and the Data Exporter's instructions.
- for the duration of the Agreement and subject to clause 14 of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

The competent Supervisory Authority of the Data Exporter shall be:

- Where the EU GDPR applies, the Irish Data Protection Authority – The Data Protection Commission.
- Where the UK GDPR applies, the UK Information Commissioner's Office, (ICO).
- Where the FDPA applies, the Swiss Federal Data Protection and Information Commissioner, (FDPIC).

Exhibit B Technical and Organisational Security Measures

(Including Technical and Organisational Measures to Ensure the Security of Data)

Below is a description of the technical and organisational measures implemented by the Processor (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Where applicable this Exhibit B will serve as Annex II to the SCCs.

Measure	**Description**
Solution Architecture	Donorfy is Software-as-a-Service, running on Microsoft Azure's Platform-as-a-Service (read more) which securely: ● hosts and delivers the software - which means the Donorfy web app, Forms, the API, the Data Service etc ● hosts the data Microsoft Azure is a global cloud computing service. It has a network of data centres. Donorfy is hosted in the North Europe data centre, which is located in Dublin, Republic of Ireland. Clients opting for Own Azure can choose the data centre in which they would like their data to reside "at rest". Regardless of the data residency, it is still processed by the software in the North Europe data centre.
Organisation and Personnel	**Donorfy Security Group** We believe that security is not just the responsibility of the product development team, it is company-wide. Therefore we have established a cross-functional Security Group that meets quarterly to review security as a whole, discuss new developments and plan their implementation if appropriate. **Cyber insurance** Donorfy Ltd is covered by cyber insurance from Hiscox.

	Training Donorfy team members have to undergo security training from CyberClear Academy. **Access to the infrastructure** Access to the SaaS / PaaS infrastructure is provided to appropriate personnel, and is protected by Two-Factor Authentication and IP filtering.
Physical Security	As would be expected from one the leading global cloud hosts, Microsoft have comprehensive measures in place to secure all of their data centres from physical as well as electronic intrusion. This includes access request and approval protocols; perimeter and building access controls; biometric authentication; time-limited visits; full-body scanning and zoned access areas. Read more.
Encryption	**Encryption of data at rest** Donorfy employs Transparent Data Encryption (read more) , which is a feature of the Azure SQL database in which Donorfy data is stored. This extends to backed up data too. **Encryption of data in transit** Donorfy uses the https, otherwise known as Secure Sockets Layer (read more) to encrypt data in transit - for example between the browser and the Donorfy web app.
Security features in the Donorfy app	Donorfy contains numerous safeguards to enhance its security. These include: ● HTTP response headers are optimised to provide a high level of protection, achieving an 'A' rating on the independent security site securityheaders.com. ● Donorfy notifies users of logins from previously unknown locations. This enables you to take necessary action (eg. changing passwords) should you suspect a rogue login. ● Two-Factor Authentication. ● Automated sign-out after an hour's inactivity.

	• Users of the app are assigned an account type which governs the data that can be seen, retrieved and downloaded. • Donorfy Forms and donation widgets are protected by Google reCAPTCHA v3 and IP filtering, which together provide an effective defence for card testing and bots. Forms automatically block IPs if multiple repeat attempts at submitting them are identified in a short space of time. • No payment card or bank details are stored in Donorfy, We store tokens instead, with the card and account details held by the payment processors Stripe, PayPal and GoCardless. • The Donorfy API and Data Service are IP filtered. • HTML sanitisation - Donorfy checks uploaded content for potentially malicious content, such as the <code>, <object>, <embed> and <link> tags, and removes them accordingly. This prevents malicious code from being injected and subsequently executed.
The Donorfy Security Centre	The Security Centre promotes good practice by highlighting areas of potential weakness in the Customer's configuration of Donorfy. A security rating is provided, along with tips about how to improve it.
Software and Development	Donorfy is developed and tested according to the standards of the Open Web Application Security Project (OWASP).
Anti-Virus and Malware	Donorfy is scanned daily for viruses and malware, using Microsoft Defender.
Backup	Donorfy data is backed up daily to two locations: • Azure - North Europe data centre • AWS - Frankfurt data centre Backups are encrypted. Own Azure clients can add additional backups to locations of their choice.

Compliance Standards and Certifications	Microsoft Azure has many compliance certifications including the information security standard ISO 27001. The full list of certifications can be viewed here.
Pen Testing	Penetration (pen for short) testing is an authorised attempt to hack a computer system with the objective of evaluating the system's security and identifying security vulnerabilities so that they can be fixed. **Donorfy pen testing** We periodically commission pen testing on the entire Donorfy solution. We use a variety of pen test agencies to do this, and implement recommendations from their reports accordingly. If you'd like to know more about this please click on the button below to request more info. You will be asked to accept our non-disclosure agreement. **Independent Pen Testing** Customer's can commission their own pen testing of Donorfy (the software and/or the database) according to the following terms: ● It is available only to Customer's with an active paid-for subscription. ● Before the testing can be done, Donorfy must approve: o the organisation / person doing the pen testing; o the scope of the testing to be performed; o its timing. ● The full cost will be paid by you. ● If the pen test requires Donorfy's involvement there may be an associated charge. We will confirm that if and when it arises. ● The full report is made available to Donorfy within 30 days of it becoming available. ● The report must not be published or made available to any third parties. ● Donorfy reserves the right to use the report ● Donorfy may act on recommendations from your pen test report, but doesn't guarantee if or when.

	Failure to comply with the terms may result in you losing access to Donorfy.
Data Processor	In the eyes of the GDPR Donorfy Limited is the Data Processor (read more) and you, the Customer are the Data Controller. As such we have a comprehensive data processing agreement which sets our commitments and obligations as your data processor. This is updated from time to time in line with legislation and improvements. The full DPA can be viewed here. Your data is safe and sound in our servers. But sometimes your data may be handled by other parties - for example when you integrate Donorfy with Mailchimp. These sub-processors, as they are called in GDPR, are listed here.
Sensitive Data	Credentials such as passwords and API keys are strongly encrypted. Donorfy does not store any usable credit card or bank account details. They are stored by the payment processors' systems (see Integrations) which themselves are subject to the strictest compliance regulations.
Donorfy's role is enabling you to comply with data protection legislation	Donorfy provides a host of features to enable you to meet your obligations as a data controller, and to enable you to set and comply with your own data management policies. These features include: ● Legitimate Interest or Opt In policy, for each comms channel. ● Preference Centre. ● Subject Access Request (coming soon). ● Bulk archive and bulk delete to ensure data retention policy can be adhered to. ● Filtering based on channel permissions.

Exhibit C

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The date set out in Annex I of the Approved EU SCCs.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: the Customer named in the Agreement. Main address (if a company registered address): As set out in Annex I of the Approved EU SCCs. Official registration number (if any) (company number or similar identifier): Where set out in the Agreement.	Full legal name: Donorfy Limited. Main address: Amelia House, Crescent Road, Worthing, BN11 1QR, England. Official registration number: 08922148
Key Contact	Full Name (optional): As set out in Annex I of the Approved EU SCCs. Job Title: As set out in Annex I in the Approved EU SCCs Contact details including email: As set out in Annex I the Approved EU SCCs.	Full Name: Robin Fisk Job Title: Chief Executive Officer Contact details including email: robin.fisk@donorfy.com
Signature (if required for the purposes of Section 2)	no signature is required.	no signature is required.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 11 (Option)	Clause 9a General Authorisation	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	no	not used	-	-	-
2	yes	not used	yes	30 days	-
3	no	not used	no	-	-
4	no	not used	-	-	no

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: for Module 2 and Module 3
Annex 1B: Description of Transfer: for Module 2 and Module 3
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: for Module 2

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Importer Exporter

Part 2: Mandatory Clauses

Entering into this Addendum

Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.

UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

> "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of

"Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including

the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.