ENGAGING NETWORKS, LTD.
Personal Data Processing Agreement

This agreement is dated [INSERT] and references the Master Services Agreement agreed between the parties dated [INSERT]

PARTIES

(1) Party signed to Master Services Agreement with Engaging Networks **("Client")**

(2) ENGAGING NETWORKS LIMITED incorporated and registered in England and Wales with company number 03848111 whose registered office is at Dixcart House Addlestone Road, Bourne Business Park, Addlestone, Surrey, KT15 2LE **("Engaging Networks")**

BACKGROUND

(A) Engaging Networks and Client are parties to a Master Services Agreement (the "Master Services Agreement") outlining the services contracted for between the parties, and any subsequent renewals and extensions which remain in full force and effect subject to the terms and conditions herein.

(B) Client subscribes to the Services set forth in the Master Services Agreement, as amended from time to time. For the purposes of provision of services, Engaging Networks is to be regarded as a Processor, and Client a Controller of personal data.

(C) This Data Processing Agreement (**Agreement**) sets out the additional terms, requirements and conditions on which Engaging Networks will process Personal Data when providing services under the Master Services Agreement and in accordance with Applicable Data Protection Law.

AGREED TERMS

1. DEFINITIONS AND INTERPRETATION

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

Applicable Data Protection Law: refers to all or any data protection legislation applicable to Engaging Networks acting as a processor in the course of providing services for client.

Where the Processor is based in the United Kingdom and the Controller may be also, for the purposes of the processing of personal data of data subjects who are in the United Kingdom this shall mean the United Kingdom General Data Protection Regulation 'UK GDPR' the Data Protection Act 2018 (UK) and any applicable national implementing laws, regulations and secondary legislation in England and Wales relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time.

Where the Controller is based in the EEA or where the Processor is processing the personal data of data subjects who are in the EEA this shall mean the General Data Protection Regulation (Regulation 2016/679) 'GDPR' 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.

Where the processor is based in the United States of America and the data subjects are in the United Kingdom, the EEA or Switzerland any processing will take place under the terms of the EU-US Data Privacy

Framework, the UK Extension to the EU-US Data Privacy Framework or the Swiss-US Data Privacy Framework. No processing will take place until the processor is enrolled against these Frameworks with the US Department of Commerce.

Authorized Persons: the persons or categories of persons that the Client authorizes to give Engaging Networks personal data processing instructions.

Business Purposes: the services described in the Master Services Agreement and in *Schedule A*.

Data Subject: an identifiable natural person.

Engaging Networks USA: means ENGAGING NETWORKS USA INC incorporated and registered in the state of Delaware with file number 4538098 whose registered address is Corporation Trust Center, 1209 Orange St, Wilmington 19801, Delaware, USA

Personal Data: means any information relating to an identified or identifiable natural person that is processed by Engaging Networks as a result of, or in connection with, the provision of the services under the Master Services 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.

Processing, processes and process: either any activity that involves the use of Personal Data or as Applicable Data Protection Law otherwise define processing, processes or process.

ICO: Information Commissioner's Office, the regulatory authority for Data Protection in the United Kingdom. Any reference to the ICO shall be taken to mean the Commissioner in that capacity also 'the commissioner' as described in Art 51 UK GDPR.

International Data Transfer Agreement "IDTA" This shall refer to relevant contractual clauses which shall be subject to relevant UK government or Information Commissioner's Office 'ICO' approval for the purposes of providing a mechanism for the transfer of personal data outside of the UK.

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. Or otherwise defined in accordance with applicable data protection law.

Special Categories of Personal Data: any category of personal data specified in Article 9(1) of the UK GDPR or GDPR whichever shall apply

Standard Contractual Clauses (the "SCC"): Refers to the model contractual clauses as approved by the European Commission for international data transfers from controllers or processors in the EU/EEA on 4 June 2021 or any future model contractual clauses which compliment or replace them.

Supervisory Authority: independent public authority as described in Article 51 GDPR and 'the commissioner' as described in Art 51 UK GDPR whichever shall be relevant in accordance with Applicable Data Protection Law.

UK Government: shall mean the Government of the United Kingdom, and in particular with respect applicable data protection law, the Secretary of State of that government.

1.2 This Agreement is subject to the terms of the Master Services Agreement and is incorporated into the Master Services Agreement. Interpretations and defined terms set forth in the Master Services Agreement apply to the interpretation of this Agreement. This Data Protection Addendum shall take effect from the effective date of the Master Services Agreement.

1.3 In conjunction with the Master Services Agreement *Schedule A* describes the subject matter, duration, nature and purpose of processing and the Personal Data categories and Data Subject types in respect of which Engaging Networks may process to fulfil the Business Purposes of the Master Services Agreement.

1.4 The Schedules form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Schedules.

1.5 A reference to writing or written includes faxes and email, both subject to confirmation of receipt by the receiving party.

1.6 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this Agreement and any provision contained in the Schedules, the provision in the body of this Agreement will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in the Schedules, the provision contained in the Annexes will prevail;

(c) any of the provisions of this Agreement and the provisions of the Master Services Agreement, the provisions of this Agreement will prevail; and

2. PERSONAL DATA TYPES AND PROCESSING PURPOSES

2.1 The Client and Engaging Networks acknowledge that for the purpose of Applicable Data Protection Law, the Client is the controller, Engaging Networks is the processor.

2.2 Client agrees and acknowledges that Engaging Networks, as a processor, provides Client's access to a range of tools which may be of assistance to the Client in fulfilling its obligations, as a controller, under Applicable Data Protection Law. These tools include, but are not limited to, the ability to amend, delete, import, export, access, etc, Personal Data.

2.3 Client shall, in its use of Engaging Networks' Services, process Personal Data in accordance with Applicable Data Protection law, and further the client:

i. retains control of the Personal Data and remains responsible for its compliance obligations under the Applicable Data Protection Law

ii. shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Client acquired Personal Data.

iii. shall ensure instructions to Engaging Networks regarding the Processing of Personal Data are compliant with Applicable Data Protection Law.

3. ENGAGING NETWORKS' DUTIES AND OBLIGATIONS

3.1 Engaging Networks will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Client's written instructions from Authorized Persons. Engaging Networks will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or Applicable Data Protection Law.

3.2 Where Client cannot reasonably perform the task themselves, Engaging Networks will promptly comply with any Client request or instruction from Authorized Persons requiring Engaging Networks to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorized processing.

3.3 Engaging Networks will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Client or this Agreement specifically authorizes the disclosure, or as required by law.

3.4 If a law, court, regulator or supervisory authority requires Engaging Networks to process or disclose Personal Data, Engaging Networks must first inform the Client of the legal or regulatory requirement and give the Client a reasonable opportunity to object or challenge the requirement (taking into account any time limit in complying with such requirement), unless the law prohibits such notice.

3.5 Engaging Networks will reasonably assist the Client with meeting the Client's compliance obligations under the Applicable Data Protection Law, taking into account the nature of Engaging Networks' processing and the information available to Engaging Networks, including in relation to data subject rights, data protection impact assessments and reporting to and consulting with relevant supervisory authorities.

3.6 Engaging Networks will inform immediately the client if, in its opinion, it receives an instruction from Client which infringes Data Protection Law.

3.7 When aware of changes, Engaging Networks must promptly notify the Client of any changes to Applicable Data Protection Law that may adversely affect Engaging Networks' performance of the Master Services Agreement or its obligations as a processor as a result of the terms of the agreement herein.

4. ENGAGING NETWORKS' EMPLOYEES

4.1 Engaging Networks will ensure that all its employees:

(a) are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;

(b) have undertaken training with respect their obligations related to Applicable Data Protection Law regarding handling Personal Data and how it applies to their particular duties in connection with the Services and this Agreement; and

(c) are aware both of Engaging Networks' duties and their personal duties and obligations under the Applicable Data Protection Law and this Agreement.

4.2 Engaging Networks will take reasonable steps to ensure the reliability, integrity and trustworthiness of, and conduct background checks consistent with applicable law on all of Engaging Network employees with access to the Personal Data.

5. SECURITY

5.1 Engaging Networks, will at all times implement appropriate technical and organizational measures against unauthorized 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 Personal Data including, but not limited to, the security measures set out in Schedule *B*. Engaging Networks will document those measures in writing and periodically review them to ensure they remain current and complete, at least annually.

6. PERSONAL DATA BREACH

6.1 Engaging Networks will within a reasonable time and without undue delay and in any case within 24 hours notify the Client if it becomes aware of:

(a) any accidental, unauthorized or unlawful processing of the Personal Data; or

(b) any incident which may be regarded a Personal Data Breach with respect Applicable Data Protection Law.

6.2 Where Engaging Networks becomes aware of (a) and/or (b) above, it shall, without undue delay, also provide the Client with the following information:

(a) description of the nature of (a) and/or (b), including the categories and approximate number of both Data Subjects and Personal Data records concerned; and

(b) description of the measures taken or proposed to be taken to address (a), including measures to mitigate its possible adverse effects.

6.3 Immediately following a) or b) above the parties will co-ordinate with each other to investigate the matter. Engaging Networks will reasonably co-operate with the Client in the Client's handling of the matter, including:

(a) assisting with any investigation;

(b) making available all relevant records, logs, files, data reporting and other materials required to comply with Applicable Data Protection Law or as otherwise reasonably required by the Client; and

(c) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Personal Data processing.

6.4 Engaging Networks will cover all reasonable expenses associated with the performance of the obligations under this clause unless the matter arose from the Client's specific instructions, negligence, wilful default or breach of this Agreement, in which case the Client will cover all reasonable expenses.

6.5 In accordance with the conditions of the Master Services Agreement, Engaging Networks will also reimburse the Client for actual reasonable expenses (including legal expenses) that the Client incurs when responding to a Personal Data Breach to the extent that Engaging Networks caused, either directly or indirectly, such a Personal Data Breach.

7. CROSS-BORDER TRANSFERS OF PERSONAL DATA

7.1 For the purposes of this clause:

(a) The Client agrees to the transfer of the Personal Data to Engaging Networks USA in the United States of America under the terms of the EU/UK/CH -US Data Privacy Framework for the purposes of technical and other support (but for no other purpose).

Engaging Networks USA is a wholly-owned subsidiary of Engaging Networks and provides maintenance and support services to Engaging Networks, in the course of which it may access Personal Data as a sub-processor of Engaging Networks. For the purposes of this transfer a relevant transfer mechanism shall be in place in order to affect the legality of the transfer. Any transfer shall relate only to access of the personal data, and this personal data shall be subject to encryption in accordance with Schedule A and B as well as a 'Linked Agreement' signed between Engaging Networks Limited and Engaging Networks USA.

(b) the Client agrees further to the transfer of the Personal Data to Engaging Networks' servers in Canada (hosted by a third-party sub-processor as referred to in clause 8) for processing; and agrees and acknowledges that as of the Effective Date of this Agreement, Canada has been deemed adequate for transfers of Personal Data outside of the European Union, the United Kingdom and Switzerland; and

7.2 Other than that set out in 7.1 above, Engaging Networks shall seek the agreement of the Client prior to the transfer of personal data outside of the United Kingdom or the European Union. Where such consent is granted, Engaging Networks may only process, or permit the processing, of Personal Data outside the United Kingdom or the European Union under the following conditions:

(a) Where the relevant authorities in either the United Kingdom, the European Union or Switzerland make a finding that the territory provides adequate protection for the privacy rights of individuals.

(b) Engaging Networks participates in another valid cross-border transfer mechanism, either SCC, IDTA, Binding Corporate Rules, Code of Conduct or otherwise, in compliance with the Applicable Data Protection Law so that Engaging Networks (and, where appropriate, the Client) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Applicable Data Protection Law.

(c) Engaging Networks must identify the transfer mechanism that enables the parties to comply with these cross-border data transfer provisions and Engaging Networks must immediately inform the Client of any change to that status.

(d) The transfer otherwise complies with Applicable Data Protection Law.

8. SUBPROCESSORS

8.1 The Client hereby agrees to the use of all sub-processors by Engaging Networks as are listed as sub-processors in Schedule A from the Effective date. A full list of current Engaging Networks Sub-processors will be maintained online at https://knowledge.engagingnetworks.net/softwaresecurityandprivacy/engaging-networks-sub-processors-list

8.2 Subsequent to the effective date Engaging Networks may only authorize additional sub-processors to process the Personal Data if:

(a) the Client is provided with an opportunity to object to the appointment of the sub-processor within thirty (30) days of Engaging Networks supplying the Client with full details regarding such sub-processor.

(b) Engaging Networks enters into a written contract with the sub-processor which determines the nature and duration of the processing that guarantees a similar level of data protection compliance and information security to that provided for herein and, upon the Client's written request, provides the Client with copies of such contract;

8.3 Where the sub-processor fails to fulfil its obligations under such written agreement, Engaging Networks remains fully liable to the Client for the sub-processor's performance of its agreement obligations and in accordance with the conditions of the Master Services Agreement.

8.4 On the Client's written request and at the Client's cost, Engaging Networks will audit a sub-processor's compliance with its obligations regarding the Client's Personal Data and provide the Client with the audit results.

9. COMPLAINTS, DATA SUBJECT REQUESTS AND THIRD-PARTY RIGHTS

9.1 Engaging Networks must not disclose the Personal Data to any Data Subject or to a third party other than at the Client's request or instruction, as provided for in this Agreement or as required by law.

9.2 Engaging Networks will notify the Client immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Applicable Data Protection Law. Engaging Networks must notify the Client as soon as reasonably possible if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under Applicable Data Protection Law.

9.3 While Client, via the programmes provided by Engaging Networks, is able to access the personal data that they Control for the purposes of exercising data subject rights or engaging with supervisory authorities, in the extremely rare scenario of it being necessary for the involvement of Engaging Networks to aid this response, Engaging Networks will take such reasonable technical and organisational measures as may be appropriate, and promptly provide such information to the Client as the Client may reasonably require, to enable the Client to comply with:

(a) the rights of Data Subjects under Applicable Data Protection Law 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; and

(b) information or assessment notices served on the Client by any supervisory authority under Applicable Data Protection Law.

10. TERM AND TERMINATION

10.1 This Agreement will remain in full force and effect so long as:

(a) the Master Services Agreement remains in effect (including subsequent renewals and extensions of the same); or

(b) Engaging Networks retains any Personal Data related to the Master Services Agreement in its possession or control (the "**Term"**).

10.2 Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Master Services Agreement in order to protect Personal Data will remain in full force and effect.

10.3 Engaging Networks' failure to comply with the terms of this Agreement is a material breach of the Master Services Agreement. In such event, the Client may terminate the Master Services Agreement as provided therein.

10.4 If a change in any Applicable Data Protection Law prevents either party from fulfilling all or part of its Master Services Agreement obligations, this shall not end the contract between the parties as expressed in the Master Services Agreement, the parties will suspend the processing of Personal Data until that processing complies with the new requirements.

11. DATA RETURN AND DESTRUCTION

11.1 At the Client's request, Engaging Networks will give the Client a copy of or access to all or part of the Client's Personal Data in its possession or control in .csv format. This may be achieved as far as possible by the use of the software tools provided to the Client by Engaging Networks as part of its services.

11.2 On termination of the Master Services Agreement for any reason or expiry of its term, Engaging Networks will securely delete or destroy or, if directed in writing by the Client, return and not retain, all or any Personal Data related to this Agreement in its possession or control.

11.3 If any law, regulation, or government or regulatory body requires Engaging Networks to retain any documents or materials that Engaging Networks would otherwise be required to return or destroy, it will notify the Client in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

12. RECORDS

12.1 Engaging Networks will keep detailed, accurate and up-to-date written records regarding any processing of Personal Data it carries out for the Client, including but not limited to, the access, control and security of the Personal Data, approved sub-processors and affiliates, the processing purposes, categories of processing, any transfers of personal data to a third country and related safeguards, and a general description of the technical and organizational security measures referred to herein ("**Records**").

13. AUDIT

13.1 Subject to this Section, Engaging Networks will permit the Client and its third-party representatives to audit Engaging Networks' compliance with its Agreement obligations, no more than once every 12 months (except in the case of suspected breach of this Agreement or fraud, in which case such audit right shall be unlimited) and on at least thirty days' prior written notice, during the Term. Engaging Networks shall provide Client and its third-party representatives all reasonably necessary assistance to conduct such audits.

The Client will pay Engaging Networks' actual reasonable costs incurred and directly arising from such audit.

13.2 The notice requirements in *Clause 13.1* will not apply if the Client reasonably believes that a Personal Data Breach occurred or is occurring, or Engaging Networks is in breach of any of its obligations under this Agreement Applicable Data Protection Law.

13.3 If a Personal Data Breach occurs or is occurring, or Engaging Networks becomes aware of a breach of any of its obligations under this Agreement or any Applicable Data Protection Law, Engaging Networks will:

(a) promptly commence its own audit to determine the cause;

(b) produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;

(c) provide the Client with a copy of the written audit report; and

(d) remedy any deficiencies identified by the audit within ninety (90) days of completing the audit referred to herein.

13.4 At least once a year, Engaging Networks will conduct regular audits of its Personal Data processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this Agreement.

13.5 On the Client's written request, Engaging Networks will make all of the relevant audit reports available to the Client for review. The Client will treat such audit reports as Engaging Networks' confidential information under this Agreement.

14. WARRANTIES

14.1 Engaging Networks warrants that:

(a) Engaging Networks shall seek to ensure that employees have received required training on Applicable Data Protection Law relating to the Personal Data;

(b) Engaging Networks shall seek to ensure that anyone operating on its behalf will process the Personal Data in compliance with Applicable Data Protection Law and other laws, enactments, regulations, orders, standards and other similar instruments;

(c) Engaging Networks has no reason to believe that Applicable Data Protection Law prevents it from providing any of the Master Services Agreement's contracted services; and

(d) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures, including the security measures set out in Schedule B, to prevent the unauthorized or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:

(i) the harm that might result from such unauthorized or unlawful processing or accidental loss, destruction or damage;
(ii) the nature of the Personal Data protected; and
(iii) comply with all Applicable Data Protection Law and its information and security policies.

14.2 Client warrants and represents that Engaging Networks' expected use of the Personal Data for the Business Purposes and as specifically instructed by the Client will comply with Applicable Data Protection Law.

14.3 Client also warrants, as the data controller, that they must take appropriate technical and organisational measures of their own to prevent the unauthorized or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data and ensure a level of security appropriate to the Applicable Data Protection Law.

15. SEVERANCE

If any provision or part-provision of this Agreement 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 this Agreement.

16. LIABILITY

Each party fully indemnifies and holds harmless the other from and against any and all losses, claims, fines, investigations, damages, costs, charges, expenses (including reasonable legal expenses), liabilities, demands, proceedings and actions which the other party may sustain or incur or which may be brought or established against it by any person to the extent that these arise out of, or are in relation to, a breach by that party of any of the terms of this Data Processing Agreement or by reason of the negligence on the part of that party in relation to this Agreement. Any indemnification shall not supersede any term agreed in the Master Services Agreement between the parties.

17. GOVERNING LAW AND JURISDICTION

Where UK GDPR applies to the personal data subject to data processing, the agreement shall be subject to English Law and English Courts, who shall have jurisdiction for its interpretation and enforcement.

Where GDPR applies to the personal data subject to data processing the agreement shall be subject to the laws of the Republic of Ireland and the courts of the Republic of Ireland, who shall have jurisdiction for its interpretation and enforcement.

Where the Swiss – US Data Protection Framework and Swiss Data protection Law applies the agreement shall be subject to the laws of Switzerland and the courts of Switzerland who shall have jurisdiction for its interpretation and enforcement.

This agreement has been entered into on the date stated at the beginning of it.

Signed by

Job title:

for and on behalf of **‘Client’**

Client name:

Signed by

Job title:

for and on behalf of **Engaging Networks Limited**

SCHEDULE A

PERSONAL DATA PROCESSING PURPOSES AND DETAILS

Subject matter of processing:

Personal Data collected by the Client using the Engaging Networks service

Duration of Processing:

Personal Data will be processed for so long as the Client remains a client of Engaging Networks

Nature of Processing:

Personal Data will be stored by Engaging Networks and retrieved by the Client using Engaging Networks software tools provided as part of the Engaging Networks Service for the purpose of communications with the individual data subjects.

The data will be gathered from individual data subjects who take campaigning actions on behalf of Client e.g. emailing their MP. Data will also be gathered from individuals making donations to Client. The data will be used to keep a record of who has taken supporter actions and for the purposes of communicating further updates, fundraising and campaign actions to individuals.

Personal Data may also be accessed by Engaging Networks in providing support and technical assistance to the Client.

Business Purposes:

The purpose of the processing is to enable the Client to communicate with its supporters in a targeted way, to obtain donations and to allow the Client to seek to involve its supporters in campaigns.

Personal Data Categories:

The personal data transferred concern the following categories of data:

Identity Data includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth, gender.
Contact Data includes billing address, delivery address, email address and telephone numbers.
Transaction Data includes details about payments to and from the data subject and other details of products and services the data subject has purchased. However, while the Client can use the Service to process financial payments, credit / debit card payments are done through a third party and no payment card details are retained by Engaging Networks.
Technical Data includes internet protocol (IP) address, login data.
Profile Data includes the personal data which the data exporter chooses to collect which can include username and password, purchases or orders made by the data subject, data subjects' interests, preferences, feedback and survey responses.
Marketing and Communications Data includes data subjects' preferences in receiving marketing from the data controller and third parties and data subjects' communication preferences.

Special Categories of Personal Data (Client please tick at least one box):

Personal data which is on, which reveals, or which concerns:

☐ racial or ethnic origin

☐ political opinions

☐ religious or philosophical beliefs

☐ none of the above

☐ genetic data

☐ biometric data (if used to identify a natural person)

☐ health

☐ sex life or sexual orientation

☐ criminal convictions and offences

☐ trade union membership

Data Subject Types:

Individual supporters and donors of the Client, Client employees when they have submitted a form.

Approved sub-processors:

An up-to-date sub-processors list is available at:

https://knowledge.engagingnetworks.net/softwaresecurityandprivacy/engaging-networks-sub-processors-list

Schedule B: Security

Engaging Networks is PCI-DSS Level 1Compliant. Maintaining PCI compliance requires that Engaging Networks engage in ongoing activities that include, but are not limited to, build, and maintain a secure network, protect sensitive data, maintain a vulnerability management program, implement strong security measures, and regularly test and monitor networks and systems. Additionally, Engaging Networks has achieved SOC 2 Type II compliance, and our computing providers have undergone SOC 2 compliance.

Any compliance program, including PCI -DSS requires that we implement both administrative and technical security controls to protect not only cardholder data, but also customer data as well. Some of the measures we have implemented at Engaging Networks are below:

Design and implementation of a secure computing environment – Engaging Networks has designed a secure and compliant computing infrastructure that meets the requirements outlined by PCI-DSS. Our compute infrastructure utilizes fully CIS-Benchmark complaint images for our applications as well as leveraging AWS services for cache and database services. These components are configured with least-privilege access ensuring that the back-end components are run without administrative permissions. Combined with other best practices such as removing all unneeded utilities and applications, our internal application footprint is greatly reduced. No computer resources are directly connected to the Internet and all traffic inflows and outflows are monitored by real-time intrusion detection and prevention systems.

Protection of client data – Our platform utilizes multiple layers of role-based and user permissions. Service accounts are only assigned the minimum level of permissions required for application functionality. Client accounts can only access data that is part of their environment. Client-level permissions can further be assigned in a granular manner depending on how the platform is used. More information on user permissions can be found on the support pages. All user activity both front-end and back-end is logged and reviewed daily.

All administrator and support personnel who maintain the platform as well as provide client technical support have certain security requirements:

- All laptops and workstations used are documented on an asset inventory
- Two-Factor Authentication (2FA) is required to access the EN platform backend VPN and console application. 2FA is also mandated for any 3-rd party application used to support the environment (such as Jira, Salesforce, and other applications used by staff)
- Complex passwords are required to authenticate to the laptop or workstation
- Current antivirus and antimalware software is used on all devices
- Current and patched operating systems are used
- Full disk encryption used on all fixed drives
- All remote access and activity is monitored when accessing the EN platform and console applications
- All staff are required to use a VPN when working, as per the terms laid out in the company’s Remote Access Policy.

Data at rest on the platform is encrypted - We utilize encrypted storage volumes, snapshots, and backup images on the platform. Only Engaging Networks has access to the encryption keys preventing our service provider from having direct access to client data.

Data in transit on the platform is encrypted - All connections to Engaging Networks' dashboards and pages are made secure using TLS 1.2 or higher and encrypted using cyphers with 256-bit encryption.

Realtime Logging and Vulnerability Detection – In addition to using CIS-Benchmarks on compute infrastructure to define how logging is configured at the operating system level, our platform also generates detailed activity logs. Combined with the log data that is collected from our web-proxy, we have complete visibility to traffic flows entering our platform. We have multiple Web-Application-Firewalls (WAF) that identify, and automatically block suspect traffic such as spammers or exploitation attempts. Our platform is subject to enumeration and attack attempts on a daily basis; we review this data to understand new attack vectors and make adjustments to our platform as necessary to keep the platform secure and available to our customers.

Scans and Assessments - We regularly conduct both external and internal vulnerability scans against our platform. This is used to ensure that we are following best practices when it comes to configuration as well as to ensure patch compliance of the software in the environment. Prior to major software or infrastructure changes, we conduct penetration tests to ensure that no unforeseen vulnerabilities are introduced. For penetration testing, we follow PTES and OWASP best practices.

Personnel security – All Engaging Networks employees are subject to comprehensive background investigations at the time of hire. Employees are also required to complete multiple information security and customer data protection training courses annually. All employees and contractors are required to sign and understand acceptable use and provided access agreements prior to accessing our platform.