Engaging Networks Privacy Notice

Contents

This version was last updated on 20 February 2023.

Introduction

As individuals, we want to know that personal information about ourselves is handled properly and we and others have specific rights in this regard. In the course of its activities Engaging Networks will collect, store and process personal data, and it recognises that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

Status of the policy

This policy sets out Engaging Networks' rules on data protection, data subject rights and the data protection principles. These principles specify the legal conditions that must be satisfied in relation to the obtaining, handling, processing, transportation and storage of personal data. This privacy notice aims to give you information on how Engaging Networks collects and processes your personal data through your use of this website, including any data you may provide through this website when you sign up to receive information from the Company, receive a demonstration of or subscribe to the services (subject to the terms of the Company's Data Privacy Addendum executed upon subscription). This notice and all of our services are not intended for children and we do not knowingly collect data relating to children. Anyone who considers that this policy has not been followed in respect of personal data about themselves or others should raise the matter with the Data Protection Officer in the first instance (DPO@engagingnetworks.net (mailto:DPO@engagingnetworks.net)). Please also use the Glossary to understand the meaning of some of the terms used in this privacy notice.

1. Who we are

We are Engaging Networks, a registered company England and Wales. We provide a platform for not-for-profits. While we do not need to process certain data (e.g. Special Category data), our clients may do. We cannot advise or comment on the privacy policies or practices of organisations who use our platform, but we encourage responsible and compliant behaviours. Our office addresses/contact details are:

UK: Third Floor, 10-12 Emerald Street London WC1N 3QA United Kingdom Phone: +44 (0)20 7253 0753 Email: info@engagingnetworks.net (mailto:info@engagingnetworks.net)	**US:** One Thomas Circle, Suite 700 Washington DC 20005 United States Phone: (+1) 202 525-4910 Email: info@engagingnetworks.net (mailto:info@engagingnetworks.net)

For queries regarding personal data, our Data Protection Officer can be contacted at DPO@engagingnetworks.net (mailto:DPO@engagingnetworks.net). All users of Engaging Networks' UK services and website have the right to complain to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk (https://ico.org.uk/)) and to seek compensation through the Courts. You may contact our European Representative as Required under Article 27 GDPR as follows: Email: engagingnetworks@gdprnomrep.eu

(mailto:engagingnetworks@gdprnomrep.eu) Postal Address: Engaging Networks Nominated Representative, c/o Castlebridge Nominated Representative Services, Unit 7, 12 Mountjoy Square, Dublin 7, Ireland

2. Glossary of data protection terms

Data is recorded information whether stored electronically, on a computer, or in certain paper-based filing systems. **Data subjects** for the purpose of this policy include all living individuals about whom Engaging Networks holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information. **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in possession of Engaging Networks). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). It can even include a simple e-mail address. It is important that the information has the data subject as its focus and affects the individual's privacy in some way. Personal details such as someone's contact details or salary fall within the scope of The General Data Protection Regulation 2016/679 **Sensitive personal data** includes information about a person's political opinions, racial or ethnic origin, religious or similar beliefs, trade union membership, sexual orientation, genetic, biometric and health data. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned. **Data controllers** are the people or organisations who determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with GDPR. Engaging Networks is the data controller of all personal data belong to employees and clients of our company. Our clients are data controllers for all of their supporters' personal data. Only they determine the purposes and means of the processing of personal data that we carry out. **Data users** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following Engaging Networks' data protection and security policies at all times. **Data processors** include any person who processes personal data on behalf of a data controller. Engaging Networks is a processor of the personal data entrusted to us by our clients, who are the Data Controllers of their supporters' personal data. **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, storing, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties. We may not transfer/share personal data under the control of our clients without the client's explicit permission. **Third parties are:**

- Other companies in the Engaging Networks Group [acting as joint controllers or processors] and who are based outside of the United Kingdom (UK) or European Economic Area (EEA) and provide IT and system administration services and customer and sales support.
- Service providers acting as sub-processors based in Canada who provide IT and system administration services.
- Third party payment processors who may be located outside of the EEA – once personal details leave our servers, personal data is subject to payment processor terms.

3. The data we collect about you and how it is collected

Engaging Networks is the Data Controller for all personal data provided by employees, our customers (clients) own personal data and the personal data of potential customers. We are the Data Processor for all personal data that is provided to us by our clients (in particular their supporter records). The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in The General Data Protection Regulation 2016/679 (GDPR), the UK Data Protection Act 2018, and other regulations. Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). We may, depending on the processing, collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

- **Identity Data** includes first name, last name, username or similar identifier, title.
- **Contact Data** includes job title, employer information, work contact information, billing address, email address and telephone numbers.
- **Transaction Data** includes details about payments to and from you and other details of services to which you subscribe from us.
- **Technical Data** includes internet protocol (IP) address, browser type and version, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website.
- **Usage Data** includes information about how you use our website, products and services.
- **Marketing and Communications Data** includes your preferences in receiving marketing from us, Engaging Network Group, and our third parties and your communication preferences.
- We use personal data of users of our website to gather statistical inferences from it, for example, we may aggregate your usage data to calculate the percentage of users accessing a specific website feature. Any data derived from your personal data that

can be linked back to you is treated as personal data which will be used in accordance with this privacy notice.
- We may process Special Categories of Personal Data (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data) only where this has been collected by our clients, who in this instance are the data controllers.

Web Beacons

We may use automatic data collection technologies to collect certain information about your equipment, browsing actions, and patterns, which includes Web Beacons. Pages of our Website and our emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit us, for example, to count users who have visited those pages or opened an email and for other related website statistics (for example, recording the popularity of certain website content and verifying system and server integrity). We do not retain any financial data (including bank account and payment card details).

Third Party Links

Our website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

Personal data needed to provide you with our services

Where we need to collect personal data under the terms of a contract we have with our clients and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with our services). In this case, we may have to cancel a product or service you have with us, but we will notify you if this is the case at the time.

4. How is personal data collected?

We use different methods to collect data from and about you including through:

- **Direct interactions.** You may give us your identity and contact details by filling in online or paper forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:
    - apply for our services
    - create an account
    - subscribe to our service or publications
    - request marketing to be sent to you
    - give us feedback (e.g. in a survey)
- **Automated technologies or interactions.** As you interact with our website, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. You can refuse cookies by enabling cookie blocking technology. Alternatively, you can decide which cookies to allow when you visit our website for the first time (or after clearing your browser history) by making use of the cookie banner that appears. You can withdraw your cookie consent at any time by visiting our 'cookie policy' page.
- **Third parties or publicly available sources.** We may receive personal data about you from various third parties [and public sources] as set out below:

(a) analytics providers such as Google based outside the EEA or UK; (b) advertising networks such as Google Adwords, Facebook Lookalike Audiences or similar services based inside or outside the EEA UK; and (c) search information providers [such as Google, Bing or similar based inside or outside the EEA or UK).

5. How we use personal data

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- When we are contacting you in response to an explicit request from you to learn more about Engaging Networks and the software it offers.
- When we need your data in order to perform a contract with you at your request
- When it is necessary for our legitimate interests and these interests do not override your interests and fundamental rights
- When we need to comply with a legal or regulatory obligation.
- When you have given your consent, for example where you give explicit consent to receiving direct marketing from us.

Lawful Bases

Below are the lawful bases we rely on to process personal data: **Legitimate Interest** means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by Contacting us. **Performance of Contract** means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract. **Comply with a legal or regulatory obligation** means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

Purposes for which we use personal data

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Purpose/Activity	**Type of data**	**Lawful basis for processing**
Registering new customers	(a) Identity(b) Contact	Performance of a contract
Processing and delivering orders including:(a) Managing payments, fees and charges(b) Collecting money owed to us	(a) Identity(b) Contact(c) Transaction	Performance of a contract
Advocacy Databases	(a) Identity(b) Contact	Performance of a contract (access to publicly available contact details of political representatives in the UK and Northern Ireland, Canada, Australia, the United States, Germany and the European Parliament)

Relationship management including:(a) Notifying you about changes to our terms or policies(b) Asking for reviews or issuing user surveys	(a) Identity(b) Contact(c) Marketing and Communications	(a) Performance of a contract(b) Necessary to comply with a legal obligation
To enable you to complete a survey or provide feedback about the service or participate in special promotions	(a) Identity(b) Contact(c) Usage(d) Marketing and Communications	(a) Consent(b) Performance of a contract with you
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity(b) Contact(c) Technical	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise).(b) Necessary to comply with a legal obligation
To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(a) Identity(b) Contact(c) Profile(d) Usage(e) Marketing and Communications(f) Technical	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	(a) Technical(b) Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)

To make suggestions and recommendations to you about goods or services that may be of interest to you	(a) Identity(b) Contact(c) Technical(d) Usage	Consent. Our legitimate Interests

Cookies

When you use our website, if you provide consent, we will store cookies on your computer in order to facilitate and customise your use of our site if your settings allow us to. A cookie is a small data text file, which a website stores on your computer's hard drive (if your Web browser permits) that can later be retrieved to identify you to us. Read our Cookie Policy and manage your cookie preferences here (https://companysitedev.wpengine.com/cookie-policy/)

Promotional offers from us

You will receive marketing communications from us if you have requested information from us or subscribed to services from us and, in each case, you have not opted out of receiving that marketing. We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you. We may use email addresses and first name / last name details to create 'custom audiences' and identify 'lookalike' audiences on social media channels to provide information, services, or products that we feel may be of use or interest to those audiences. This involves uploading these supporter details to third-party social media organisations, including Facebook, from which they identify 'lookalike' cohorts. This upload is governed by terms and conditions restricting the processing and use of the data and you can manage your Facebook ad settings on https://www.facebook.com/help/568137493302217 (https://www.facebook.com/help/568137493302217). To stop receiving marketing messages, you can click on the unsubscribe link on any email sent from us to you or by contacting us at any time at info@engagingnetworks.net (mailto:info@engagingnetworks.net). Where you opt out of receiving these marketing messages, this will not apply to personal data provided to us because of a product/service purchase, warranty registration, product/service experience or other transactions.

Change of purpose

We will only use your personal data for the purposes for which we collected it. If we need to use your data for any other purpose, we will contact you directly.

6. Disclosures/sharing of personal data

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions. We share personal data within the Engaging Networks Group. This will involve transferring your data outside the EEA and UK. Whenever we transfer personal data out of the United Kingdom or the EEA, we ensure a similar degree of protection is afforded to the data by using service providers and signing specific contracts that satisfy European Commission or Information Commissioner's Office (ICO) standards, giving personal data the same protection that it has in Europe or the United Kingdom.

7. Retention Policy

The following table identifies the terms referred to in this policy:

Client	Organisation that has contracted Engaging Networks to provide software platform & publicly available advocacy databases for the purposes of fundraising, data management, advocacy, bulk email and event management.
Supporter	Persons actively engaged with the client organisation e.g. sending emails to MPs in support of the client cause
Donor	Persons who donate money towards supporting the work of the client
Contractors	People or entities who work for Engaging Networks on a xed contract
Employees	Full time employees of Engaging Networks
Partners	Organisations who work in partnership with Engaging Networks to provide a service to clients

We use the following technologies and processes:

1. Salesforce

- **Personal Data:** Client / prospect name, organisation name and address, job title and contact email address.
- **Purpose of Processing:** Managing our client and prospects database.
- **Where the data is processed**: USA, using Standard Contractual Clauses approved by the European Commission and the United Kingdom Government which offer sufficient safeguards on data protection for the data to be transferred internationally.
- **Legal Basis of Processing:** To perform a contract with a client, legitimate interests.
- **Duration of processing:** All disqualified leads deleted on the final working day of the month, two years after the record was initially created, with all organisation leavers deleted on the final working day of the month, five years after the record was last modified in Salesforce.

2. Google Workspace

- **Personal Data:** Client name, prospective client name, contractor name, partner name, email, and other contact information including office address, phone number.
- **Purpose of Processing:** Gmail, Google Docs, Sheets, Google Calendar, & Google Hangouts (etc), is used across the business to support day to day work.
- **Where the data is processed**: The European Economic Area (EEA).
- **Legal Basis of Processing:** Our legitimate interests, performance of a contract or to take steps prior to entering into a contract.

3. Egnyte

- **Personal Data:** Client name, supporter name and details, telephone number, email address, etc.
- **Purpose of Processing:** Clients can have temporary access, if required, to securely transfer supporter data or other files via their own dedicated Egnyte folder for their business purposes, once they agree to user agreement (by Egnyte).
- **Where the data is processed:** USA, using Standard Contractual Clauses approved by the European Commission and the United Kingdom Government nwhich offer sufficient safeguards on data protection for the data to be transferred internationally.
- **Legal Basis of Processing:** Our legitimate interests, performance of a contract or to take steps prior to entering into a contract.
- **Duration of Processing:** Client contract files can be held for duration of contract but client can delete these files at any time + three years in UK, employee files held for duration of employment plus six years.

4. Zoom

- **Personal Data:** Client name, prospective client name, contractor name, partner name, organisation name and email addresses for all the above.
- **Purpose of Processing:** Zoom is used for video conferencing and webinar use. Prospective client name and email is captured in Salesforce (1).
- **Where the data is processed**: USA, using Standard Contractual Clauses approved by the European Commission and the United Kingdom Government which offer sufficient safeguards on data protection for the data to be transferred internationally.
- **Legal Basis of Processing:** Our legitimate interests, performance of a contract or to take steps prior to entering into a contract

5. Software hosting

- **Personal Data:** Client name, client email, clients' supporter name, supporter email and other contact information determined by client
- **Purpose of Processing:** Hosting company (sub-contractor) for Engaging Networks proprietary software
- **Where the data is processed:** Data for all Engaging Networks client organizations that are subject to GDPR is stored in Canada
- **Legal Basis of Processing:** Performance of a contract
- **Duration of Processing:** For the duration of contract**.** If a client stops subscribing to the Engaging Networks' service, all their supporter data is cleared down by contract expiry and data is securely transferred back to client (data controller)

6. Engaging Networks Platform

- **Personal Data:** Client name, client email, clients' supporter name, supporter email and other contact information determined by client
- **Purpose of Processing:** Clients' use of Engaging Networks proprietary platform to create pages, execute campaigns, send bulk email to supporters and engage in ecommerce
- **Where the data is processed**: Canada (point 5, above)
- **Legal Basis of Processing:** Performance of a contract
- **Duration of Processing:** For the duration of contract**.** If a client stops subscribing to the Engaging Networks' service, all their supporter data is cleared down by contract expiry and data is securely transferred back to client (data controller)

7. Conference Networking

- **Personal Data:** Attendees' names, business addresses, telephone numbers and email addresses
- **Purpose of Processing:** Lead generation, client retention

- **Where is personal data processed:** At conference location, in Engaging Networks platform and Salesforce™
- **Legal Basis of Processing:** Necessary for the purposes of the legitimate interests pursued by Engaging Networks

8. Thinkific

- **Personal Data:** Client name, organisation name, job title and email address.
- **Purpose of Processing:** Thinkific is a SAAS online learning management system. We use the service to deliver online training delivered through our Academy.
- **Where is personal data processed:** USA.
- **Legal Basis of Processing:** Necessary for the purposes of the legitimate interests pursued by Engaging Networks. For more information see the 'Academy' user policy at the bottom of this page.
- **Duration of processing:** See the data retention section of the 'Academy' user policy that can be found at the bottom of this page.

9. ZoomInfo

- **Personal Data:** Business contact name, email and other solely business-related information related to organisations who may be interested in the Engaging Networks software, or are clients already.
- **Purpose of processing:** Engaging Networks makes use of ZoomInfo's database of business contacts to help identify organisations we can reach out to about the software. We are also able to clean the business-related data we do hold on clients or prospects (in Salesforce, see 1 above) after cross checking it with ZoomInfo's database.
- **Where is personal data processed:** We are not processing personal data, we just subscribe to ZoomInfo's database. For more information on ZoomInfo, visit their Privacy Centre (https://www.zoominfo.com/about-zoominfo/privacy-center).
- **Legal Basis of Processing:** Not applicable.

10. Mixmax

- **Personal Data:** Business contact name, email and other solely business-related information related to organisations who may be interested in the Engaging Networks software, or are clients already.
- **Purpose of processing:** Mixmax is an email tracking and marketing automation tool. With Mixmax we are able to schedule email campaigns and monitor tracked emails to gauge prospect and client engagement. Activity from Mixmax is logged in our Salesforce account (see 1 above).

- **Where is personal data processed:** USA, using Standard Contractual Clauses approved by the European Commission and the United Kingdom Government which offer sufficient safeguards on data protection for the data to be transferred internationally.
- **Legal Basis of Processing:** Our legitimate interests, performance of a contract or to take steps prior to entering into a contract.

11. Trustpilot

- **Personal Data**: Business contact name, email address and reference number. Trustpilot may also process any other personal data included in the order confirmation messages that businesses send to their consumers
- **Purpose of processing**: We may contact you via email to invite you to review Engaging Networks in order to collect your feedback and improve our services (the "Purpose"). We use Trustpilot A/S ("Trustpilot"), to collect your feedback which means that we may share your contact name and business email address with them for the Purpose. If you want to read more about how Trustpilot processes your data, you can find their Privacy Policy here (https://uk.legal.trustpilot.com/for-reviewers/end-user-privacy-terms). We may also use such reviews in other promotional material and media for our advertising and promotional purposes. Trustpilot acts as a data processor on our behalf when sending review invitations. They have a clear infographic on how this works here (https://support.trustpilot.com/hc/en-us/articles/360001141547--Is-Trustpilot-a-data-processor-or-data-controller-).
- **Where is personal data processed**: Data is stored in the EU by AWS/Google Cloud Services, but for the purpose of sending out review invitation emails it is being transferred to Twilio SendGrid – Trustpilot's sub-processor in the USA.
- **Legal Basis of Processing**: Our legitimate interests, performance of a contract or to take steps prior to entering into a contract. Data Processing Agreement, including Standard Contractual Clauses (SCCs) and sub-processors list are in place and available on request.
- **Duration of processing:** Read more about Trustpilot's data retention policy and how to delete review invitations here (https://support.trustpilot.com/hc/en-us/articles/360001157168-Delete-your-review-invitations-data). We are not able to delete submitted reviews however we can report them to Trustpilot's 'Content Integrity' department if we believe they violate their guidelines.

12. WordPress Engine

- **Personal Data:** Any form field added to, for example, a 'contact us' or 'demo request' form on this website will go into the WordPress (WP) Engine database after a user has

submitted a the form. The data submitted will generally be: business contact name, email, organisation name and job title though the form fields can vary.

- **Purpose of processing:** We are using embedded forms on our website to improve user experience for form submission. The data submitted in these forms is stored in the WP Engine database. Once a user submits a form, the relevant staff at Engaging Networks will follow up to answer the query (demo request, support request etc).
- **Where is personal data processed:** In the European Union, in Germany.
- **Legal Basis of Processing:** Our legitimate interests, performance of a contract or to take steps prior to entering into a contract. WP Engine's DPA can be found here. (https://wpengine.co.uk/legal/dpa/)
- **Duration of processing:** We have a standard setting to delete all data from submitted forms after seven days.

13. ChurnZero

- **Personal Data:** Contact name and email address of Engaging Networks' clients or account holders only
- **Purpose of processing:** ChurnZero is integrated into the backend of Engaging Networks for the purpose of segmenting, communicating with and determining how active – or not – our clients are inside of their account(s), therefore improving their usage of the software
- **Where is personal data processed:** European Union
- **Legal Basis of Processing:** Legitimate Interests
- **Duration of processing:** For as long as the users are Engaging Networks clients or decide to opt out of the ChurnZero service.

14. Sage Business Cloud (Sage)

- **Personal Data:** Contact name, (organisation) address and billing contact email related to clients of Engaging Networks
- **Purpose of processing:** Engaging Networks makes use of Sage to send all business invoices to clients or any other companies we may send invoices to (no payment details, such as bank account numbers, are stored or processed through Sage)
- **Where is personal data processed**: United Kingdom
- **Legal Basis of Processing:** Performance of a contract
- **Duration of processing:** For current financial year plus six years

15. Dropbox

- **Personal Data:** Business contact name, email and other solely business-related information related to clients of Engaging Networks

- **Purpose of processing:** Engaging Networks uses Dropbox to send subscription contracts for e-signing, either to organisations who are signing up to become clients, or are renewing their subscription contract
- **Where is personal data processed:** USA
- **Legal Basis of Processing:** Performance of a contract
- **Duration of processing:** For two years after the end of the current contract term

16. Hubspot

- **Personal Data**: Minimum data requirements are an email address and first name, however we will also try and collect: Surname, Job Title, Business Phone Number, LinkedIn Profile (where publicly available), Location (country)
- **Purpose of processing**: To integrate Hubspot into our sales and marketing processes for efficient and effective prospecting and client acquisition. This is related to Business-to-Business (B2B) data only, not personal data subjects.
- **Where is personal data processed**: European Union
- **Legal Basis of Processing**: Consent
- **Duration of processing**: Inline with Salesforce retention policy (1)

8. Data protection principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully and transparently
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (“purpose limitation”)
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”)
- Accurate and up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (“storage limitation”)
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“integrity and confidentiality”)

Engaging Networks is responsible for our clients’, their supporters’ and our employee’s personal data and must be able to demonstrate compliance with all of the above principles through our policies, actions and documentation.

Fair, Transparent and lawful processing

GDPR is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case Engaging Networks), the purpose for which the data is to be processed by Engaging Networks, and the identities of anyone to whom the data may be disclosed or transferred. For personal data to be processed lawfully by Engaging Networks, at least one of the following conditions must be met:

1. That the data subject has explicitly consented to the processing
2. that the processing forms part of a contract or steps taken at the request of the data subject to enter a contract
3. that the processing is necessary for the legitimate interests of the data controller or by a third party
4. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
5. processing is necessary for compliance with a legal obligation to which the controller is subject
6. processing is necessary in order to protect the vital interests of the data subject or of another natural person

When sensitive personal data is being processed, additional conditions must be met to ensure highly levels of protection and security. In most cases the data subject's explicit consent to the processing of such data will be required.

Purpose limitation

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by GDPR. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed and explicit consent given before any processing occurs.

Data minimisation

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject or as instructed by our clients. Any data which is not necessary for that purpose should not be collected in the first place.

Accurate data

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

Storage limitation

Personal data should not be kept longer than is necessary for the purpose. This means that data is destroyed or erased from Engaging Networks systems when it is no longer required.

9. Data Subjects' Rights

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- **Request access** to any data held about them by a data controller. Commonly known as a "data subject access request", this enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- **Have any inaccurate personal data corrected or updated (rectified).** This enables you to have any incomplete or inaccurate data we hold about you corrected or appended. We may need to verify the accuracy of the new data you provide to us.
- **Object to the processing** of your data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes.
- **Request erasure of your data**. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- **Restrict the processing of personal data.** This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

- **Transfer personal data** to a third party on request, where the data was obtained by consent or contract. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- **Withdraw consent at any time** where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

10. Data security

Engaging Networks must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss. GDPR requires Engaging Networks to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if we have full agreement from the controller and the third-party agrees to comply with those procedures and policies and or if they put in place adequate measures themselves. Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- **Con dentiality** means that only people who are authorised to use the data can access it
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the Engaging Networks' central computer system (data centre)

In the event of an incident affecting the security of personal data as Processor, it is Engaging Networks' responsibility to notify our clients (Controllers) as soon as the issue is detected.

Other Policies

Event Refund Policy

Engaging Networks hosts company information events, either in person or online. Individuals registering and paying to attend these events are entitled to a 50% refund of the event ticket price if they cancel at least 10 working days prior to the date of the event. No other refunds are offered.

Academy User Policy

Engaging Networks provides training to clients and agencies through our online training platform (The Academy). Our academy user policy is detailed here (http://client.engagingnetworks.academy/pages/terms).