Engaging Networks Privacy Notice

This version was last updated on 14 January 2025. This policy can also be downloaded in PDF format here.

Introduction

As individuals, we want to know that our personal information is handled properly, and what our rights are in this regard. During its activities Engaging Networks (EN) will collect, store and process personal data, and recognises that the correct and lawful treatment of this data will maintain confidence in the organisation and will protect your data rights. This privacy notice aims to give you information on how EN collects and processes your personal data through your use of this website or other interaction with the company. The data collected will include any data you may provide through this website when you sign up to receive information from EN, if you 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 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). Please also use the Glossary to understand the meaning of some of the terms used in this privacy notice.

Who we are

We are Engaging Networks, (EN), a registered company in England and Wales; we have a subsidiary company registered and based in the US. We provide a Software as a Service platform for not-for-profits. While we do not collect and process certain data (e.g. Special Category data), our clients might. 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: LABS House 15-19 Bloomsbury Way, London WC1A 2TH United Kingdom Phone: +44 (0)20 7253 0753 Email: info@engagingnetworks.net
US: One Thomas Circle, Suite 700 Washington DC 20005 United States Phone: (+1) 202 525-4910 Email: info@engagingnetworks.net

For queries regarding personal data, our Data Protection Officer can be contacted at DPO@engagingnetworks.net.

All users of EN's 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) and to seek remedy through the Courts of England and Wales. You may contact our European Representative as Required under Article 27 GDPR as follows:

Email: engagingnetworks@gdprnomrep.eu Postal Address: Engaging Networks Nominated Representative, c/o Castlebridge Nominated Representative Services, Suite 6, New Work Junction, Clonard Village Centre, Clonard, Wexford, Y35 WR02, Ireland

Glossary of data protection terms

Data is recorded information whether stored electronically, on a computer, or in paper-based filing systems.

Data subjects are identified or identifiable natural persons about whom, in this case, EN collects and 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 N). 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 be a simple e-mail address. Personal details such as someone's contact details or salary fall within the scope of The General Data Protection Regulation. It does not include data where the identity has been removed (anonymous data).

Sensitive personal data includes information about a person's political opinions, their 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 those people or organisations who determine the purposes for which, and the manner in which, data is processed. They have a responsibility to establish practices and policies in line with GDPR. EN is the data controller of all personal data belonging to those individuals whose data we collect when they visit our website, use one of our services, enquire about our services or who enter into a dialogue with us as representatives of a company we have a contract with. Our clients are the data controllers for all personal data of the members/supporters that they collect and manage using our software. Only they determine the purposes and means of the processing of personal data that we carry out on their behalf.

Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following EN's data protection and security policies at all times.

Data processors include any person or organisation that processes personal data on behalf of a data controller. EN is the 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 that process the personal data on behalf of EN. They may be located in the UK or in other, third countries. EN utilise the following types of third-party processors to provide IT and system administration services and customer and sales support.

- Service providers based in Canada who provide IT hosting 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.
- Companies in the EN Group [acting as joint controllers or processors] and who are based

outside of the United Kingdom (UK) or European Economic Area (EEA).

Applicable Data Protection Law:

Refers to all or any data protection legislation applicable to Engaging Networks acting as the Data Controller of the data it collects or as the processor in the course of providing services for clients.

- Where the Controller and Processor are based in the United Kingdom the relevant data protection law is the United Kingdom General Data Protection Regulation, 'UK GDPR,' the (UK) Data Protection Act 2018 and any applicable national implementing laws, regulations and secondary legislation in the four nations of the UK 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 EU 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 in these Frameworks with the US Department of Commerce.
- Engaging Networks complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Engaging Networks has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. Engaging Networks has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/
- By certifying to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF. and the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland Engaging Networks and its compliance with the Frameworks is liable to the investigation and enforcement powers of the Federal Trade Commission for its compliance.

Data protection principles

When processing personal data EN 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”)

EN is responsible for the personal data we collect from our clients and potential clients, and must be able to demonstrate compliance with all of the above principles through our policies, actions and documentation.

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.
- **Remedy/Arbitration.** Where an individual has sought to resolve and issue with an organisation relating to the treatment of their data rights in relation to the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) has the right to seek a binding arbitration with no fee if:
    - They have raised the claimed violation with the organisation and given the organisation enough time to resolve the issue
    - Made use of the independent recourse mechanism under the Principles of the DPF or
    - Raised the issue through the individual's DPA to the Department and given enough time for the Department to resolve the matter

  An individual may not take the matter to binding arbitration if:
    - The claim has previously been to binding arbitration
    - The matter was subject to a final judgement in a court action, or
    - The matter had previously been settled

The data we collect about you and how it is collected

EN is the Data Controller for all personal data provided by those individuals who visit our website as potential customers or as users of services we offer, or who contact us to manage the relationship we have with their organisation. The personal data, which may be held on paper or on a computer or other media, is subject to legal safeguards specified in The General Data Protection Regulation (GDPR), the UK Data Protection Act 2018, and other regulations. 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, EN 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.

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 on 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

Visitors to our website are not required to submit personal data, but where we need to collect personal data to contact you in relation to queries about our services if you do not submit your contact data we will not be able to contact you. Similarly, to set up and administer a contract we have with our clients you will be required to enter contact data to enable us to contact you, in performance of the contract or to deliver the requested training. In this case, we may have to cancel a product or service you have with us.

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, by corresponding with us or giving it in person. 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)
    - access the Engaging Networks Academy
    - visit our stand at a symposium/convention/trade event
- **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:
    - advertising networks such as Google Adwords, Facebook Lookalike Audiences or similar services based inside or outside the EEA UK; and
    - search information providers (such as Google, Bing or similar based inside or outside the EEA or UK).

How we use personal data

We will only use your personal data when the law allows us to. We will not use your personal data

for any purposes other than those declared at the point of collection without you express approval and we require all sub-processors to treat your data in the same way. 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 EN 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.
- When accessing training through the Engaging Networks Academy

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, and the European Union
Relationship management including:(a) Notifying you about changes to our terms or policies(b) Asking for reviews or issuing user	(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	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).

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 (Marketing)	(a) Identity (b) Contact (c) Technical (d) Usage	Our legitimate Interests Consent

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.

Choice

Change of purpose. Engaging Networks and its sub-processors 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 to explain our proposal and, where required, offer you the option to opt out of the processing.

Disclosure to Third Party. Where Engaging Networks seeks to disclose your personal data to a third part not previously disclosed to and agreed by you, we will contact you directly to explain why we wish to disclose your data to the new third party and to offer to you the ability to opt out of the disclosure.

Disclosures/sharing of personal data

EN 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 of business contacts within the EN Group. This will involve transferring your data outside the EEA and UK to the US. Whenever we transfer personal data out of the UK 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 the EEA or the UK.

Disclosure to Public Authorities

Engaging Networks is under GDPR required to disclose personal information in response to lawful requests by Public Authorities. Under the terms of the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) Engaging Networks is required to disclose personal information to US Public Authorities in response to lawful requests under US law.

Data Transfers

Data collected by EN for the purposes of running the company, including HR data, supporting sales or contracts is for the most part collected and stored on third party applications that store the data in the UK, EEA or a country that has data adequacy under the GDPR, This data may be transferred between UK, EU and US employees as a part of the running of the business and remains subject to GDPR through the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).

Data stored by EN on our own systems either as the data controller or as the processor of our client's data is stored in Canada but may be transferred for short periods of time to the United States of America to be worked on by our engineering team. Once the engineering work is complete the data is returned to Canada and the copy of the data is deleted from the US based servers. These transfers take place under the auspices of the EU/UK/CH – US Data Privacy Framework that EN US is a registered member of.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Engaging Networks commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF.

Liability. Where we transfer personal data to third parties for processing Engaging Networks, as the Data Controller, remain liable for the actions of the third party if they process that information in a manner that is inconsistent with DPF Principles. Our liability remains unless we can clearly demonstrate that Engaging Networks is not responsible for the event or behaviour that caused or allowed and event to occur.

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 where 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. 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. 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.

Engaging Networks Sub-Processors

Engaging Networks remain responsible for the sub-processors treatment of the data and uses Data Processing Agreements to set and control how the data may be treated. Please see the list of sub-processors that EN uses to provide processing activities on behalf of our clients.

Data security

EN works to ensure that appropriate security measures are taken against unlawful or unauthorized processing of personal data, and against the accidental loss of, or damage to, personal data it is the controller or processor of. GDPR requires EN 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 data subject or 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:

- **Confidentiality** 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 collected and processed
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.
- **Reporting.** In the event of an incident affecting the security of personal data collected by our clients, as Processor, it is Engaging Networks' responsibility to notify our clients (the Data Controllers) as soon as the issue is detected.

Compliance and Security Commitments

EN designs its systems, processes and procedures to meet its objectives which are based on the service commitments it makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that the company has established for the services. The system services are subject to the Security, Availability, and Privacy commitments established internally for its services. For more information about our compliance and security commitments please visit our Trust Center.

Academy User Policy

EN provides training to clients and agencies through our online training platform, The Academy. Our academy user policy is detailed here.