ENGAGING NETWORKS

EMPLOYEE AND CONTRACTOR DATA PROTECTION POLICY

Last updated: April 2020

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.

The types of personal data that Engaging Networks may be required to handle include information about current, past and prospective employees, suppliers, clients, client supporter records, and others with whom it communicates. 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's Data Protection Act 2018 and other regulations. Data protection law imposes restrictions on how Engaging Networks may process personal data, and a breach of these laws could give rise to criminal sanctions as well as bad publicity.

Engaging Networks is the Data Controller for all personal data provided by employees, customers (clients) and potential customers and is the Data Processor for all personal data that we process on behalf of our clients.

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.

Engaging Networks' Data Protection Officer is responsible for ensuring compliance with GDPR and with this policy. The Data Protection Officer is Elaine Comyn. Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Data Protection Officer (dpo@engagingnetworks.net).

It is a condition of employment that employees and others who obtain, handle, process, transport and store personal data will adhere to the rules of the policy. Any breach of the policy will be taken seriously and may result in disciplinary action.

Anyone who considers that the 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.

DEFINITION 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

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

LAWFUL BASES

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.

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.

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.

THIRD PARTIES

- Other companies in the Engaging Networks Group [acting as joint controllers or processors] and who are based outside of the EEA and provide IT and system administration services, internal communications support and employee services. These include Slack, Zoom, Egnyte and Salesforce

- Service providers acting as sub-processors based in Canada who provide IT and system administration services (Pivotree)

- Third party payment processors who may be located outside of the EEA.

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 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.

Processing of employee data forms part of a contract or steps taken at the request of the data subject to enter a contract. When sensitive personal data is being processed, additional conditions must be met to ensure highly levels of protection and security. In most cases the employee's explicit consent to the processing of such data will be required.

TRANSPARENCY

We are Engaging Networks, a registered company in England and Wales. Our addresses/contact details are:

US:

1146 19th Street NW, Suite 800
Washington, DC 20036
United States
Phone: (202) 525-4910
Email: info@engagingnetworks.net

UK:

3rd Floor
10-12 Emerald Street, London, WC1N 3QA
United Kingdom Phone: 020 7253 0753
Email: info@engagingnetworks.net

For queries regarding your personal data, please contact your manager or our Data Protection officer in confidence at DPO@engagingnetworks.net .

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 we cannot collect your personal data for one purpose and then use it for another. If it becomes necessary to change the purpose for which your data is processed, we will gain your explicit consent 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 you. Data which is not necessary for that purpose will 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 will be destroyed. You have a responsibility to help us ensure that your personal information is correct and up to date.

STORAGE LIMITATION

Personal data should not be kept longer than is necessary for the purpose. This means that data will be destroyed or erased from Engaging Networks systems when it is no longer required. Our retention periods for data are as follows:

1. **Employee name**

   Purpose of Processing: Digital communications between employees
   Where is personal data processed: Slack™
   Legal Basis of Processing: Our legitimate interests
   Duration of Processing: For duration of employment plus six years (Limitation Act 1980, UK & Wales)

2. **Clients, prospective clients, employees, contractors, partners**

   Purpose of Processing: "GSuite" is used by Engaging Networks as out primary means of sharing work and emailing internally and externally
   Where is personal data processed: Gmail, Google Docs, Google Calendar & Google Hangouts are all hosted in the European Union (this migration is taking place in the summer of 2020)
   Legal Basis of Processing: Our legitimate interests, performance of a contract or to take steps prior to entering into a contract
   Duration of Processing: Duration of client contract with Engaging Networks plus six years to allow for Limitation Act 1980, UK & Wales

3. **Employee, client and supporter Name, telephone number, email address,**

   Purpose of Processing: Egnyte is used primarily to temporarily store secure files shared between Engaging Networks and its clients as well as subscription contracts. It is also used to store and maintain employee files and other company documents. Clients can have access to supporter files in their own dedicated folder when required for their business purposes once they agree to user agreement (by Egnyte)
   Where is personal data processed: Asheville, North Carolina (Egnyte has Engaging Networks HQ down as Washington, DC: Egnyte customers access data from datacentres based on the geographic location of their HQ)
   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 folders held for duration of contract + 3 years in UK, employees files held for duration of employment plus 6 years

4. **Potential employee name, address, telephone number, email address, referee names (provided by candidate)**
   Purpose of Processing: Recruitment of employees
   Where is personal data processed: UK
   Legal Basis of Processing: To take steps at the request of the data subject prior to entering into a contract
   Duration of Processing: Until recruitment process is complete plus 6 months (under The Equality Act 2010)

5. **Employee files**
   Purpose of Processing: To comply with employment laws and to ensure that terms and conditions of employment are properly adhered to and managed.
   Where is personal data processed: UK
   Legal Basis of Processing: Performance of a contract,
   Duration of Processing: duration of employment plus 6 years (Limitation Act 1980, UK & Wales, Equality Act 2010, Income Tax law)

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 that we 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 they agree to comply with those procedures and policies.

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 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 or individual PCs owned by Engaging Networks.

Security procedures include:

- **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

- **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

- **Methods of disposal.** Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.

- **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

DEALING WITH SUBJECT ACCESS REQUESTS

Employees who receive a written request should forward it to the Data Protection Officer immediately at DPO@engagingnetworks.net

When receiving telephone enquiries, employees should be careful about disclosing any personal information held on Engaging Networks' systems. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.

- Suggest that the caller put their request in writing where the employee is not sure about the caller's identity and where their identity cannot be checked.

- Refer to the Data Protection Officer for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

YOUR LEGAL RIGHTS

You have the right to:

- **Request access** to your personal data (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.

- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

- **Request erasure** of your personal 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.

- **Object to processing** of your personal 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. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

- **Request restriction of processing** of your 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

- **Request the transfer** of your personal data to you or to a third party. 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.

Remember, if you have queries, please don't hesitate to talk to your manager or email DPO@engagingnetworks.net