ENGAGING NETWORKS

DATA SUBJECTS RIGHTS PROCEDURE

Last updated: April 2020

These procedures set out how to respond to requests from people ("Data Subjects") in accordance with their rights as data subjects under the UK Data Protection Act 2018 (as amended). The EU (Withdrawal) Act 2018 (EUWA) retains the GDPR (General Data Protection Regulation) in UK law.

The scope of these procedures apply to information that we hold about all current and former clients, sales leads, agency partners, marketing leads, and staff.

These procedures support the Data Protection Policy and also other policies relating to the management of customer and staff records, including the Data Retention Policy.

The GDPR details people's data protection rights. As a Data Controller for staff personal information and Data Processor for our client's databases, Engaging Networks must be able to comply with these Rights.

Data Subject Rights

The GDPR provides the following Rights for individuals:

1. Right to be Informed
2. Right of Access (Also known as a Subject Access Request)
3. Right to Rectification
4. Right to Erasure / Right to be Forgotten
5. Right to Restrict Processing
6. Right to Data Portability
7. Right to Object
8. Rights in Relation to Automatic Decision Making and Profiling

Exemptions to these rights – Schedule 2 of Data Protection Act

1. To safeguard cabinet confidentiality, judicial independence and court proceedings, parliamentary privilege, national security, defence and the international relations of the State.
2. For the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties.
3. For the administration of any tax, duty or other money due or owing to the HM Government, a local authority or other public authority or body.
4. **Legal Privilege**: in contemplation of or for the establishment, exercise or defence of, a legal claim, prospective legal claim, legal proceedings or prospective legal proceedings whether before a court, statutory tribunal, statutory body or an administrative function (including Parliament) or out of court procedure.

5. For the enforcement of civil law claims, including matters relating to any liability of a controller or processor in respect of damages, compensation or other liabilities or debts related to the claim.
6. For the purposes of estimating the amount of liability of a controller on foot of a claim for the payment of a sum of money, whether in respect of damages or compensation, in any case in which the application of those rights or obligation would be likely to prejudice the interests of the controller in relation to the claim.
7. **Expression of opinion**: the personal data relating to the data subject consisting of an expression of opinion about the data subject by another given in confidence or on the understanding that it would be treated as confidential to a person who has a legitimate interest in receiving it.
8. **Archiving purposes in public interest or processing of data is for scientific or historical research purposes**: A request can be refused if the exercise of those rights would be likely to render impossible or seriously impair the achievement of archiving purposes or such restriction is necessary for the fulfilment of those purposes.

1. Subject Access Requests

Data subjects have a right to find out, free of charge, if a person (an individual or an organisation) holds information about them. They also have the right to be given a description of the information and to be told the purpose(s) for holding their information.

A request for information must be made in writing. The data controller must send the data subject the information within 1 calendar month.

Data subjects have a right to obtain a copy, clearly explained, of any information relating to them kept on computer or in a structured manual filing system or intended for such a system, by any entity or organisation.

If Engaging Networks refuses or fails to respond to a Data Subject Request as Data Controller
Note: a Controller determines the purposes and means of the processing of personal data

If we do not comply with a valid data subject request ***within one month***, it is open to the data subject to make a complaint to the UK Data Commissioner, the ICO (Information Commissioner's Office). The ICO contact us and we could then go through a formal process to bring a resolution to the complaint. The ICO will investigate the matter for the data subject and ensure that their rights are fully upheld. The ICO has wide powers to investigate complaints made and will take appropriate action against any organisations that are not in compliance with the provisions of Data Protection Law.

If Engaging Networks refuses or fails to respond to a client as Data Processor
Note: a Processor processes personal data on behalf of the controller

As controllers, our clients are responsible for the security and protection of the personal information on their databases. However, we must also be able to demonstrate compliance with the obligations of the controller and this forms part of our contract with them. That said, we have a contractual obligation to provide not only information on we are processing on the data subject, but also exactly what the data is being processed for. If a client requests any such material from us, we must ensure they (the client) receive it within 48 hours.

You must not respond to the data subject directly – all information to go to client

Engaging Networks Process for responding to the Data Access Requests directly (as Controller)

All requests must be in writing: If the request is made by phone, ask the requestor to put it in writing. An email or letter is sufficient for a request. Never give out personal information over the phone. The requestor's identity should be verified. If at all possible, verify the requestor without asking for further personal data, for example, the last transaction/communication made to Engaging Networks or our client that you can verify. If not, a copy of a passport/driving licence or other identification needs to be supplied by the requestor.

A valid request could read as follows:

Dear ...
I wish to make an access request under the Data Protection Acts for a copy of any information you keep about me for the period from [ ], on computer or in manual form in relation to.... (Fill in as much information as possible to assist the organisations to locate the data that you are interested in accessing e.g. customer account number, staff number etc.

I would like the information returned to me in [electronic / hard copy] format.

The data subject should also include any additional details that would help to locate the information - for example, a customer account number or staff number.

A. Acknowledgement: When a valid request is received, an acknowledgement of the request should be sent to the requestor as soon as possible.

B. Where to send the request: If anyone other than the Data Protection Officer (DPO) receives the request, it should be immediately forwarded to the DPO at DPO@engagingnetworks.net as the clock starts on the date of receipt of the request by Engaging Networks.

C. Proof of Identification: Whether the request is submitted directly by the Data Subject or by a third party acting on behalf of the Data Subject, e.g., their solicitor or via a client, a copy of the Data Subject's proof of identity needs to be provided. A suitable means of validation should be used (eg. past employee leaving date) and should ideally ***not*** involve the transfer of further personal data (such as copy of passport).

Response time for request: A request must be responded to without undue delay and the access request must be concluded within one (1) month. Extensions to three (3) months can occur only where the requests are complex or numerous. However, this must be fully explained within the one (1) month deadline.

D. Extremely broad Requests: If a request is extremely broad, clarification should be sought from the requestor as to the exact scope of data required. This should include relevant timeframes and/or specific documents that are desired.

E. Third Party Requests: If someone makes a request on behalf of another person, i.e., a Solicitor on behalf of a Data Subject, the requestor must provide evidence of their authority to make the request on behalf of the Data Subject. For instance, this can be confirmation of power of attorney or the written consent of the Data Subject. If in doubt (i.e., if the signature does not match those on record), it is necessary to contact the Data Subject for confirmation of their consent to disclose their personal data to the third party. If the request is a user of a client's

platform, the client is the Controller and the onus must be on them to validate identity, you may of course help them in doing this.

F. **Where to get information needed for request:** Once the scope of the request is clear, the relevant systems and files should be searched for the relevant personal data. A note of the efforts made to search for data should be kept in the event of a complaint by the requestor to the ICO.

G. **Requests from current or former Employees:**
Where the requestor is an employee of the company, contact the solicitor in the Legal Department dealing with employment matters. This is to ensure a full understanding of the circumstances and background of the request and whether legal privilege can be applied. Contact the HR Manager to ensure a copy of all correspondence is put on the personnel file and that a copy of the personnel file is provided. The data subject's line manager will also need to be contacted for any emails, correspondence, telephone records they may have either directly with the Data Subject or with other persons that discuss the Data Subject. IT will need to be contacted to obtain telephone records and retrieve email correspondence.

H. **Exemptions:** Once the relevant data has been gathered, the next step is to decide if all of the data must be disclosed or whether an exemption might apply. The DPO/Legal will establish this.

I. **Responding to the Request:** A copy of the data must be forwarded to the requestor. This should be sent by encrypted email with a delivery receipt unless the Requestor specifies that it should be provided in a different format, i.e., hard copy. If it is sent by post it should be by registered post.

J. **Cover letter accompanying the Data:** A cover letter/email should be sent with the data which clearly explains a) the data that has been sent, b) if data is being withheld, the reasons for the withholding, and c) if there were redactions, the reasons for the redactions.

K. **Refusing a Request:** If we decide not to comply with the data access request, we must send a letter or email setting out the reasons for non-compliance to the Requestor along with the caveat that they may complain to the ICO.

L. **Audit Trail of Requests:** All subject access requests and requests from third parties must be recorded so that the Company has an audit trail of actions taken in response to a request and can justify each decision in case there is an investigation by the ICO. The record must include details of the request, contact details of the Requestor, evidence sought and obtained to verify their identity, the decision to release or withhold the information requested, the reasons for the decision and a copy of the information disclosed.

2. Right to Rectification

Data Subjects are entitled to have their personal data rectified if it is inaccurate or incomplete. If the information in question has been disclosed to a third party, we must inform the third party of the request for rectification, where possible. The Data Subject is also entitled to be informed of the third parties to whom their data has been disclosed, where appropriate.

3. Right to Erasure

This right is also known as the 'Right to be Forgotten'. It enables Data Subjects to request the deletion or removal of their personal data where there is no compelling reason for its continued processing by the Data Controller.

The Right to Erasure only applies in the following circumstances:

- The personal data is no longer necessary in relation to the purpose for which it was originally collected

- The processing was based on consent, and the Data Subject has now withdrawn their consent
- The Data Subject objects to processing and there is no overriding legitimate interest of the Data Controller
- The data was being unlawfully processed
- The data must be erased to comply with a legal obligation

4. Right to Restrict Processing

When this Right is exercised, the personal data is permitted to be stored but not to any further processing. Limited information about the individual may be retained to ensure that the restriction is respected in the future.

The Right to Restrict Processing applies in the following circumstances:

- When a Data Subject contests the accuracy of their personal data, processing should be restricted to storage only until accuracy is verified.
- When a Data Subject objects to processing which is being carried out for the reason of performing a task in the public interest or for the legitimate interests of the Data Controller, then the Data Controller must restrict processing to storage only whilst they consider whether their legitimate grounds override the Rights and freedoms of the individual.
- Where processing is unlawful and a Data Subject opposes erasure and requests that data held be restricted just to storage.
- When the Data Controller no longer needs the personal data but the Data Subject requires it for the purpose of a legal claim.

5. Right to Data Portability

This Right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows the individual to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way in a common data format.

The Right to Data Portability applies in the following circumstances:

- When the personal data was originally provided to the controller directly by the Data Subject
- Where the processing is based on consent or performance of a contract
- When processing is carried out by automated means

6. Right to Object

Individuals have the Right to object to:

- Processing based on legitimate interest or performance of a task in the public interest (including profiling)
- Direct marketing (including profiling)
- Processing for the purposes of scientific/historical research and statistics

7. Rights in Relation to Automatic Decision Making and Profiling

This Right provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

The Right not to be subject to a decision applies when:

- It is based on automated processing
- It produces legal/significant effects on the individual

It does not apply if the decision:

- Is necessary for entering into or performance of a contract
- Is authorised by law
- Is based on explicit consent
- Does not have a legal/significant effect on the data subject