



Data Protection Policy Policy date - January 2022 Review date - September 2025 Registration number - 15430520

At Engage Community we take your privacy seriously. This notice describes how we collect and use your personal data in accordance with the General Data Protection Regulation (GDPR) and other applicable laws, as amended or updated from time to time, in the UK. Please read this notice carefully to understand our practices regarding your personal data and how we will treat it.

ABOUT US

Engage Community Ltd is a company offering “Community engagement” and coaching services. We are registered in England and Wales under registration number 15430520. Our registered office is at 28 Spicer Placer, Bilton, Rugby, Warwickshire, England, CV22 7EA. For the purposes of data protection legislation and this notice, we are the “data controller”.

WHAT INFORMATION WE COLLECT

The information we hold about you may include the following:
Your personal details, e.g. your name and/or address
Electronic contact details, e.g. your email address, skype address, telephone number
Details of any products or services you have received from us Communications and correspondence with you
Information about enquiries or complaints you make to us
Information from other publicly available sources, such as Companies House, Linked-In, trade associations etc

HOW WE USE PERSONAL INFORMATION

We may process your personal data for purposes necessary for the normal conducting of our business activities. These may include:
Account set up and administration
Providing goods and services

Delivering marketing communications Personalisation of content
Internal audit requirements

Reporting

LEGAL BASIS FOR PROCESSING YOUR PERSONAL DATA

We may process your personal data for the purposes of our own legitimate interests, including processing for marketing, business development and

E: info@engagecommunity.co.uk **w:** www.engagecommunity.co.uk



administration purposes. This processing is necessary and proportionate for our legitimate commercial interests and will not override any of your own interests, rights and freedoms, which require the protection of personal data.

DATA SHARING

Your personal data will be treated confidentially and will not be shared with third parties, except where such sharing is necessary to fulfil our legitimate interests, to provide the product or service you have requested, or where it is required by law.

WHERE WE STORE AND PROCESS PERSONAL DATA

The data that we hold is stored and processed in the UK, however it may sometimes be necessary for us to share your personal data outside the European Economic Area (EEA), e.g.

- With service providers located outside the EEA
- If you are based outside the EEA
- Such transfer of data would only be what was strictly necessary for the provision of the product or service you have requested from us.

DATA SECURITY

We have put in place reasonable and appropriate security measures to prevent accidental loss, unauthorised access or use of your personal data. Access to your personal data is limited to employees who have a need to know in order to conduct our legitimate business interests. They are subject to a duty of confidentiality. If there is a suspected data security breach, we will notify you and the applicable regulator where we are legally required to do so. Appropriate measures are also in place to enable disaster recovery and business continuity following an unforeseen event.

RETENTION OF PERSONAL DATA

Your personal data will only be retained for as long as it is necessary to fulfil the purpose for which it was collected. The retention period will be determined by:

- The requirements of our legitimate business interests and related products/services provided
- Any statutory or legal obligations
- Whether in future the purpose of the processing could reasonably be fulfilled by other means
- The type of personal data we have collected

E: info@engagecommunity.co.uk **w:** www.engagecommunity.co.uk



YOUR RIGHTS IN RELATION TO PERSONAL DATA

You have the right to:

- Request access to your personal data
- Request correction or deletion of the personal data we hold about you
- Object to the processing of your personal data where we are relying on legitimate interests and something in your personal circumstances gives you a reason to object.
- You also have the right to object where your personal data is being processed for direct marketing purposes.
- Request restriction of processing, e.g. while establishing accuracy of the data or our reason for processing
- Lodge a complaint with the Information Commissioner's Office

The above rights may be limited in certain circumstances, e.g. where you have asked to delete data that we are required to keep by law.

BREACH REPORTING PROCESS

- Data breach events are detected, reported and monitored consistently
- Incidents are assessed and responded to appropriately.
- Action is taken to reduce the impact of a breach
- Relevant breaches are reported to the Data Protection Team within the 72 hour window.
- Improvements are made to prevent recurrence
- Lessons learnt are communicated to the wider organisation.

DATA AUDIT PROCESS

- What data do we hold and why?
- How do we collect the data?
- How and where the data is stored
- What do we do with the data?
- Who owns and controls the personal data?
- Retention and deletion
- Who is responsible for the data and processors associated with data?

DEFINITIONS OF KEY TERMS

Lawfulness, fairness, and transparency: Any processing of personal data should be lawful and fair. It should be transparent to individuals that personal data



concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.

Purpose Limitation: Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. However, further processing for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes (in accordance with Article 89(1) GDPR) is not considered to be incompatible with the initial purposes.

Data Minimisation: Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum (see also the principle of 'Storage Limitation' below).

Accuracy: Controllers must ensure that personal data are accurate and, where necessary, kept up to date; taking every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. In particular, controllers should accurately record information they collect or receive and the source of that information.

Storage Limitation: Personal data should only be kept in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

Integrity and Confidentiality: Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorised or unlawful access to or use of personal data and the equipment used for the processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability: Finally, the controller is responsible for, and must be able to demonstrate, their compliance with all of the above-named Principles of Data Protection. Controllers must take responsibility for their processing of personal data and how they comply with the GDPR.



Business Discovery: Interviewing stakeholders to understand the business questions that your organisation needs to solve and identifying best practices to apply.

Data Discovery: Reviewing disparate sources of data to determine what data you have, where it resides, what format the data is in, and who has access to the data. This includes reviewing multi-country implementations, the frequency of data availability, and any changing data formats.

Technology Discovery: Outlining available technology and future roadmap to store, access, process and disseminate information.

LAWFUL PURPOSES

Contract

Legal Obligation Vital Interests Public Tasks Interests Consent

PERSON RESPONSIBLE FOR DATA PROTECTION

Matt Price - Founder

Simon Price - Managing Director

HOW TO CONTACT US

Should you wish to exercise any of the above rights, or for any query related to this Privacy Notice, please email us at: info@engagecommunity.co.uk. Alternatively, you can write to us at:

Data Protection Engage Community Ltd
28 Spicer Place
Bilton, Rugby
Warwickshire
CV22 7EA

Should you wish to make a complaint to the Information Commissioner's Office (ICO), their contact details are:

Information Commissioner's Office Wycliffe House
Water Lane
Wilmslow

Cheshire
SK9 5AF
Tel: 0303 123 1113 (local rate) or 01625 545 745 Website: <https://ico.org.uk>

E: info@engagecommunity.co.uk **w:** www.engagecommunity.co.uk



We Define 'Your Data' as Information:

Generated by a customer and acquired by us in the course of conducting our business

Generated by ourselves (i.e. about our customers, suppliers, employees and wider community)

Veritas Believes in Best Practice in Terms of 'Information Security Management':

We are registered with the Information Commissioner's Office as a 'Data Controller' under the terms of the Data Protection Act (1998) - Security No. CSN5586441

We are fully committed to maintaining the confidentiality and security of Your Data at all times

We ensure Your Data is securely destroyed when the purpose for which it was originally generated or acquired by us no longer applies

We Believe Absolutely in the Need to Further Improve the Security of Your Data:

We regularly review our business procedures (what we do) and working practices (how we do it), including proactively seeking feedback from stakeholder groups



E: info@engagecommunity.co.uk **w:** www.engagecommunity.co.uk