This document is intended to address the changes in data protection regulations with the introduction of GDPR, enforced from May 25th 2018.

With this in mind, we have prepared this document to ensure that we as an organisation are:

- Protecting our clients, staff and other individuals
- Following “Best Practice” for handling your data
- Complying with legal requirements as stated in GDPR guidelines
- Protecting the organisation

Types of data

Beem (and its derivative software) is a social platform and content aggregator designed to empower employee communication within your business. We need to record data about you and your interests to better serve content and need to record your interactions, such as viewing and liking an article, as this impacts engagement for other users of the platform and helps provide useful insights to your business on how the application is being used.

Some of the data gathered can be considered “Personally Identifiable” or otherwise be used to deduce your identity, but we do not store “Sensitive” data about you.

A list of the information we collect about you and it’s purpose:

Full Name: We use your full name in our application to:

- help identify you amongst other users
- Link you to any content you create
- in certain cases, log you in to the application

Email Address: Your email address is used to:

- In certain cases, log you in to the application
- Identify you within the platform

Device ID: Your Devices ID is used to:

- Link your account to your device.
- Identify you within the platform

Profile Picture: If supplied, your profile picture will be:

- Displayed in your company directory to better help users identify you

Contact Number: If supplied, your contact number will be:

- Displayed in your company directory to better help users identify you

Policy statement

Beem takes your legal rights as an individual very seriously. We also care about protecting you and your colleagues where we can.

We are committed to:

- Complying with both the law and best practices
- Respecting individuals' rights
- Being open and honest with individuals whose data we hold
- Providing training and support for staff who interact with your data
- Following a breach notification policy where we notify you and the ICO if anything untoward occurs with your data.

More information on data breaches from the ICO can be found here:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

More information on an individuals rights under the GDPR can be found here: *https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/*

Key risks

While we take every care to ensure your data is secure and accurate, cyber security is an ever evolving technology and criminal elements are tenacious. There are risks to any online presence.

- To prevent data getting into the "wrong hands" we are:
    - Enforcing internal policy on handling your data within our business, this is to ensure only authorised staff have access to this data.
    - Auditing every request to access personal data, so that we have a record of who accessed what and when
    - Carrying out regular system maintenance, to ensure we stay ahead of any exploits or vulnerabilities in the platform
    - Holding periodic reviews and automating log analysis to ensure nothing takes us by surprise
    - Enforcing Customer Identification Policies to ensure we are not exposing data to the wrong people
- If your data is inaccurate
    - We only record what we have received. If you notice that the data we have about you is inaccurate or false then you can contact us and request it be rectified.

Security

Whilst data security is not wholly a Data Protection issue, it's important for us to establish sensible guidelines to ensure your data is adequately protected.

Setting security levels

All of the data we collect is categorized based on the level of confidentiality. Personally Identifiable information (PII) is marked as "Critical" and falls under the strictest security measures within Beem.

Security measures

For PII, where possible, this information is encrypted using a unique key generated for your business or account. This information is also stored separately in terms of access from other data within the business - for example, your identity as an individual is separated from your account information used to log in, and is only accessed via special request.

Non PII data is stored and mapped to your identity by way of an Identity Number, this keeps things like your post history, likes, and comments separate from who you are in a logical way, some of the data can be used to infer your identity and as such is treated in a similar way to PII.

Any emails containing PII are retained for 30 days, they are flagged for deletion and removed from our systems.
Any content transmitted, such as CSVs or Excel documents containing PII are also flagged for deletion after 30 days, during which time they are stored securely in an encrypted partition.

Based on the confidentiality of the information, access is restricted. Where access is requested it is audited and logged.

Retention periods

As stated above, we employ a 30 day retention period for transmitted data that is not added to the system.

Archiving

Data such as engagement and interaction metrics will be stored in perpetuity - all efforts will be made to ensure the likelihood of inferring your identity from this data is minimal. We will be archiving any data older than 6 months from the system which will only be accessible by Beem employees as per guidance within this policy.

Right of Access

As per GDPR, you have a right to access the information we have about you. All requests must be made in writing and can be submitted through our help desk (beem.zendesk.com) or as an email to your contact at Beem.

We will review and respond to your request within 30 days of receiving it.

More info on your right of access can be found here:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

Provision for verifying identity

Where the person managing the access procedure does not know the individual personally we will enforce Customer Identification Policies. You will be asked a series of questions to ensure you are authorised to access the requested information.

Charging

For most requests, there will be no charge. However, if the requests are frequently made you will be liable to pay a reasonable administration charge. This charge will vary on the complexity of the request.

Procedure for granting access

At this time any requests to access data must be made electronically, via email, or over the phone.

Transparency

Commitment

We are committed to ensuring that you are kept aware of:

- What data is being processed
- For what purpose it is being processed
- What types of disclosure are likely
- how to exercise your rights in relation to the data

Lawful Basis

Lawful Basis of the information we store about is included in the “Types of data” section above. If you have any questions or concerns regarding our basis for retaining this information please feel free to contact one of our DPO’s by emailing: mydata@wearebeem.com

Opting out

If you would no longer like us to process data about you you will be given the option to “opt out” or “Withdraw consent”. Doing so will revoke your ability to use the platform.
There may be occasions where we have no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn. In these cases best efforts will be taken to ensure any PII relating to the withdrawn consent is suitably anonymised.