



best companies™

Data Processing Record

Data Processing Record

Name and contact details

Best Companies Limited
Hamilton House
Rackery Lane
Llay
Wales, UK
LL12 0PB

Data Protection Officer: Eleanor Blore
Email: Privacy@b.co.uk
Tel: 01978 856 222
ICO Registration No: Z8349843

Main Data Controller: The person, firm, company or organisation who is requesting the Service and by accepting the terms of service agreement, is opting to make use of the Best Companies Service being provided ("**Client**" or "**Employer**")

Data Subjects: Employees of Data Controller ("Employee")

Separate Data Controller: Best Companies Limited, Hamilton House, Rackery Lane, Llay, Wrexham, United Kingdom, LL12 0PB ("**Best Companies**")

EU Representative: Best Companies has instructed Rickert Law as our EU Representative in accordance with Article 27 of the GDPR for EU supervisory authorities and EU citizens.

Email: art-27-rep-bestcompanies@rickert.law
Post: Rickert Rechtsanwaltsgesellschaft mbH, Best Companies Limited, Colmantstraße 15, 53115 Bonn, Germany

Notes

This document will be maintained, saved and provided to our Clients, EU Representative and where requested, Supervisory Authority(s). Each party to the services, shall maintain a record of the categories of processing activities carried out.

For the avoidance of doubt, Best Companies will process the data as a Separate Data Controller, this is completed under the lawful basis of legitimate interest.

The Client will not have sole data controller responsibility for the service(s) even though they initiated the work by commissioning the report(s). Responsibility also lies with Best Companies as the professional service provider itself because it independently determines what information to obtain and process to do the work and because it is answerable itself for the content. This is in line with the UK Information Commissioner's Office guidance. To ensure transparency and fairness we contractually oblige all our clients to assist us in the delivery of our privacy notice, for employees (data subjects) to recognise Best Companies as a Data Controller of their data.

Personal Data

The personal data requested and shared between parties, has been considered as the minimum required for the processing by the Client.

In consideration of processing fields may include:

First Name, Surname, Payroll/ Unique Number, Email Address, Delivery Postcode, Eligible for Accreditation, Reporting Office Postcode, Employment Group, Manager Name, Manager Payroll/ Unique Number, Date of Birth, Start Date, Contracted weekly hours, Annual salary, Registered Sex at Birth, % Time Spent Working Remote, Job role, Job Grade/Level, People manager, Reason for survey exclusion.

* Mandatory

** Mandatory for electronic delivery

As per the Best Companies Terms of Service

Personal Data provided by the Main Controller who is requesting the services, are the Data Controller of the Personal Data provided, and Best Companies is the Data Processor.

Personal Data collected directly from the individual survey respondents; Best Companies is sole and considered a separate Data Controller of all survey responses.

Purpose

Best Companies services fulfil two purposes for organisations that work with us:

1. Insightful reporting, to inform the organisation's people strategy
2. Recognition, evaluation for an accolade (Accreditation and national, sectoral and regional lists)

Services: Survey(s) and engagement reporting
 Accolade evaluation

Client(s) consider their lawful basis in understanding the levels of employee engagement within its organisation, unless specifically advised otherwise, the Client has selected Legitimate Interest. Best Companies will administer the data received from the Client to provide a survey to the Clients employees. To provide anonymous reporting to the Client, Best Companies acting as a separate Data Controller will conduct statistical analysis and benchmarking across other clients, nationally, in sector and regionally, to provide the Client with a Best Companies Index (BCI) Score or a Pulse Best Companies Index (PBCI) Score (service dependent). Best Companies will evaluate the client application for an Accolade (Best Companies Accreditation) and for position on a Best Companies lists where an organisation scores a minimum of 600 BCI.

Best Companies has a Legitimate Interest for further research such as historical and statistical purposes, providing benchmarking and data analysis (as Data Controller).

The further processing of data Best Companies conduct can reasonably be determined as compatible with the original purpose. The GDPR specifically states that further processing for the following purposes should be considered, compatible lawful processing operations:

- Scientific research purposes; and
- Statistical purposes

Balance Assessment for Legitimate Interest

Sharing of data is achieved on the legal basis of Legitimate Interest.

The legal basis for data processing is: Legitimate Interest. Best Companies has conducted a Legitimate Interests Assessment (LIA) to ensure the decision is justified. The GDPR acknowledges that organisations may have a legitimate interest in processing data as long as the processing does not have a disproportionate impact on the individual. On balance, the legal basis of legitimate interest against the individual impact: the services are reasonable, the Client organisation interests in the services appear compelling, with there being little impact on the individual. The additional research conducted by Best Companies is considered compatible under Data Protection Law.

It is reasonable to expect that the anonymous reporting data provided to the Client based on the collective individual responses should benefit not only the employer, but every employee across the organisation. This is in consideration of the ability for employers to:

- better support their staff to become happier and more productive
- increase publicity in the organisation by being recognised as a 'Best Company'
- may assist in retaining existing talent and in attracting top talent by generating unique PR and marketing opportunities on a national stage with an accreditation and potential place on Best Companies lists
- measure employee engagement within the organisation to inform the people strategy and to improve engagement

The additional research conducted by Best Companies:

- greatly assists employers with understanding how employee engagement impacts their organisation
- produce(s) best practise content
- provides ability for comparative historical research
- provides learning for the benefit of the wider society in the form of white papers, case studies and articles

Methodology

Behind the processing sits the methodology that all organisations are assessed by, [Best Companies Methodology](#).

The modelling of the methodology looks for statistically improbable survey response patterns. This is to ensure the integrity of:

- fair competition
- meaningful reporting

The process using the Best Companies methodology will exclude surveys, where they are following certain patterns. Insight on the reasons a survey may be excluded can be considered in

the article [How we ensure the integrity of the data we report upon \(b.co.uk\)](#).

To ensure fair competition for all organisations being evaluated, and to protect the integrity of our services, Best Companies would not look to reverse a decision based on the methodology. To ensure no organisation is placed at a competitive advantage, disclosure of when a survey has been excluded or the specific reason of exclusion will not be disclosed. The methodology ensures we fulfil the purpose for organisations requesting Best Companies services.

Data transfer(s) to Best Companies

Client to Best Companies

Personal data is securely uploaded by the Client via the Best Companies dashboard. In the event additional assistance is required, the Client should contact Best Companies, who will provide instructions for supplying the data through Zivver. This ensures a secure method for transferring data to and from Best Companies.

Data Subject to Best Companies

Email: Employees will receive an email invitation containing a unique link and login details to the b-Heard survey. The email will come from survey@b.co.uk. The email will be personalised to the employee.

Description of the Processing

Best Companies will provision and provide the administration of a b-Heard survey to the Client. This is for Best Companies to measure levels of employee engagement within the Client organisation and provide a BCI or PBCI Score.

In advance of the data sharing, the Client is contractually obliged to assist with the delivery of the Best Companies Privacy Notice, www.b.co.uk/privacy-notice. We recommend this is shared within the organisation when announcing that they will be taking part in the b-Heard survey and to make employees aware of Best Companies and how their data is to be processed. This is to ensure transparency and fairness, and that the employee recognises Best Companies as a Separate Data Controller. This also reassures the employee that they can respond honestly, all responses are reported back anonymously.

The Client will provide pre-populated fields for Best Companies to administer the delivery of the survey. They will contain a unique identifier for each Data Subject such as a payroll number to ensure there is accuracy from duplication of records. They will also provide known demographics where it would appear reasonable for the organisation, already having this information to provide to Best Companies in advance, thus saving the employee time in completion and to ensure data accuracy.

Best Companies as Separate Data Controller will conduct statistical analysis and benchmarking across its client database, regionally, nationwide and/ or sector, to provide the Client with a Best Companies Index (BCI) Score. Best Companies will consider the client application for a Best Companies Accreditation and where the organisation scores high enough, they may be considered, for a position on a Best Companies lists.

Data processing is not expected to be a risk to the rights and freedoms of data subjects.

Elevate (where purchased)

Client Lawful Basis: Contractual

Completed on the request of the Client

Elevate is a development platform, to transform the performance of individuals with data driven coaching for leaders and future managers, based on real team and organisation feedback.

The Client organisation will share data required for the processing, including but not limited to, employee name, reporting manager name/payroll number and identifying where an individual manages employees. Personal data will also be collected directly from the employees completing the survey. Survey responses submitted by employees completing the survey will inform the reporting.

The Client organisation project leads will review the reporting structure to ensure employees are aligned correctly to the reporting manager. Managers will also get the opportunity to verify their direct reports.

Elevate involves automated processing including profiling. UK Data Protection Legislation advises that you can carry out this type of decision-making when it is necessary for the lawful basis of performance of a contract. The Client will have a contract of employment with the employee that is being reported on which will include clauses or can reasonably be referred to one or more of:

- a) managing a team
- b) completing the job function to a certain standard
- c) personal development.

On balance, we have reasonably determined that Elevate provides:

- a) An in-depth understanding of individual manager performance, enabling decision-making, impact tracking and continuous improvement,
- b) Development opportunities for high-performing managers and teams through improved organisational clarity, enhanced team cohesion, and successful relationship building,
- c) Empowering managers to take ownership of their development, resulting in stronger leadership skills, improved performance, and increased retention across teams,
- d) Acceleration leadership growth and positively impact employee performance, engagement, and retention, ultimately contributing to the organisation's overall success,
- e) Providing effective leadership support and development through increased transparency and organisational visibility, fostering stronger leadership across all levels.
- f) Insights for those on their journey into management to be future ready leaders

Should a manager disagree with the results, they can request a manual review, provide their perspective, and challenge the outcome to ensure fairness and transparency.

Diversity Monitoring (where requested)

Best Companies can include (on request) a series of diversity statements, these are intended to provide a better understanding, without collecting special category data.

Where the Client has a requirement to report on specific diversity levels within its organisation and selects the diversity survey. Best Companies will collect the consent from each employee at point of surveying to report back the findings anonymously. The Employee is consenting for the data to be collected and reported anonymously to their employer. The employee responses do not become part of the Client data set.

To comply with the general equality duty, some organisations need to have an adequate evidence base for their decision-making. By collecting and using the equality information, we may work with organisations to create bespoke reporting (on request) to better understand the needs of staff from different protected groups and thereby improve the efficiency of the organisation. The employee has a clear and free choice in their response to the survey in its entirety including the option to abstain at a question level.

Whilst the GDPR considers the processing of special categories of data to be a higher risk, the data processing activity is not expected, to be a risk to the rights and freedoms of data subjects. The processing of this data for the Client can be considered occasional to assist your organisation with ensuring equality of opportunity or treatment within the organisation.

Research Extending to Further processing by Best Companies

Best Companies will conduct its own processing of the data collected for benchmarking purposes. Best Companies may conduct historical, scientific and statistical research, to further understand the issues surrounding employee engagement. The data analysis we conduct involves a process of inspecting, cleansing, transforming and modelling the data we have with the goal of discovering new information, suggesting conclusions and supporting decision-making. We conduct data analysis on behalf of 3rd parties, such as organisations who want further insights and correlations in how the data we have collected compares with other organisations in their sector or nationally. We also conduct our own independent research, which we may make publicly available. All reporting to other parties or when reporting data is made publicly available is anonymous. No personal data is shared with third parties. Data rendered anonymous is not considered personal data under Data Protection Legislation.

Best Companies is relying on legitimate interest for the further processing of the data it holds, and further processing shall only be completed where it can reasonably be considered as compatible.

Majority of international data protection legislation, including the GDPR allows for further processing for research purposes and should be considered a compatible lawful processing operation.

To protect the rights and freedoms of data subjects, the responses provided to Best Companies as a separate data controller do not become part of a Client dataset. The Employee has been provided Best Companies Privacy Notice (delivered multiple times through Client announcements and at point of surveying,) to ensure fair and transparent surveying. Data processing by Best Companies is not expected to be a risk to the rights and freedoms of data subjects.

Data Retention

Best Companies will retain personal data for up to three years following the lapse of the subscription term. During this period Best Companies will continue processing this data after the provision of the initial service to the organisation as a Controller. In addition to providing benchmarking, we process the data to conduct new and further research on employee engagement, for historical, scientific and statistical purposes. This term is documented within Best Companies privacy notice.

Best Companies recognises that a Client has an invested interest for Best Companies to retain personal data for up to three years following the lapse of the subscription term. Organisations go through restructure and change every few years. On request, Best Companies can reconfigure the personal data held from previous year(s) participation, to correlate the reports from the latest b-heard survey. Following an organisation restructure, employers have a real need to understand the impact it has made on their employees. The ability to be able to alter the reporting to reflect the new organisation structure provides organisations with valuable data that reflects the true position of the organisation against those previous years surveyed. Should a Client decide they do not require Best Companies to retain the personal identifiers for this length of time, a written request can be made that the personal data is anonymised. This is completed within one month of receiving a request. To ensure fairness and transparency to the Employee, Best Companies would not accept a request to extend the retention period.

Best Companies will retain demographics and employee responses for their own research purposes. The UK Data Protection Act 2018 and General Data Protection Regulation (GDPR) does not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

Vulnerable Employees

Best Companies expects a Client to identify a vulnerable employee. In this situation, the Client will consider the capacity of the individual to complete the b-Heard survey in the purchased format and the Employee ability to understand Best Companies privacy notice.

When delivery of the privacy notice to an employee in its standard method may not be, appropriate, for example, if they are partially sighted. All employees should be supported so they could understand how their data is to be used. If you require assistance in delivering a simpler form of our Privacy Notice, Client will contact Best Companies for an alternative version.

Best Companies has set the minimum age for its service(s) at 16 years of age. This has been considered and applied to protect the rights and freedoms of a child. Individuals of 15 years and under may not have the capacity to understand how their data may be used and could be unduly influenced, without Client intention.

General Overview of Security measures

Best Companies processes personal data securely by means of appropriate technical and organisational measures having taken into consideration, the state of the art and costs of implementation. Best Companies has an information security policy and has taken steps to make sure the policy is implemented. To ensure availability and continued operations, Best Companies also has a business continuity plan.

Encryption: All data is encrypted in transit, 256-bit encryption algorithms and all our websites

use a 4,096-bit public key. All our websites are https. All backups with Barracuda and Microsoft Azure are encrypted at rest. All Laptop (PCs) with Windows OS is Microsoft BitLocker encrypted with TPM, whilst those with a macOS are encrypted with FileVault. On the rare occasion a USB pen is required in the business, these are also encrypted and logged in and out.

Multifactor Authentication (MFA): Authorised users that need to access our network externally, do so through our VPN and are required to login with their password and a onetime use generated password. MFA is also available at a company level to Clients accessing the Best Companies applications.

Office Security: To break into our offices someone would have to go through multiple locked doors and override a modern alarm system. There is internal and external CCTV recording 24/7 with partial motion detection. Recordings are kept for 30 days. There is an electrified fencing at the rear of our offices.

Backups: Backups are taken at the end of every working day. We have backups kept securely with Barracuda Networks. These are kept for three months and encrypted at rest in a UK Datacentre. We also have backups of the Azure setup in Azure, where we keep six-monthly backups at a time and 30 days of daily backups. All backup data is encrypted in transit.

Development: All development code is peer reviewed before being pushed to a staging environment. At this point it is checked by front-end users. This way we aim to catch development issues before they hit the live server. Code is checked for security, performance, and functionality. We perform dynamic vulnerability and static source code security scanning and review through our www.mend.io

High Availability: Best Companies websites run on infrastructure in an N+1 configuration, meaning systems will continue to run if a component fails.

Vulnerability Assessment and Penetration Tests: We instruct an External Company to perform an annual vulnerability assessment and penetration test and, should they find any issues we will always ensure these are rectified without undue delay. We conduct quarterly network perimeter scans and frequently review our security posture through Security Scorecard (<https://securityscorecard.com/>) which is reported to the board as an agenda item.

Access: All data is only accessible by Best Companies authorised personnel. Restrictions apply to users designated on our customer accounts and third parties who can access the information only in specific and limited circumstances, and are bound by confidentiality agreements.

Services of Sub-Processors

Like most organisations, Best Companies works with other organisations to enable us to provide you with the best possible service. These third-party suppliers perform the functions to be considered sub-processors under applicable data protection laws.

All sub-processors have undergone due diligence and have written contracts in place relevant to the data processing.

For information on the sub-processors, please review the below article.

Data Transfers

Best Companies is in the United Kingdom, our Data Processors that are assisting us in processing personal data, are located within the UK and the EEA (“European Region”).

No personal data will be transferred outside the European Region for the provision of services where the personal data has been provided from within the European Region. For the avoidance of doubt, this includes personal data received by Best Companies whether collected directly or indirectly from data subjects. For our EEA clients, in relation to transfers from the EEA to the UK, an adequacy decision remains in place for now. Client should confirm the current status of adequacy decisions periodically to ensure ongoing compliance.

Rest of World

Where our services extend to countries outside of the European Region, please be aware personal data will be transferred, stored and processed within the European Region. This includes personal data received by Best Companies whether collected directly or indirectly from data subjects.

To organisations operating outside of the UK, and within a country without a UK adequacy decision which are subject to an international Transfer Agreement, please send your request to enter an international transfer agreement to privacy@b.co.uk. (Where Applicable).

Publishing Partners

Should a Client be included on one or more of our National, Sector or Regional lists, Best Companies will supply, when necessary, the Client project lead contact details to our Best Companies publishing partner(s) which include but not limited to 3rd party writers. This will only extend to the detail necessary to contact that person, including Name, Organisation, Phone Number, Email Address and Organisation Address. They will make contact where their contractual obligations require them to and when additional information is required for creation of company profiles and case studies. The lawful basis of this processing is Legitimate Interest.

Best Companies Events

Service offered by Best Companies, participation as a guest speaker or attendee watching the event, live or on demand. Best Companies events include but are not limited to workshops, insights and celebrations.

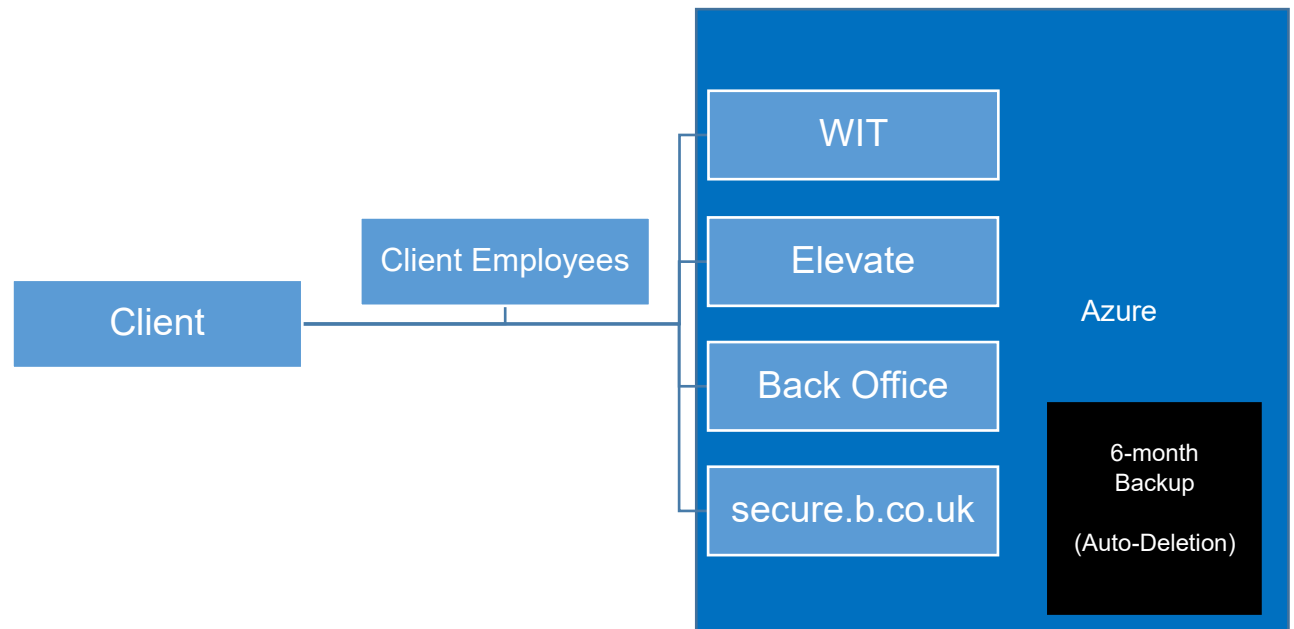
Best Companies on the lawful basis of Legitimate Interest will invite individuals to register for the event who have an association with Best Companies. Employers may select to extend that invitation to the whole organisation as a focal point to celebrate their achievement as a company. Best Companies is the Data Controller of the personal data it receives from individuals who register for the event.

Data Flows

As per diagram 1, data is collected (directly as represented) from the Client and via Client Employees (Employee Engagement data) which goes directly to a SQL database hosted with in Azure. All the calculations are completed and shown in the relevant dashboards WIT, Elevate

hosted within Azure - unless they are having any bespoke reporting which needs manual manipulation - in which case it is held on the on-premise servers which are backed up with Barracuda. Data is deleted in situ, automatically within set retention periods.

Data Storage (diagram 1)



Microsoft Azure: Our live websites are hosted on servers in the cloud with Microsoft Azure: The main data centre we use is called UK South (Situated in London, UK). The Developer System where our code is stored is in Azure (Amsterdam), this can include client data when we have to make manual script changes, alternatively, details are stored on work items in Azure DevOPs.

www.b.co.uk No personal data content so not included (Login Credentials Stored only)

Off- site Cloud Backup (diagram 2)

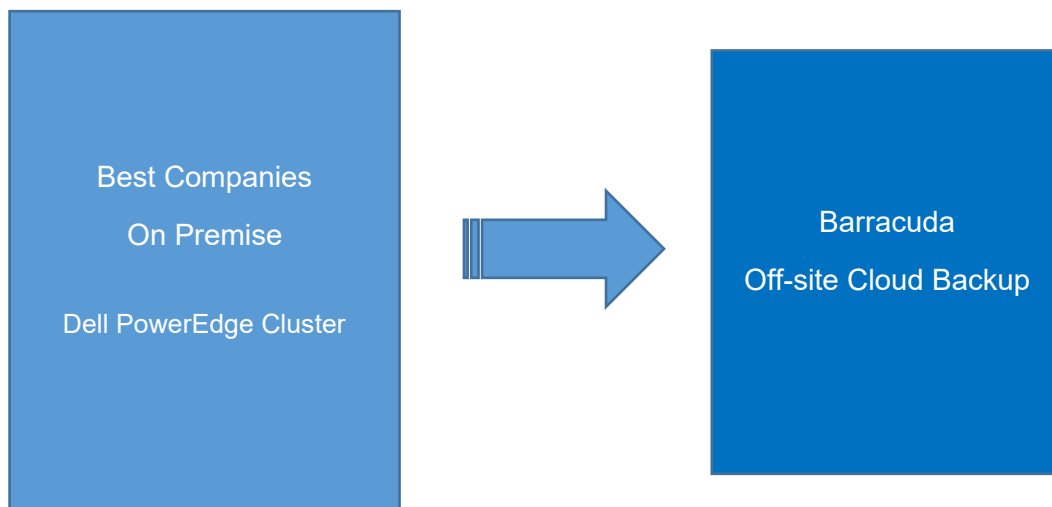


Diagram 2. Off-site Cloud Backup (Barracuda): Data from our on-premise server cluster, is replicated to an on-site Barracuda NAS device, it is then replicated securely to the Barracuda data centre. (Situated in Reading, UK). No data is replicated outside of the EU/EEA.

Deletion (Diagram 3)

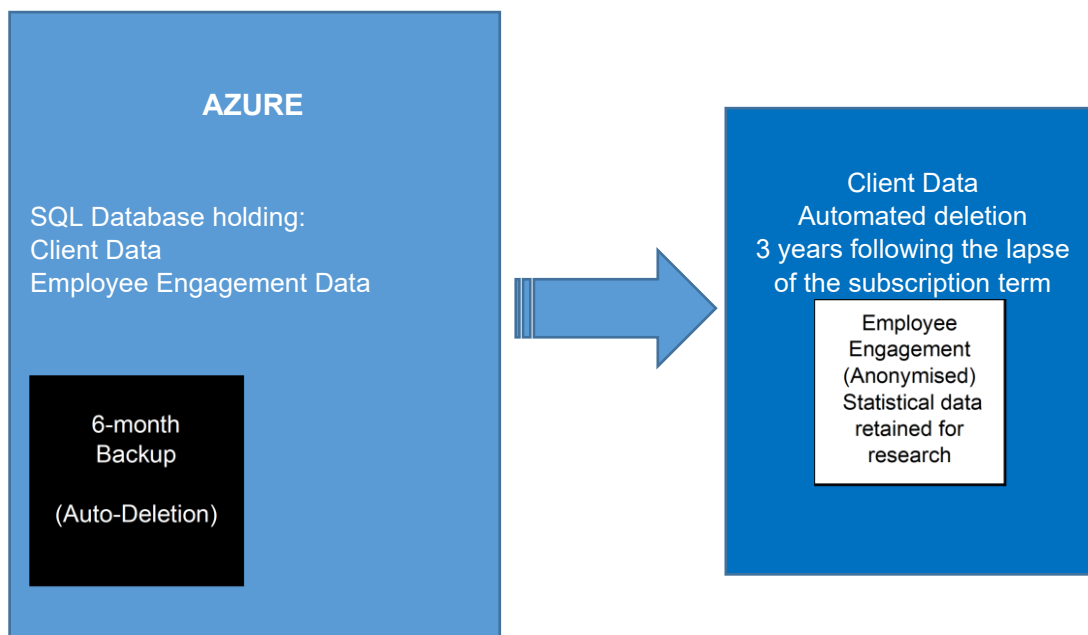


Diagram 3. Data collected from the Client (Client Data) and the survey respondents (Employee Engagement Data) is held on a SQL database within Azure. The Client Data is retained on behalf of the Client as per the contractual agreement, for up to three years following the lapse of the subscription term. Once the Client Data is deleted, the remaining survey respondent data has lost the personal identifiers rendering the data anonymous, leaving behind statistical data only. The statistical data is kept indefinitely and is no longer considered as personal data. Six months backup of the Azure configuration is maintained within Azure, with automated deletion.