HealthBoxHR Ltd – Privacy & Data Processing Policy

Updated and effective as of 20th March 2025

About Us

At HealthboxHR Ltd, we are committed to respecting your privacy. This Privacy Policy explains how we collect, use, and disclose personal information that we receive when you may make use of our HR platform HealthBoxHR (the "**Platform**")

It is important that you read this Privacy Policy so that you are fully aware of how and why we are using your data.

The Platform is owned and operated by HealthBoxHR Ltd (HBHR) a company registered in England and Wales with company number 16132339 and with its registered office at Second Floor, 2 Queens Square, Ascot Business Park, Lyndhurst Road, Ascot, Berkshire, SL5 9FE ("**HBHR**", "**we**", "**our**", and "**us**"). HBHR is registered as a Data Controller with the Information Commissioner's Office (ICO), registration number ZB632544.

Contacting Us

If you have any questions about our Privacy Policy or your information, or wish to exercise any of your rights as described in this Privacy Policy or under data protection laws, you can contact our Data Protection Officer at:

By post:
Data Protection Officer
HealthBoxHR Ltd
Second Floor, 2 Queens Square
Ascot Business Park
Lyndhurst Road
Ascot
Berkshire
SL5 9FE

By email: dataprotection@healthboxhr.com

Definitions

Account Data - personal names, usernames, email addresses and system usage data associated with the client's account

Client Data – personal identifiers, employment information, payroll and financial information, benefits and compliance information

UK GDPR – UK General Data Protection Act. The Data Protection Act (DPA) came into force on 25 May, 2018. The Act updated data protection laws in the UK, supplementing the General Data Protection Regulation (EU) 2016/679 (GDPR). We operate within the UK GDPR which sits alongside an amended version of the DPA 2018

Privacy & Data Processing

HBHR's processing policy in relation to the Client Data provided as part of the Client's use of the Service is in Appendix A of this document. The processing policy sets out the scope, nature and purpose of processing by HBHR, the duration of the processing and the types of Personal Data within the Client Data and categories of data subject. HBHR reserves the right to modify its processing policy where required by the UK GDPR from time to time.

Both parties shall comply with all applicable requirements of the UK GDPR. This clause is in addition to, and does not relieve, remove, or replace, a party's obligations under the UK GDPR.

The parties acknowledge that for the purposes of the UK GDPR, for any Personal Data within:

1. Account Data, HBHR is the data controller.

2. Client Data, the Client is the data controller and HBHR is the data processor. HBHR may only process personal data in line with the Clients documented instructions unless it is required to do otherwise by UK Law. (where data controller and data processor have the meanings as defined in the UK GDPR).

Without prejudice to the generality of the forgoing of this clause, HBHR shall, in relation to any Personal Data within the Client Data:

1. Process that Personal Data only on the written instructions of the Client unless HBHR is required by UK Law to process that Personal Data otherwise. For the avoidance of doubt, entering this Agreement by the Client constitutes written instructions to HBHR to process the Personal Data within the Client Data to enable HBHR to operate and provide the Services, and to otherwise process such Personal Data as identified in this Agreement.

2. Ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it).

3. Ensure that all personnel who have access to and/or process Personal Data are obliged to keep Personal Data confidential.

4. Assist the Client, at the Client's cost, in responding to any request from a data subject and in ensuring compliance with its obligations under the UK GDPR with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators.

5. Notify the Client without undue delay on becoming aware of a Personal Data breach.

6. In anticipation of termination of this Agreement either return or delete the Personal Data in accordance with the Retention and Security of Data in Appendix A, unless required by UK Law to continue to store the Personal Data.

7. Maintain complete and accurate records and information to demonstrate its compliance with this clause and allow for audits by the Client or the Client's designated auditor.

8. HBHR will not transfer any Personal Data within the Client Data outside of the United Kingdom unless requested by the client.

HBHR is permitted to process the Client Data by anonymising it and (where applicable following such anonymisation) aggregating it with other data sources in connection with HBHR's development of its products, strategies, or services or any further purpose related to HBHR's business, including for analytics, marketing, research, development, benchmarking purposes and additional services. For the avoidance of doubt, following such anonymisation, the derivative data shall not be considered to be Personal Data for which HBHR is the data processor on behalf of the Client.

The Client consents to HBHR appointing the following classes of third-party processors of Personal Data under this Agreement:

1. Service providers acting as processors based in the United Kingdom who provide IT, hosting development and system administration services.

2. HM Revenue & Customs, regulators and other authorities acting as processors or joint controllers based in the United Kingdom who require reporting of processing activities in certain circumstances.

HBHR (processor) will not engage any other processor (a sub-processor) without the Client's (controller) prior specific or general written authorisation. If a sub-processor is employed under the Clients general written authorisation, HBHR will let the Client know of any intended changes and give the Client a chance to object to them.

HBHR confirms that it has entered or (as the case may be) will enter into a written agreement incorporating terms which are substantially similar to those set out in this Agreement with any third- party processor who has access to Personal Data within Client Data. As between the Client and HBHR, HBHR shall remain fully liable for any failure of such third-party processor to fulfil such substantially similar data protection obligations as if such actions were the actions of HBHR.

HBHR may, at any time on not less than 30 days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when replaced by attachment to this Agreement).

Appendix A

Processing Policy

This processing policy applies to the Personal Data that we process when providing the Services to you. This Policy must be read alongside the Privacy policy and the T&C's ("Agreement") and any other documents referred to in it. The definitions contained in the Agreement apply to this policy.

Purpose of Processing Data
We process data for the following purposes:
- To manage employment records and HR-related activities.
- To administer payroll and process salary payments.
- To comply with legal and regulatory obligations.
- To facilitate communication and engagement with employees.
- To maintain records for auditing and reporting purposes.
- To provide access to HR and payroll services via our platform.

Our Processing of Data
In providing the Services we will:

- Process the Personal Data that you enter into the Service about the people engaged in your business ("People") that relates to their employment
- Process that Personal Data in the following ways:
  - storing data
  - making data available to you in different formats and media; and
  - presenting that data to you in the form of summaries and reports based on the data.
- For the following purposes:
  - to collate personnel and human resources information together with work and calendar tasks so that the same can be accessed securely and simply
  - to allow such data to be edited and expanded safely and quickly
  - to make tools available to you so that you can analyse the data
  - performance management, absence tracking, and payroll/benefits administration.
  - processing of sensitive data, such as health information and emergency contacts, where applicable.
  - use of AI features for analytics, reporting, or other automated processes.

We will carry out these activities for the duration of our contract with you. Unless we are required by the UK GDPR to store the Personal Data, when the contract ends, we will delete or return the Personal Data to you in accordance with your instructions.

Categories of Data
Data may include, but is not limited to, the following categories of personal information:

Personal Identifiers
- Full name
- Date of birth
- Address
- Email address
- Contact number
- Emergency contact number
- Photographs
- Geolocation
- National Insurance number

Employment Information
- Job title and role
- Department and location
- Employment status (e.g., full-time, part-time, contractual)
- Start and end dates of employment
- Work schedule and shift patterns
- CV's
- Employment history
- Training history and certificates
- Third party references
- DBS applications
- Leave and absence records (holiday entitlement, sick leave)
- Performance and appraisal records
- Training and certification records
- Health and safety compliance data
- Disciplinary records

Payroll and Financial Information
- Salary details
- Payroll and salary history
- Bank account details
- HMRC taxation information, including PAYE details
- Pension contributions and deductions
- Any applicable statutory deductions
- Other absence (including maternity, paternity, bereavement)
- Expenses

Retention and Security of Data

We retain data only for as long as is necessary to fulfil the purposes outlined above and in accordance with the Client's instructions. Unless otherwise requested or required to be kept by a statutory or regulatory body in compliance with our legal obligations, all data will be permanently deleted upon termination of the contract. Appropriate technical and organisational measures are implemented to protect the data against unauthorised access, loss, alteration, or destruction.