GDPR

CLIENT PRIVACY POLICY

This policy sets out the obligations of Handover HR Limited regarding the General Data Protection Regulation and the rights of our clients, their employees and our other business contacts in respect of their personal data.

Avalon House, Waltham Business Park, Brickyard Road, Swanmore, Hampshire, SO32 2SA

0845 389 3505

info@handoverhr.co.uk
www.handoverhr.co.uk

Contents

GDPR

Data Protection Principles

"We are committed not only to the letter of the law, but also to the spirit of the law and we place high importance on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom we deal"

Processed lawfully

Data will be processed lawfully, fairly, and in a transparent manner in relation to the data subject.

Collected for specified purposes

Data will be collected for explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Adequate, relevant and limited

The collection and use of data will be limited to what is necessary in relation to the purposes for which it is processed.

Accurate and kept up to date

Every reasonable step will be taken to ensure that personal data that is inaccurate is erased or rectified without delay.

Kept for no longer than necessary

Data will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

Processed securely

Data will be processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisation measures.

We process HR-related personal data in accordance with these data protection principles.

Lawful, Fair, and Transparent Data Processing

The regulation defines "personal data" as any information relating to an identified or identifiable actual person (a data subject).

This policy sets out the procedures which we will follow when dealing with the personal data or our clients, their employees and our other business contacts.

The regulation states that processing of personal data shall be lawful if at least one of the following applies:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the controller is subject.
- Processing is necessary to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Rights of Data Subjects

The regulation sets out the following rights for data subjects:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (also known as the right to be forgotten)
- The right to restrict processing
- The right to data portability
- The right to object
- Rights with respect to automated decision-making and profiling

"Let us know if you are unhappy about us processing any of your personal data "

What to do if you object to personal data being processed; If you object to us processing your personal data please tell us and we will stop, unless we are able to demonstrate that our legitimate grounds for such processing override your interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

If at any time you object to the Company processing personal data for direct marketing purposes, we will stop as soon as we are made aware.

Lawful, Fair, and Transparent Data Processing continued

Data Subject Access

A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which we hold about them.

We will normally respond within one month of receipt (this can be extended by up to two months in the case of complex and /or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

All subject access requests received must be in writing and forwarded to our data protection officer.

We don't charge a fee for the handling of normal SAR's, but we reserve the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded, vexatious or excessive, particularly where such requests are repetitive.

RECTIFICATION OF PERSONAL DATA

If a data subject informs us that the personal data we hold is inaccurate or incomplete, the personal data in question will be rectified and the data subject informed of the rectification, this will normally happen within one month of receipt of the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases we will inform them of the need for the extension).

ERASURE OF PERSONAL DATA

Data subjects may request that we erase the personal data that we hold

about them in the following circumstances:

- It is no longer necessary for us to hold that personal data with respect to the purpose for which it was originally collected or processed.
- The data subject wishes to withdraw their consent to us holding and processing their personal data.
- The data subject objects to us holding and processing their personal data (and there is no overriding legitimate interest to allow us to continue doing so).
- The personal data has been processed unlawfully.
- The personal data needs to be erased in order for us to comply with a particular legal obligation.

Unless we have reasonable grounds to refuse to erase personal data, all requests shall be complied with, and the data subject will be informed of the erasure, within one month of the request (this can be extended to two months in the case of complex request, and in such cases we will explain the need for the extension).

In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, we will also inform those third parties (unless it is impossible or would require a disproportionate effort to do so).

RESTRICTION OF PERSONAL DATA PROCESSING

Data subjects may request that we cease processing the personal data that we hold about them. If a data subject makes such a request, then we will retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

In the event that any affected personal data has been disclosed to third parties, those parties will be advised of the applicable restrictions on processing (unless it is impossible or would require disproportionate effort to do so).

DATA BREACH NOTIFICATION

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage) the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay, and in any event **within 72 hours** after having become aware of it.

Lawful, Fair, and Transparent Data Processing continued

DATA BREACH NOTIFICATION CONTINUED

Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of our data protection officer (or other contact point where more information can be obtained).
- The likely consequences of the breach.
- Details of the measures taken, or proposed to be taken, by us to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Processing HR-related personal data

We detail the reasons for processing HR-related personal data and how we use it within this policy. We promise not to process it for other reasons.

STORING HR-RELATED PERSONAL DATA

Personal data gathered during the employment, worker or contractor relationship, is held in an individual's personnel file (electronically only) and on our HR system. All third parties providing software or internet and cloud-based services to HHR for the purposes of processing HR-related personal data have demonstrated their compliance with the GDPR.

The periods for which we hold HR-related personal data are detailed below.

DATA SECURITY

We take the security of HR-related personal data seriously. We have internal policies and controls in place particularly to ensure that data is not accessed, except by our staff or our clients' staff in the proper performance of their duties.

Handover HR staff are fully aware of their obligations with regards to the confidentiality of HR-related personal data and the requirements of the GDPR.

"We will not transfer HR-related personal data to countries outside of the EEA"

INDIVIDUAL RESPONSIBILITIES

Employees, workers and contractors are also responsible for helping us keep personal data up to date. Please ensure that you let us know if data provided to us changes, if applicable by updating your records via the self-service HR portal or by using the appropriate form.

Handover HR staff have access to the personal data of others and as a result are required:

- to access only data that they have the authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules of access to premises, computers, password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal drives that are used for work purposes; and
- to report data breaches of which they become aware.

Client Data processed by HHR

Data	Data Subject	Originated from	What is it used for	Where is it stored	How long will we keep it
Personal	Employee / Worker/ Contractor	Individual	HR-related administration and communications	HR System Cloud based file server	For 6 years after the termination of employment or of the contract between HHR and the Client
Contractual	Employee / Worker/ Contractor	Client	HR-related administration and communications	HR System Cloud based file server	For 6 years after the termination of employment or of the contract between HHR and the Client
Payroll	Employee / Worker	Client / Individual	HR-related administration and communications	HR System Cloud based file server	For 6 years after the termination of employment or of the contract between HHR and the Client
Absence	Employee / Worker	Client / Individual	HR-related administration and communications, and compliance	HR System Cloud based file server	For 6 years after the termination of employment or of the contract between HHR and the Client
Accidents	Employee / Worker/ Contractor	Client	Client H&S administration and compliance	HR System Cloud based file server	For 6 years after the termination of employment or of the contract between HHR and the Client
Benefits	Employee / Worker	Client	HR-related administration and communications	HR System Cloud based file server	For 6 years after the termination of employment or of the contract between HHR and the Client
Documents	Employee / Worker/ Contractor	Client / Individual	HR -related administration	HR System Cloud based file server	For 6 years after the termination of employment or of the contract between HHR and the Client
Professional Memberships	Employee/ Worker/ Contractor	Individual	Role specific compliance	HR System Cloud based file server	For 6 years after the termination of employment or of the contract between HHR and the Client

Client Data processed by HHR

Data	Data Subject	Originated from	What is it used for	Where is it stored	How long will we keep it
Qualifications and Training	Employee/ Worker/ Contractor	Individual	Role specific compliance	HR System Cloud based file server	For 6 years after the termination of employment or of the contract between HHR and the Client
Disciplinary & Grievance	Employee/ Worker	Client / Individual	HR-related administration, advice and guidance	HR System Cloud based file server	For 6 years after the termination of employment or of the contract between HHR and the Client
Employment relations information	Employee / Worker	Client / Individual	HR-related administration, advice and guidance	HR System Cloud based file server	For 6 years after the termination of employment or of the contract between HHR and the Client
Recruitment	Applicants for a vacancy (Employee/ Worker/ Contractor)	Individual	Selection of appropriate candidates, and role specific compliance	HR System Cloud based file server	Successful candidates - For 6 years after the termination of employment or of the contract between HHR and the Client Unsuccessful candidates – Records are deleted after 6 months
DBS Verification Certificate	Employee/ Worker/ Contractor	Client	Specific role requirement	HR System Cloud based file server	For 6 years after the termination of employment or of the contract between HHR and the Client
Next of Kin	Employee / Worker/ Contractor	Individual	Advisory in case of emergency.	HR System Cloud based file server	For 6 years after the termination of employment or of the contract between HHR and the Client
Company information	Client contacts	Client / individual representing the company	Contacting clients, providing advice and guidance, sending newsletter, sending invoices.	HR System Cloud based file server, accounting system and CRM	Until the client asks for the details to be removed

Client Data processed by HHR

Data	Data Subject	Originated from	What is it used for	Where is it stored	How long will we keep it
Work contact details	Employee/ Worker/ Contractor	Client / Individual	Contacting clients, providing advice and guidance, sending newsletter, sending invoices	HR System Cloud based file server, accounting system and CRM	Until the client asks for the details to be removed
Sales information	Client contacts	Client / individual representing the company	Managing client relationship, sales administration including reviews and invoicing	HR System Cloud based file server, accounting system and CRM	Until the client asks for the details to be removed

Handover HR Limited is registered with the Information Commissioners Office as a Data Controller

Registration reference: Z8512669
Registration start date: 23 March 2004