H2H Storage Solutions Ltd

Data Protection and Privacy Policy

Version: 1

Issued: March 2023

Contents

Introduction

H2H Storage Solutions Ltd (referred to as the Company, us and our) is committed to meeting the requirements of the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA). Therefore, compliance with current GDPR legislation is regarded as the absolute minimum standard acceptable. This policy sets out how the Company manages those responsibilities.

We recognise the importance of looking after personal data consistent with our legal responsibilities and wider Company values and is fundamental to our success. The Company is registered with the Information Commissioner Office, as a data processor, registration number: ZA928388.

Proper management of personal data is seen as an integral part of the efficient management of the Company's activities, and critical to developing the professional culture of the business and establishing and maintaining a solid reputation with all parties connected with H2H Storage Solutions Ltd.

The Company's arrangements to meet the requirements of the GDPR legislation are detailed in the policy below.

H2H Storage Solutions Ltd obtains, uses, stores and otherwise processes personal data relating to its employees (former and current), customers (including prospective), suppliers, individuals who send enquiries/information to us, visitors to our premises, and for those applying for employment. These are collectively referred to in this policy as data subjects.

A copy of this policy will be held internally with the Staff Handbook located so that employees are able to access this at all times. A paper copy will be kept with the Staff Handbook in each Office location and an electronic version will be kept on Sharepoint. Furthermore, it is also available externally on the Company website https://www.h2hselfstorage.co.uk/privacy-policy/ .

The Company will:

- provide any training necessary as and when appropriate;
- seek specialist advice when required;
- endeavour to adhere to recommendations made by the Information Commissioners Office (ICO); and
- commit adequate resources so that legal obligations can be met.

The Company is committed to being transparent about how it collects and uses the personal data of its data subjects and to meeting its data protection obligations. This policy sets out the Company's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy therefore seeks to ensure that H2H Storage Solutions Ltd:

- Are clear about how personal data must be processed and our expectations for all those who process personal data on its behalf;
- Comply with the data protection law and with good practice;
- Protect our reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights
- Protect us from risks of personal data breaches and other breaches of data protection law.

The GDPR's requirements apply to EU residents' personal information and anyone in the Company who processes that data.

The Data Protection Officer (DPO)

One of the Company Owners, Michelle Broadbent is ultimately responsible for ensuring that the requirements of this policy are achieved, and therefore is referred to as the Data Protection Officer (DPO) for the Company.

The DPO is responsible for ensuring that all employees of the Company, comply with this policy.

Questions about this policy, or requests for further information, should be directed to the Data Protection Officer, via email: michelle@h2hstoragesolutions.co.uk

Definition of key terms

"Data subject" means an individual who is the subject of personal data, of which we hold.

"Personal data" is any information that relates to an individual who can be identified from that data alone or in combination with other identifiers the Company possesses or can reasonably access. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (e.g. name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

"Processing/Process" this includes an activity that involves the use of personal data. It therefore includes, the obtaining, recording or holding data, or carrying out any operation or set of operations on the data. This includes, organising, amending, retrieving, using, disclosing, erasing or destroying. Processing also includes transmitting or transferring Personal Data to third parties. In brief, it is anything that can be done to personal data from its creation (inclusive) to its destruction (inclusive).

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

"Data controller" this is the person or organisation that determines when, why and how to process personal data. They are responsible for establishing practices and policies in accordance with the GDPR. H2H Storage Solutions is the Data Controller of a personal data relating to it and used delivering services to our customers, conducting research and all other purposes connected with it, including business purposes.

"Consent" is the agreement, which must be given freely, is specific and informed and therefore unambiguous in the indication of the data subjects wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.

Data protection principles

The Company ensures that the following data protection principles are followed at all times:

- Personal data is processed lawfully, fairly and in a transparent manner.
- Personal data is collected only for specified, explicit and legitimate purposes and not processed further, in a manner incompatible with those purposes (purpose limitation)
- Personal data is only processed where it is adequate, relevant and limited to what is necessary for the purposes of processing.

- Only personal data that is accurate, relevant and limited to what is necessary is kept (stored) and takes all reasonable steps to ensure that inaccurate or out of date personal data is rectified or deleted without delay.
- Personal data is only kept for the period necessary for processing. Please refer to the Data Retention section of this Policy for further information.
- Appropriate measures are adopted to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The Company tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in this policy. It will not process personal data of individuals for other reasons without express consent.

The Company will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate. It is the responsibility of the individual to ensure that we hold up-to-date records. The Company keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

This includes the following:

- To be informed about the way we collect and use personal data;
- Where the legal basis of the Company's processing is Consent, to withdraw that Consent at any time;
- To ask for access to the personal data that we hold (please see Subject Access Requests below for more information)
- To prevent our use of the personal data for direct marketing purposes;
- To object to our processing of personal data in limited circumstances;
- To ask us to erase personal data without delay:
    - If it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
    - If the legal basis of processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data;
    - If the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and the Company can show no overriding legitimate grounds of interest;
    - If the data subject has objected to the Company's processing for direct marketing purposes;
    - If the processing is unlawful.
- To ask us to rectify inaccurate data or to complete incomplete data;
- To restrict processing in specific circumstances e.g. where there is a complaint about accuracy;
- To ask us for a copy of the safeguards under which personal data is transferred outside of the EU;
- The right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract with the

Company; it is based on the data subject's explicit consent and is subject to safeguards; or is authorised by law and is also subject to safeguards;

- To prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- To be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- To make a complaint to the ICO; and
- In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

Subject access requests

Individuals have the right to make a subject access request. If you wish to do this, you must contact Michelle Broadbent, one of the Company owners at michelle@h2hstoragesolutions.co.uk

In some cases, we may need to ask for proof of identification before the request can be processed. The Company will inform the individual if it needs to verify their identity and the documents it requires.

The Company will provide the individual with a copy of any personal data undergoing processing, that they have requested. This will normally be in electronic form, unless they agree otherwise.

Commonly asked questions:

- **If the data subject wants everything that includes their name, does the Company need to provide this to them?** – No. Only information that is about them, will be provided to them. Information that includes their name, but no information about them, will not be provided.
- **If the Company holds a vast amount of data, regarding the data subject making the request, what will be provided?** – The Company will ask the data subject to be specific, with regards to the information required.
- **What will happen if the data subject is requesting information about them, but also includes personal data regarding someone else?** – The information will be assessed on a case by case basis, as to whether the Company needs the other person's consent to provide their information to the data subject, and if so, carry out the required steps to do this.
- **When might the Company withhold data during a subject access request?** – The Company will try and supply all the personal data a person has asked for. This is because the data protection law is about openness and transparency and therefore people have the right to access their own personal data. However, sometimes it may be appropriate to withhold some or all of the information that someone has asked to be provided. These situations – or exemptions – do not always apply. However, they should always be considered. The two most common are:
    - Third party data; and
    - Crime and taxation (where disclosing the data may prejudice an investigation).

  However, the Company will be required to justify and document their reasons for relying on an exemption.

- **On what grounds can a subject access request be refused entirely?** – Where the Company can, they will give the data subject the data they've asked for in the subject access request. However, it's very unlikely that the Company will be able to refuse the request altogether, but it's possible in certain situations such as if the request is excessive. If the Company decide to refuse all or part of the request, they will note the reasons why. Another possible situation in which the Company might be able to refuse a subject access request is if its unfounded or unreasonable. This can be where the Company has reasonable grounds to believe the person making the request has no real interest in obtaining the information they've asked for, and is only making the request to harass or cause expense to the Company. Both of these situations call for a decision to be made based on the specific situation and if necessary the Company will seek advice and support from the ICO.
- **When would a request be considered as excessive?** – If it repeats or overlaps other recent requests. However, a request isn't excessive just because a large amount of data has been asked for. In these cases though, the Company can ask you to narrow your request or may charge a fee due to the administration time use.
- **Can the Company charge me a fee?** – Yes, if the data subject wants additional copies due to the administration cost of providing these, and if the request is manifestly unfounded or excessive, which again will be based on the administration cost of responding to the request.
- **How long will it take the Company to respond?** - The Company will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the Company processes large amounts of the individual's data, it may respond within three months of the date the request is received. The Company will write to the individual within one month of receiving the original request to tell them if this is the case and to explain why the extension is necessary.

If the Company is not going to respond to the request, the individual will be informed of their right to make a complaint to the ICO or another supervisory authority and their ability to seek to enforce this right through a judicial remedy in accordance with legislative guidelines.

Impact assessments

On rare occasions, some of the processing that the Company carries out may result in high risks to privacy, where the processing would result in a high risk to individual's rights and freedoms, the Company will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

If the Company discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner Office (ICO) within 72 hours of discovery, and without undue delay.

If the ICO decides to undertake an audit following this reporting, the Company will fully cooperate with this process and adhere to any recommendations subsequently made by the ICO.

The Company will record all data breaches regardless of their affect and whether or not the Company is required to notify the ICO using the internal Data Protection Register saved on Sharepoint with the ICO Information.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals without undue delay that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

Main parties

The Company is committed to being transparent about how it collects and uses data and to meeting its data protection obligations.

For the business to function effectively and to provide our business services to our clients, the Company processes personal data relating to five main parties:

1. Applicants

As part of any recruitment process, the Company collects and processes personal data relating to job applicants. From time to time the Company will also receive speculative job submissions.

2. H2H Storage Solution Ltd.'s employees

The Company collects and processes personal data relating to its employees to manage the employment relationship. This includes former employees, contractors, temporary and casual workers.

3. Customers (including prospective)

The Company collects and processes personal data relating to our customers and prospective customers (e.g. those who have sent enquiries/information to us). This is to support the Company in providing the required, relevant and requested business services to them.

4. Suppliers

The Company collects and processes our suppliers personal data for the benefit of managing our business arrangements.

5. Visitors to our premises

The Company collects and processes our visitors to the premises personal data for the benefit of health and safety, fire safety and general security for our employees, clients and business.

What information does the Company collect?

Examples of the information that the Company collects in relation to the main parties described above includes but is not limited to:

Employees (including former, prospective, casual, temporary and contractors)

- name, address and contact details, including email address and telephone number;
- details of qualifications, skills, experience and employment history;
- information about current level of remuneration, including benefit entitlements;
- information about medical or health conditions, including whether or not an individual has a disability for which the Company needs to make reasonable adjustments;
- information about nationality and entitlement to work in the UK;
- the terms and conditions of an individual's employment;
- bank account details (including debit and credit card information where applicable) and national insurance number;
- information about marital status, next of kin, dependants and emergency contacts (the Company will assume that the employee has obtained consent already from the individual they are providing the information for);
- information about an individual's criminal record where applicable;
- details of working hours and attendance at work;
- details of periods of leave taken by the individual, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which an individual has been involved, including any warnings issued to them and related correspondence;
- assessments of performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence; and
- equal opportunities monitoring information, to be used for that purpose only, including information about gender, age, ethnic origin, sexual orientation and religion or belief.
- Information on the pages that you have visited on our websites, demographics and interests (please see our Cookies Policy (https://www.h2hselfstorage.co.uk/cookie/) for more information)
- CCTV imagery (please see the CCTV policy for further information regarding this)

The Company may collect this information in a variety of ways or may be given this information through speculative submissions. For example, data might be collected/contained in application forms, CVs or resumes, obtained from passports or other identity documents, or collected through interviews, meetings or other forms of assessment.

In some cases, the Company may also collect personal data about individuals from third parties, such as references supplied by former employers, information from employment background check providers, information from credit reference agencies and information from criminal records checks permitted by law.

The Company will seek information from third parties only once a conditional job offer has been made and will inform the individual that it is doing so.

Customers (including prospective)

- Name (including title, first name, surname);
- Contact information (address, email address, telephone number);
- Information on the pages that you have visited on our websites, demographics and interests (please see our Cookies Policy (https://www.h2hselfstorage.co.uk/cookie/) for more information);
- If you are another business, we will ask you to confirm your relevant business sector and a URL for your business website;
- Photo identification e.g. passport, driving licence;
- Date of birth;
- Emergency contact details (including name, telephone number and email address) – in this situation, the Company will assume that the customer has sought consent already from the individual they are providing the information for;
- Bank details (including if required debit/credit card information)
- CCTV imagery (if you are visiting our premises)

Where does the Company store personal data?

Data will be stored securely in a range of different places, including paper copies in customer files, personnel files, application forms/records and on IT systems (including cloud storage and email).

Please be advised that we transfer data within our Company and with our suppliers and service providers. We do not transfer data outside of the EEA to suppliers or service providers.

Why does the Company process personal data?

The Company needs to process data for a number of different reasons. For example, to process an individual's data before entering into a contract of employment directly with an individual at the Company.

In some cases, the Company, needs to process data to ensure that the Company is complying with legal obligations. For example, the Company is required to check a successful applicant's eligibility to work in the UK before employment starts, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

In other cases, the Company has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing personal data allows the Company to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;

- obtain occupational health advice, to ensure that the Company complies with duties in relation to individuals with disabilities, meets obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the Company complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- provide references on request for current or former employees of the Company; and
- respond to and defend against legal claims.

The Company may process special categories of data, such as information about ethnic origin, sexual orientation or religion or belief, to monitor recruitment statistics for the purposes of equal opportunities monitoring. The Company may also collect information about whether or not a person is disabled to make reasonable adjustments for individuals who have a disability. Information about health or medical conditions may be processed to carry out employment law obligations in relation to Company employees or our client's employees. For some roles, the Company is obliged to seek information about criminal convictions and offences. Where the Company seeks and processes this information either directly or on behalf of a client, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment.

The Company uses a third party supplier to conduct criminal record checks and has written documentation from this supplier to confirm compliance with the General Data Protection Regulation and to ensure the security of the data.

If a job applicant is unsuccessful, the Company may keep the individual's personal data on file in case there are future employment opportunities for which the individual may be suited .The Company will ask for the individual's consent before it keeps personal data for this purpose and the individual is free to withdraw their consent at any time. It will be held in accordance with the Data Retention section of this policy.

The lawful bases for this processing include: Contractual, Consent, Legitimate Interests, and Legal Obligation.

Who has access to data?

Personal information may be shared internally within the Company with members of the H2H Storage Solution Ltd.'s team and with third party suppliers as and when appropriate.

The Company will not transfer personal data outside the European Economic Area. However, should this change and your personal data is effected, you will be asked to give your explicit consent.

How does the Company protect data?

Third parties

The Company takes the security of personal data seriously. It has internal policies and controls in place to ensure that personal data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties.

Where the Company engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

H2H Storage Solutions employees' individual responsibilities and training

The employees of the Company are responsible for helping us keep their personal data up-to-date. Employees should let the Company know if data provided to the Company changes, for example if an employee moves house or changes their bank details.

Employees may have access to the personal data of other individuals and of our customers in the course of their employment or apprenticeship. Where this is the case, the Company relies on its employees to help meet its data protection obligations to other staff and customers.

Employees who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the Company) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including 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 Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or client data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

The Company will provide training to all our employees about the data protection responsibilities relevant to their role as part of the induction process for any new starters and as and when appropriate for existing staff.

For how long does the Company keep data (Data Retention)?

Data must not be kept any longer than is necessary for a legitimate purpose and it must not be excessive. The Company therefore have systems in place to determine how long the data should be retained and when records should be destroyed securely.

The Data Protection Act 2018 and GDPR do not expressly set out any specific minimum or maximum retention periods.

Certain documents such as employment contracts, accident record books and other personnel records may be needed outside the DPA in a legal action.

Destruction of data will be done securely and effectively.

The Company does however, tend to operate on the following data retention basis to ensure that data is not kept longer than necessary. However, there may some exceptions to this.

Internal Retention Periods

Data Subject and Data Type	Data Retention Period
Former customers – All electronic and hard-copy records	Twenty seven months following issue of last invoice
Former employees – all electronic and hard-copy personnel records except what is specified below	Six years following termination of employment, plus a three-month buffer period. In the event of an early conciliation process, employment tribunal claim, personal injury claim or other legal proceedings including appeals, this will be amended to six years plus a three month buffer period following the resolution of any legal proceedings.
Former employees – COT3, Settlement Agreement or similar legal agreement	Indefinitely
Former employees – name, dates of service, job title, disciplinary action*	Indefinitely, for the purpose of providing employment references. *This information will only be retained in the event of their being a legal obligation to disclose, e.g. for a regulated post in financial services.
Job applicants (speculative and/or unsuccessfully apply for employment with H2H Storage Solutions Ltd) – all electronic and hard copy application and selection records	Six months following notification of decision not to offer, plus a three month buffer period.
Current employees - • Current employees - Contracts and any other documents relating to terms and conditions of employment; • Evidence of right to work; • Employee contact details, including full name, postal address, telephone numbers and personal email address (employee is responsible for providing any updated details); • Emergency contact details (employee is responsible for providing any updated details); • Data required by HMRC, including but not limited to name, date of birth, address, NI number, tax code, etc.; • Pension provider details.	To be retained indefinitely and updated where information provided unless employee become former.

Current employees – interview notes and employment references	Three months following successful completion of the probationary period. The length of the probationary period will vary depending on the role, and will be specified in the employee's contract of employment. This includes any extension of probationary period.
Current employees – file notes	To be retained for 12 months plus a three month buffer or for the duration of an issue being monitored plus a three month buffer, whichever is longer, unless either the employee or client become former.
Current employees – performance records, including appraisal documentation	To be retained for 24 months plus a three-month buffer, or for the duration of an issue being monitored plus a three month buffer, whichever is longer, unless employee becomes former.
Current employees – disciplinary records	Disciplinary warnings and associated file notes will be kept on file for the period for which they are "live"; this period will be specified in the disciplinary hearing outcome letter. During this time, unless a disciplinary warning is overturned at appeal or in some other exceptional circumstance, "right to be forgotten" requests will not be granted in relation to the disciplinary warning. Following the "live" period, disciplinary warnings and associated file notes may continue to be held on file, particularly if relevant to an ongoing performance concern, but will not be used to determine future disciplinary sanctions. The appropriateness of this will be reviewed at six-monthly audit or on receipt of a "right to be forgotten" request Please also see "Former employees" regarding the retention of records following termination of employment.
Current employees – Criminal Record Checks	Certain job roles may necessitate these to be held indefinitely, until the employee becomes former. In such cases records will be updated as appropriate to comply with the Rehabilitation of Offenders Act, e.g. six months following a conviction becoming spent.
Current employees – Medical Reports	Medical records relating to specific periods of illness that are not recurring or continuous will be retained for the period of any reasonable adjustments (including any phased return to work) plus a three-month buffer; or 12 months since last symptoms/reasonable adjustments plus a three-month buffer; or a recurrence of related symptoms plus a three-month buffer, whichever the longer. Medical records relating to an ongoing illness or disability (continuous or recurring), including records of requests for and arrangement of reasonable adjustments, will be retained indefinitely and updated where information

	provided, unless employee becomes former, when above guidelines will apply. In certain circumstances, for example for medical records specified under the Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH), statutory periods apply to the retention of medical records. In the event that a statutory retention period applies to any data held by H2H Storage Solutions Ltd, the statutory period will be adhered to, plus a three-month buffer period. The timescales set out above will be applied when no statutory retention period is relevant.
Current employees - Capability records.	Capability warnings and associated file notes will be kept on file for the period for which they are "live"; this period will be specified in the capability hearing outcome letter. Following the "live" period, capability warnings and associated file notes may continue to be held on file, particularly if relevant to an ongoing concern. The appropriateness of this will be reviewed at six-monthly audit or on receipt of a "right to be forgotten" request.
Current employees - Payroll records.	Six years from the end of the tax year to which they relate.
Current employees – Pension records.	Records will be kept about what contributions you pay to your pension scheme, for at least six years.
Current employees - Health and safety records.	Most health and safety documents need to be kept for five years. However, risk assessment records should be kept as long as the particular process or activity, to which the assessment refer, is performed. Despite this the Company will always ensure that risk assessments are kept for a minimum of three years.
CCTV Footage	Six months following the outcome of a formal decision or appeal. CCTV footage may be relevant to a disciplinary matter or unfair dismissal.

Statutory Retention Periods

In the event that a statutory retention period applies to any data held by H2H Storage Solutions Ltd, the statutory period will be adhered to, plus a three-month buffer period. Please note that in the event of any apparent discrepancy between the internal retention periods set out above, and the statutory periods listed below, the statutory retention periods (plus a three-month buffer period) will apply.

These timescales are correct at the time of this policy being approved, and will be reviewed to ensure they remain applicable. In the event of any changes to statutory retention periods being made prior to the review of this policy, the statutory retention period in force at the time of any six-monthly audit will be applied (plus a three-month buffer period).

Statutory periods from https://www.cipd.co.uk/knowledge/fundamentals/people/hr/keeping-records-factsheet

Data Type	Data Retention Period
Accident books, accident records/reports.	Three years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21). (See below for accidents involving chemicals or asbestos). See: The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980. Special rules apply concerning incidents involving hazardous substances (see below).
Accounting records	Not less than three years. See: Section 221 of the Companies Act 1985 as modified by the Companies Act 1989 and 2006.
First aid training	Six years after employment. See: Health and Safety (First Aid) Regulations 1981
Fire warden training	Six years after employment. See: Fire Precautions (Workplace) Regulations 1997
Health and Safety representatives and employees' training	Five years after employment. See: Health and Safety (Consultation) Regulations 1996; Health and Safety Information for Employees Regulations 1989.
Income tax and NI returns, income tax records and correspondence with HMRC.	Not less than three years after the end of the financial year to which they relate. See: The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended.
Medical records and details of biological tests under the Control of Lead at Work Regulations.	Forty years from the date of the last entry. See: The Control of Lead at Work Regulations 1998 (SI 1998/543) as amended by the Control of Lead at Work Regulations 2002 (SI 2002/2676).
Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH).	Forty years from the date of the last entry. See: The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677).
Medical records under the Control of Asbestos at Work Regulations.	Forty years from the date of the last entry (medical records); Four years from the date of issue (medical examination certificates) . See: The Control of Asbestos at Work Regulations 2002, 2006 and 2012 (SI 2002/ 2675) (SI 2006/2739) and (SI 2012/632)
Medical records under the Ionising Radiations Regulations 1999.	Until the person reaches seventy five years of age, but in any event for at least fifty years.

	See: The Ionising Radiations Regulations 1999 (SI 1999/3232).
Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)	Five years from the date on which the tests were carried out. See: The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (Sis 1999/437 and 2002/2677)
Records relating to children and young adults.	Until the child/young adult reaches the age of twenty one. See: Limitation Act 1980.
Retirement Benefits Schemes	Six years from the end of the scheme year in which the event took place. See: The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103).
Statutory Maternity Pay records, including Mat B1s (also shared parental, paternity and adoption pay records)	Three years after the end of the tax year in which the maternity period ends. See: The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended, Maternity & Parental Leave Regulations 1999.
Wage/salary records (also overtime, bonuses, expenses).	Six years from the end of the tax year to which they relate. See: Taxes Management Act 1970.
National minimum wage records	Three years after the end of the pay reference period following the one that the records cover. See: National Minimum Wage Act 1998.
Subject access request	One year following completion of the request. See: Data Protection Act 2018
Whistleblowing documents	Six months following the outcome (if a substantiated investigation). If unsubstantiated, personal data should be removed immediately. See: Public Interest Disclosure Act 1998 and recommended IAPP practice.
Working time records including overtime, annual holiday, time off for dependents, etc.	Two years from date on which they were made. See: The Working Time Regulations 1998 (SI 1998/1833).

What if an individual does not provide personal data?

Job applicants are under no statutory or contractual obligation to provide data to the Company during the recruitment process. However, if an individual does not provide the information, the Company may not be able to process their application properly or at all.

Customers are under no statutory or contractual obligation to provide data to the Company. However, if an individual does not provide the required information, the Company may not be able to provide the services required.

H2H Storage Solutions Ltd.'s employees have some obligations under their employment contract to provide the employing organisation with data. In particular, employees are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. Employees may also have to provide the employing organisation with data in order to exercise their statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that employees are unable to exercise their statutory rights. Certain information, such as contact details, an employee's right to work in the UK and payment details, have to be provided to enable the employing organisation to enter a contract of employment with the employee. If the employee does not provide other information, this will hinder the employing organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Changes to this policy

H2H Storage Solutions Ltd reserves the right to update this Data Protection and Privacy Policy at any time and the updated Policy will be available internally (In each Office location and on Sharepoint) and externally on the Company website when any substantial updates are made. In the event of any legislative changes, these changes will prevail if there is any discrepancy with this policy. The Company may also notify relevant parties in other ways from time to time about the processing of their personal information as appropriate.

Making a complaint to the ICO

You have the right to make a complaint to the ICO, if you believe that we are not using your data in accordance with the law.

You can do this via telephone: 030 123 1113

Or visit their website: https://ico.org.uk/make-a-complaint/