













HILL & SMITH LTD EMPLOYEE PRIVACY NOTICE

| Topic | | Page number |
|---|---|-------------|
| INTRODUCTION TO GDPR |  | 2 |
| ABOUT US & THIS NOTICE |  | 3 |
| USEFUL WORDS & PHRASES |  | 4 |
| WHAT DATA DOES GDPR APPLY TO? |  | 5 |
| WHY DO WE PROCESS YOUR PERSONAL DATA? |  | 6 |
| WHAT INFORMATION DOES GDPR APPLY TO & HOW IS IT LAWFUL? |  | 9 |
| WHO WILL HAVE ACCESS TO YOUR PERSONAL DATA AND WHY? PROCESSORS & CONTROLLERS |  | 11 |
| SECURITY & DATA BREACHES |  | 13 |
| WHEN WILL WE DELETE YOUR DATA? |  | 14 |
| YOUR RIGHTS |  | 16 |



INTRODUCTION TO GENERAL DATA PROTECTION REGULATIONS

This Privacy Notice is provided by Hill & Smith Ltd. We are a 'controller' and a 'processor' for the purposes of the General Data Protection Regulation (EU) 2016/679 ("Data Protection Laws").

In an age of information, more data is available than ever before. In order to help protect our employees, contractors, customers and suppliers from having their data used improperly, new protections have been introduced.

GDPR or the General Data Protection Regulation is a new set of EU regulations set to come into force, as an update to, whilst still enforcing the existing Data Protection Act (DPA) 1998. A lot has changed since then in terms of technology and therefore stricter security is required on how data is processed, stored and shared.

The regulations came into force on 25th May 2018. However, the implementation of GDPR will be ongoing following a planned schedule after this date and we will continue to review our current systems and paperwork in accordance with the legislation.

Key Summary:

We process your personal information as your employer and for no other purpose.

We share your information with suppliers who act on our behalf for services such as payroll, HR system support, training, flight bookings, taxi services and on-site security in order to support you during the course of your employment. In addition, we share your personal information to set up your account with providers of services such as pensions, insurance, SAYE and life assurance. They provide these services to you directly and not on our behalf. This notice explains what data we process, why, how it is legal and your rights.

This Privacy Notice applies to all Hill & Smith Limited employees, agency workers and individual contractors who we will refer to generally as 'staff', regarding updates to Data regulations on how personal and sensitive data collected by your employer, is stored.

We take your privacy very seriously. We ask that you read this Privacy Notice carefully as it contains important information about our processing and your rights.



ABOUT US & THIS NOTICE

This Privacy Notice is provided by Hill & Smith Ltd ("Hill & Smith") or "we" or "us") who is a 'controller' for the purposes of the laws governing data protection. This means that we are responsible for looking after your personal data. This Privacy Notice applies to all Hill & Smith employees, agency workers and individual contractors who we will refer to generally as 'staff'.

How to contact us

If you need to contact us about this Privacy Notice, use the details below:

- GDPR Lead – James Thomas Finance Director
- Address: Hill & Smith Ltd, Bilston WV14 0QL
- Telephone number: (: 01902 499400
- E-mail: gdpr@hill-smith.co.uk

If you would like this Privacy Notice in another format (for example: audio, large print, braille), please contact HR.

Changes to this Privacy Notice

The Privacy Notice will be provided to you when you receive your employment/service contract with Hill & Smith Ltd.

We may update this Privacy Notice occasionally. It is your responsibility to check this Privacy Notice regularly to ensure you are aware of the most recent version that applies.

The latest version is available from HR or alternatively copies will be made available within divisions and the main reception area.

Current version: v1 July 2019 [subject to change]



USEFUL WORDS AND PHRASES

Please familiarise yourself with the following words and phrases (used in bold) as they have particular meanings in the Data Protection Laws and are used throughout this Privacy Notice:

| Term | Definition |
|----------------------------|--|
| controller | This means any person who determines the purposes for which, and the manner in which, any personal data is processed. |
| criminal offence data | This means any information relating to criminal convictions and offences committed or allegedly committed. |
| Data Protection Laws | This means the laws which govern the handling of personal data. This includes the General Data Protection Regulation (EU) 2016/679 and any other national laws implementing that Regulation or related to data protection. |
| data subject | The person to whom the personal data relates. |
| ICO | This means the UK Information Commissioner's Office which is responsible for implementing, overseeing and enforcing the Data Protection Laws. |
| personal data | <p>This means any information from which a <u>living individual</u> can be identified.</p> <p>This will include information such as telephone numbers, names, addresses, e-mail addresses, photographs and voice recordings. It will also include expressions of opinion and indications of intentions about data subjects (and their own expressions of opinion/intentions).</p> <p>It will also cover information which on its own does not identify someone but which would identify them if put together with other information which we have or are likely to have in the future.</p> |
| processing | <p>This covers virtually anything anyone can do with personal data, including:</p> <ul style="list-style-type: none">• obtaining, recording, retrieving, consulting or holding it;• organising, adapting or altering it;• disclosing, disseminating or otherwise making it available; and• aligning, blocking, erasing or destroying it. |
| processor | This means any person who processes the personal data on behalf of the controller. |
| special categories of data | <p>This means any information relating to:</p> <ul style="list-style-type: none">• racial or ethnic origin;• political opinions;• religious beliefs or beliefs of a similar nature;• trade union membership;• physical or mental health or condition;• sexual life; or• genetic data or biometric data for the purpose of uniquely identifying you. |



WHAT DATA DOES GDPR APPLY TO?

Information provided by you: To employ you or enable you to work for us as an agency/contractor, we may collect the following information from you:

| Personal data | Special categories of data |
|--|---|
| <ul style="list-style-type: none"> • Name • Contact details (address, phone number, email address) • Date of birth • Country of birth • Marital status • Bank account details • National Insurance Number • Passport / right to work information • Photographs / CCTV Images • Sickness and absence records • Employment history and references • Professional qualifications • Appraisals • Training records • Nationality • Academic and professional qualifications • Employment history | <ul style="list-style-type: none"> • Medical health • GP Details • Vaccination / Immunisation History • Medical History • Absenteeism due to illness • Safety Critical Information where required • Occupational Health Reports where required • Drug and Alcohol testing results |
| Other category data | |
| <p>Monitoring of ICT usage Hill & Smith Ltd Electronic Communications Policy explains how Hill & Smith Ltd monitor the usage of IT.</p> <p>Pool vehicle/Company car If employees' drive a company car, drive on behalf of the company or make use of the pool car when it becomes available, we require a copy of employee's driving licences and information contained within it relating to address, DOB and driving sanctions etc.</p> <p>Travel Hill & Smith Ltd Travel & Expenses policy details what information is collected for employees travel.</p> <p>CCTV Hill & Smith operates a CCTV network within its work premises, which collects video footage. This footage is not monitored unless there is a cause for concern. I.e. investigation, health & safety or security. [This list is not exhaustive]. Date, time and visual images taken from various places around the site. Average storage of images is 20 days, and the storage is re-cycled. Live streams are seen in reception and the gatehouse. Signs are shown on the external fences, advising that CCTV is in operation. Please refer to the Electronic Communications Policy and the Group CCTV Policy for more information on data collected, as well as the general rules, on the operation of our CCTVs.</p> <p>Personal information provided to third parties We use other third parties to provide some of our services such as LifeWorks Employee Assistance Programme, SAYE, Bupa, Aon Life Insurance etc. When you sign up for these services, we will share your personal information only as necessary for the third party to provide that service. This could include personal and sensitive information but will only be shared if necessary for the service they supply.</p> <p>Personal information about other individuals If you provide us with information about other individuals e.g. your next of kin, or spouses or dependants named on any polices you confirm that you have informed the relevant individuals accordingly.</p> | |



WHY DO WE PROCESS YOUR PERSONAL DATA?

We use your personal data for the following purposes listed in this section. We are allowed to do so on certain legal bases (please see section 'How is processing your data lawful' for further detail).

In what way is your data processed and why?

This covers multiple things that can be done with personal data, including:

- obtaining, recording, retrieving, consulting or holding it;
- organising, adapting or altering it;
- disclosing, disseminating or otherwise making it available; and
- aligning, blocking, erasing or destroying it.

Why do we hold personal data and on what legal grounds?

We hold and use your ordinary data for employment, HR, Payroll, administration purposes such as your contract, pay and benefits, monitoring holidays and leave. Data protection law specifies the legal grounds on which we can hold and use personal data.

Why do we hold sensitive /special category data and on what legal grounds?

Special category data is usually required for specific reasons such to meet specific requirements of employment; it is considered more sensitive such as health conditions for sick pay and workplace adjustments. Family related information, parental and carers leave, categories covered under equality and diversity monitoring – Age, Gender, Sexual orientation, Race, political affiliations. Extra care and security is taken with the processing and storing of this information.

| Purpose | Explanation |
|------------------------------|--|
| Payroll Pension and Accounts | To calculate and pay your salary and pension contributions and to keep business accounts. |
| Benefits | To calculate, pay and provide benefits such as employer pension contributions, life assurance and private medical cover. |
| Business Development | To develop our business generally including through marketing (i.e. we may provide your name, work contact details and/or experience to potential and existing customers and/or suppliers). |
| Staff Administration | To administer your employment with us. For example, this will include, complying with employment contracts, assessing performance and career development, performing our legal obligations, administering our policies and to administer medical and sickness records, sick pay/leave information, holiday/absence, appraisals, promotions, disciplinary and grievance matters, maternity, parental leave and time off for dependants. |
| Business Travel | To administer any travel and/or accommodation arrangements where you are required to travel within or outside of the UK for work. |
| Prevention and Detection of | To prevent and detect crime. This might include processing special categories of data and/or criminal offences data. |

| | |
|---|---|
| Crime | |
| Equal Opportunities | To promote and monitor equal opportunities. This might include the processing special categories of data including, religious or similar beliefs and ethnic origin. |
| Tax | To administer our revenue and tax obligations. |
| Training and Career Development | To administer and supervise your training and career development. |
| Health and Safety | To comply with health and safety laws and our policies. This may include us processing special categories of data, such as details of your mental and physical health. |
| Regulatory and Professional Requirements | To comply with regulations and professional requirements to which Hill & Smith is subject. |
| Corporate finance, Mergers and Acquisitions | To carry out group company restructuring, to sell any of the Hill & Smith companies or acquire or merge with other businesses. We may disclose your personal data and special categories of data for any of the above purposes, including at negotiation stage. |
| Occupational health | To meet our duty of care as your employer to help you manage your work environment and address any health issues it may be causing. This may include us processing special categories of data, such as details of your physical health. |
| Random testing | To carry out random drugs and alcohol testing to ensure that you are physically able carry out your duties at work or to drive, and/or operate machinery where this forms part of your duties at work and generally able to perform your duties. |
| Visa information | To ensure we fulfil our obligations to employ only people with a right to work in the UK. This may involve obtaining personal data from the Home Office or other governments or bodies responsible for visas or migration globally. |

We may monitor and record communications with you (such as telephone conversations and emails) for the purpose of quality assurance, training, fraud prevention and compliance.

| | |
|----------------------------------|---|
| IT Maintenance | To maintain and update IT Resources and to monitor for viruses and other disruptive programmes. |
| Unauthorised use of IT resources | To determine whether any IT resources are being used without authorisation either by employees or external hackers. |
| Information Gathering | To establish the existence of business related facts and/or to determine whether communications are relevant to our business. For example, if you are away from work, to establish whether incoming e-mails are from |

| | |
|-----------------------------|---|
| | customers or business partners and to ensure that they are properly dealt with during your absence. |
| Legal and Policy Compliance | To determine whether Hill & Smith and/or you are complying with legal requirements, our policies and rules and any other requirements which Hill & Smith and/or you should comply with. |
| Quality Standards | To determine whether you are attaining standards which you ought to be achieving, such as customer service standards. |

What's new?

The requirement to have a lawful basis in order to process personal data is not new. It replaces and mirrors the previous requirement to satisfy one of the 'conditions for processing' under the Data Protection Act 1998 (the 1998 Act). However, GDPR places more emphasis on being accountable for and transparent about the lawful basis for processing.

The six lawful bases for processing are broadly similar to the old conditions for processing, although there are some differences. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the purpose and relationship with the individual.

If we are processing special category or criminal conviction data, we must identify both a lawful basis for general processing and an additional condition for processing this type of data.

We will be reviewing existing processing, identifying the most appropriate lawful basis, and checking that it applies. In many cases it is likely to be the same as the existing condition for processing.



WHAT INFORMATION DOES GDPR APPLY TO & HOW IS IT LAWFUL?

Personal data:

GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

We are allowed to process your personal data for the following reasons and on the following legal bases:

Legitimate Interests:

We are permitted to process your personal data if it is based on our 'legitimate interests' i.e. we have good, sensible, practical reasons for processing your personal data which is in the interests of Hill & Smith. To do so, we have considered the impact on your interests and rights, and have placed appropriate safeguards to ensure that the intrusion on your privacy is reduced as much as possible. The table below explains the personal data processed on this basis.

| Personal data | Legitimate Interests |
|---|--|
| <ul style="list-style-type: none">• Appraisals• Training records• Professional qualifications | To maintain and develop efficiency and competence of our staff. This captures information about you in the context of your job role and is therefore not intrusive. It is also beneficial to you to help you develop your skills and qualifications. |
| <ul style="list-style-type: none">• Video images caught by CCTV | To keep our premises and staff safe from unauthorised access. |
| <ul style="list-style-type: none">• Email content• Instant message content• Internet activity information• Phone usage | To protect our network and ensure that our IT resources are being used in a safe and secure manner against unauthorised access and data leakage in line with our internal information security policy. |
| <ul style="list-style-type: none">• Driving licence• Location of the company car during its use• Information on your use of the company car | To ensure that staff (i) use the car in a safe and secure manner that does not risk harm to themselves and to others and (ii) do not breach the terms of the company car policy. This helps us to ensure that you are safe, to manage our assets and make business planning decisions. The information collected about you can be shared with you. |
| <ul style="list-style-type: none">• Location of your accommodation during overseas travel | So we can inform staff of unusual risks when they are abroad e.g. natural disasters, riots, military action |
| <ul style="list-style-type: none">• Photos• Contact details• Professional experience | To promote Hill & Smith to prospective customers to develop new business or grow existing relationships |

You can object to processing that we carry out on the grounds of legitimate interests. See the section headed "[Your Rights](#)" to find out how.

[What are the lawful bases for processing?](#)

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever your personal data is processed:

[Contract](#)

It is necessary for our performance of the employment contract you have agreed to enter with us. If you do not provide your personal data to us, we will not be able to carry out our obligations under the terms of your employment contract. For example, we require your personal data to pay your salary.

[Legal obligation](#)

We are subject to legal obligations to process your personal data for the purposes of complying with applicable regulatory, accounting and financial rules, health and safety and to make mandatory disclosures to government bodies and law enforcements.

[Consent](#)

Sometimes we want to use your personal data in a way that is entirely optional for you, such as an occupational health assessment, or which is not directly linked to your job, such as your photos of your family at a Hill & Smith Ltd fundraising day. On these occasions, we will ask for your consent to use your information. You can withdraw this consent at any time and this will not affect your employment with us in any way.

[Sensitive personal data](#)

GDPR refers to sensitive personal data as "special categories of personal data". The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

[Consent](#)

You have given your explicit consent for us to process your medical history data for the purposes of an occupational health assessment.

[Employment](#)

We need to process your personal data to carry out our obligations as your employer, for example, putting in place specific equipment in our offices to cater for particular physical conditions our staff may have.

[Necessary for the purposes of occupational medicine, including the assessment of your working capacity as an employee](#)

We will process information about your health obtained during the recruitment process and further routine assessments in order to assess your medical capacity to perform the job you have applied for.

[Vital Interests](#)

It is necessary for us to process your medical/health information, for the purposes of protecting your health and safety during the course of your employment.

[Manifestly public personal data](#)

The processing relates to information that you have made public, for example, attire you wear for work and information made public on a public social media platform.

[Legal claims](#)

We need to process your personal data if, during the course of your employment with us, we are required to process your personal data to defend or establish a legal claim, for example, for employment tribunals relating to employment claims under employment law. We may also be required to process ethics data as required by law.

These principles lie at the heart of our approach to processing personal data.



WHO WILL HAVE ACCESS TO YOUR DATA & WHY?

Controller

A controller is an entity that decides the purpose and manner that personal data is used, or will be used. Hill and Smith Ltd is the Data controller. This means it is responsible for deciding how it holds and uses personal data about you.

Processor

The processor is the person or group that processes the data on behalf of the controller. Processing is obtaining, recording, adapting or holding personal data, such as HR collecting and collating information from a new employee. Payroll processes the monthly or weekly payments etc.

Why do we need it?

In a digital data-driven world there is the need for protection from data breaches, especially companies holding all kinds of personal data. We could not employ you without your personal data being provided.

Systems and Processes in place to ensure your data are kept safe:

Security: GDPR will enforce ever stricter rules upon organisations to ensure that they are taking all reasonable measures to guard against data theft, loss, or other breach. Hill & Smith Ltd will be taking action to show clear evidence that diligent measures in regard to security software, physical security, and other aspects such as disaster recovery plans are in place.

A personal data breach means a breach of security leading to one or more of the following occurring to personal data that we control or process:

- destruction;
- loss;
- alteration;
- unauthorised disclosure; or
- unauthorised access.

The cause of the above can be accidental or deliberate and can be caused by someone within the business or an external party.

We share your personal data that is relevant, where appropriate, with our ultimate group parent company Hill & Smith Holdings PLC. Our legal grounds for doing so are that it is necessary to fulfil our contractual obligations to you under the terms of your employment; it is in our legitimate interests to comply with the policies and procedures applicable within our corporate group and to obtain guidance and support from our corporate group's central support functions.

The table below lists some of our key service providers that act as our processors who will have access to your personal data. If you would like to know the names of our other service providers e.g. training providers, please contact us using the details at the start of this Privacy Notice.

We believe that sharing your information with these providers is a fair approach to take. We believe that these providers perform standard, enterprise IT services which require 'passive' processing i.e. hosting and running applications, or providing support, none of which requires those suppliers to actively deal with the data. Therefore they have not all been listed, as the list would be very lengthy and will change from time to time but not in a way that affects data subjects' rights. The controller will provide this information if someone wants it in order to be fair and transparent.

Non – Exhaustive list of companies' information is shared with; from time to time

- Spirit Occupational Health
- Site based testing with Tier 1 contractors
- Hampton Knight Drug & Alcohol Testing
- Training Providers
- HR/Payroll
- Shred It for disposal of confidential documents
- Southall's – Safety Cloud

In addition, we share your personal data with the following entities who act as separate controllers of your personal data. We provide them with your name and contact details so that they can contact you separately in order to arrange services/benefits directly with you, or to note you on our company group policies. You should review their privacy notices to find out how they process your personal data. If you have any queries or complaints about how they process your personal data by them, please contact them separately using the contact information provided on their website.

We will also share your personal data with the police, other law enforcements or regulators where we are required by law to do so.

External providers who we typically see in this context:

- Bupa/Aon - Health insurance provider
- Legal & General - Pension provider
- Aon - Insurance provider (life insurance, income protection)
- LifeWorks– Employee Assistance Programmer

Transfers of your personal data outside the EEA

We may need to transfer your personal data to countries outside the European Economic Area such as Australia, India and America, all of which are located outside the EEA, for the purpose of:

- fulfilling your employment
- fulfilment of a contract with a customer
- sharing central systems across our group of companies;

Any transfer of your data will be carried out in accordance with the law to safeguard your privacy rights and give you remedies in the unlikely event of a security breach or to any other similar approved mechanisms. If you want to know more about how data is transferred, please contact us using the details in the section above, "How to contact us".

Please note that from time to time our service providers may change.



SECURITY & DATA BREACHES

How we keep your personal data secure

We strive to implement appropriate technical and organisational measures in order to protect your personal data against accidental or unlawful destruction, accidental loss or alteration, unauthorised disclosure or access and any other unlawful forms of processing. We aim to ensure that the level of security and the measures adopted to protect your personal data are appropriate for the risks presented by the nature and use of your personal data. We follow recognised industry practices for protecting our IT environment and physical facilities.

Data Breaches:

Data Protection is everyone's responsibility:

It is the responsibility of all employees to report any data breaches via the correct procedure.

In the event that you are made aware of any kind of data breach, please see process below.

Escalation process:

1. Notify the GDPR Lead James Thomas, immediately;
2. Establish whether a personal data breach has occurred;
3. If a personal data breach has occurred agree with the GDPR Lead the steps to address the breach;
[See GDPR Breach Management Process]
4. Assess and establish, with the GDPR Lead, the likelihood and severity of the resulting risk to all relevant data subjects' rights and freedoms;
5. Complete a data breach record for the GDPR Lead's approval;
6. Implement the steps to address the breach;
7. If relevant, notify the ICO within 72 hours of the personal data breach following approval of the Group Company Secretary, Alex Henderson; and
8. If relevant, notify the affected Data Subjects directly and without undue delay following approval of the Group Company Secretary, Alex Henderson.

*****Please note that in the event of a data breach all persons affected will be informed where necessary to do so according to ICO Guidance*****



WHEN WILL WE DELETE YOUR DATA?

We will generally retain your personal data and special categories of data during the course of your employment/service contract and for 6 years after your employment/service terminates, save for any personal data that is no longer necessary for the purpose collected.

The following categories of personal data and special categories of data provide you with an example of personal data we will generally retain and data which shall have a different retention period.

| Personal data/Special categories of data | Retention period |
|--|--|
| Basic staff and training records, including: <ul style="list-style-type: none"> • Recruitment records, qualifications and references • Annual/assessment reports • Job history • Resignation, termination and/or retirement letters • Travel and subsistence claims • Disciplinary/grievance matters • Annual leave records • Written particulars of employment, contracts of employment, and notices of changes to terms and conditions | Termination of employment + 6 years (however any personal data to be kept no longer than is necessary for the purpose collected) |
| Working time opt-out forms and records to show compliance with the Working Time Regulations 1998, including: <ul style="list-style-type: none"> • Time-sheets for opted-out workers • Health assessments for night workers • Records of working hours for young-workers | Two years from the date on which they were entered into |
| Collective workforce agreements and past agreements that could affect present staff | Permanently |
| Works Council minutes | Permanently |
| Maternity records Adoption and paternity records Shared parental leave records | Termination of employment + 6 years (however any personal data to be kept no longer than is necessary for the purpose collected) |
| Sickness records required for the purposes of statutory sick pay | Termination of employment + 6 years (however any personal data to be kept no longer than is necessary for the purpose collected) |
| Staff bank details Employee personal data form (emergency contact and address information) | Termination of employment + 6 months |
| Immigration checks | Validity of document + 3 years |
| Medical, health and accident records | Termination of employment + 6 years (however any personal data to be kept no longer than is necessary for the purpose collected) |
| Employee related benefits information | Discontinuation of benefits + 8 years |

| Personal data/Special categories of data | Retention period |
|---|---|
| Payroll and wage records PAYE | 6 years from the financial year-end in which payments were made |
| Pension scheme records | 6 years from the end of the scheme year to which they relate |
| Pension scheme records – deceases retiree | Where no widow/widowers or orphan pension payable: 6 years from end of scheme year in which death occurred or date of last transaction. Where widow/widowers or orphan pension payable: 25 years from end of scheme year in which death occurred (or until orphan completes higher education, if later) |
| Any reportable accident, death or injury in connection with work | Three years from the date the report was made |
| Disability claim files | Date claim made + 10 years |
| Litigation files | Date of judgment or settlement + 7 years |
| Details of any exposure to hazardous substances and materials in the operating unit workplace | Creation of record + 40 years |
| Health and Safety Incident Logs | Creation of record + 3 years |
| Radiation Assessments and Records | Creation of record + 50 years (or until person exposed to radiation reaches the age of 75) |
| Company Directors' Records including: <ul style="list-style-type: none"> · Directors' service contracts · Any contract made between a Director and [Hill & Smith] · Pension/benefit details · Severance package records | Termination of employment + 10 years |
| Records of access / disclosure requests | 10 years (but not longer than is necessary for purpose supplied / collected) |
| Emails and email accounts | No longer than 12 months beyond leave date |



YOUR RIGHTS

As a data subject, you have the following rights under the Data Protection Laws:

- the right to object to processing of your personal data;
- the right of access to personal data relating to you (known as data subject access request);
- the right to correct any mistakes in your information;
- the right to prevent your personal data being processed;
- the right to have your personal data ported to another controller;
- the right to erasure; and
- rights in relation to automated decision making (note this does not apply).

These rights are explained in more detail below. We will respond to any rights that you exercise within a month of receiving your request, unless the request is particularly complex, in which case we will respond within three months.

Please be aware that there are exceptions and exemptions that apply to some of the rights which we will apply in accordance with the Data Protection Laws.

[Right to object to processing of your personal data](#)

You may object to us processing your personal data where we rely on a legitimate interest as our legal grounds for processing.

If you object to us processing your personal data we must demonstrate compelling grounds for continuing to do so. We believe we have demonstrated compelling grounds in the section headed "How is processing your personal data lawful". The key point to note is that much of the processing under this heading is beneficial to you, such as assisting with your career development or keeping you safe on our premises.

[Right to access personal data relating to you – Subject Access Request](#)

You may ask to see what personal data we hold about you and be provided with:

- a copy of the personal data;
- details of the purpose for which the personal data is being or is to be processed;
- details of the recipients or classes of recipients to whom the personal data is or may be disclosed, including if they are overseas and what protections are used for those overseas transfers;
- the period for which the personal data is held (or the criteria we use to determine how long it is held);
- any information available about the source of that data; and
- whether we carry out an automated decision-making, or profiling, and where we do information about the logic involved and the envisaged outcome or consequences of that decision or profiling.

This is known as a Subject Access Request.

To help us find the information easily, please provide us as much information as possible about the type of information you would like to see. We will consider your request and reasons for your request and if they are considered manifestly unfounded/excessive we may charge a fee or refuse the request.

[Right to correct any mistakes in your information](#)

You can require us to correct any mistakes in your information which we hold. If you would like to do this, please let us know what information is incorrect and what it should be replaced with.

[Right to restrict processing of personal data](#)

You may request that we stop processing your personal data temporarily if:

- you do not think that your data is accurate. We will start processing again once we have checked whether or not it is accurate;

- the processing is unlawful but you do not want us to erase your data;
- we no longer need the personal data for our processing, but you need the data to establish, exercise or defend legal claims; or
- you have objected to processing because you believe that your interests should override our legitimate interests.

[Right to data portability](#)

You may ask for an electronic copy of your personal data which we hold electronically and which we process when we have entered into a contract with you. You can also ask us to provide this directly to another party.

[Right to erasure](#)

You can ask us to erase your personal data where:

- you do not believe that we need your data in order to process it for the purposes set out in this Privacy Notice;
- if you had given us consent to process your data, you withdraw that consent and we cannot otherwise legally process your data;
- you object to our processing and we do not have any legitimate interests that mean we can continue to process your data; or
- your data has been processed unlawfully or has not been erased when it should have been.

[Rights in relation to automated decision making](#)

We do not make any automated decisions about you so this right does not apply.

[What will happen if your rights are breached?](#)

You may be entitled to compensation for damage caused by contravention of the Data Protection laws.

[Complaints to the regulator](#)

It is important that you ensure you have read this Privacy Notice - and if you do not think that we have processed your data in accordance with this notice - you should let us know as soon as possible. You may also complain to the ICO. Information about how to do this is available on the ICO's website at www.ico.org.uk

[Consent:](#)

If you would like access to your data for a specific reason, you will need to express that you consent to us processing your information in this way.

This Notice aims to ensure that you are clear about Hill & Smiths Ltd's reasons for obtaining personal data, and that what we do with the data is in line with the reasonable expectations of the individuals concerned. If you would like to read further about how GDPR and how it affects you, please visit <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>

What happens now?

1. Privacy Notices: You will be issued with information and updates relating to GDPR and any following updates will be issued, as part of your contractual employment terms.
2. Contract Change: You will also be issued with an addendum to your contract of employment relating to GDPR. We ask that you read and sign your acceptance and understanding of the statement.

We all have a responsibility to comply with these changes and your co-operation is both required and appreciated.

Thank you for your continued support.
Hill & Smith Ltd.