Paterson Simons & Co (Africa) Ltd Employee Privacy Policy QD058

Paterson Simons & Co (Africa) Ltd is a responsible and ethical employer. We regard the lawful, transparent and fair treatment of personal data as very important to maintaining confidence. We collect personal data only for specified, explicit and legitimate purposes and keep it for a specified period. Accuracy is very important, and we take all reasonable steps to ensure inaccurate personal data is rectified or deleted without delay. We adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, accidental loss, destruction or damage.

This policy sets out the Company's commitment to data protection, individual rights and obligations in relation to personal data. Please take a minute to read and understand the policy.

Who this policy covers

This policy applies to the personal data of employees, workers, contractors, volunteers, interns, apprentices and former employees, referred to as HR-related personal data. It does not apply to the personal data of job applicants, clients or other personal data processed for business purposes for which we have separate privacy policies.

Who does what – the legal bits

We hold and use your personal information in accordance with the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Data controller: Paterson Simons & Co (Africa) Ltd Limited. Telephone 01273 623843
Nominated representative: John Traynor, Managing Director. John@patersonsimons.com

Personal data: is any information that relates to an individual who can be identified from that information

Processing: is any use made of data, including collecting, storing, amending, disclosing or destroying it

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

Why we collect and process your data

We need to process data to enter into an employment contract with you and to meet its obligations. For example, we need to process your data to pay you in accordance with your employment contract and to administer your benefits.

In some cases, we need to hold and process data to ensure we comply with our legal obligations. For example, we are required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws, to enable employees to take periods of leave to which they are entitled, and for reporting purposes.

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

- Maintain accurate and up to date employment records and contact details (including who to contact in 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, 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 employees are receiving the pay or other benefits to which they are entitled
- Obtain occupational health advice, to ensure we comply with duties in relation to individuals with disabilities, meet our obligations under health and safety law
- Operate and keep a record of other types of leave including maternity, paternity, adoption, parental and shared parental leave, to allow effective workforce management, and to ensure we comply with duties in relation to leave entitlement
- Ensure effective general HR and business administration, planning, budgeting and financial management
- Provide references on request for current or former employees
- Respond to and defend against legal claims
- Maintain and promote equality in the workplace

Some special categories of personal data, such as information about health or medical conditions, are processed to carry out employment law obligations (for instance those in relation to employees with disabilities).

Where we process other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data we use for these purposes is anonymised or is collected with the express consent of employees, which can be withdrawn at any time. You are entirely free to decide whether to provide such data and there are no consequences for failing to do so.

What information we collect

We collect and process a range of personal information about you which may include:

- Your name, postal address and contact details including your email, telephone numbers both land line and mobile
- Data of birth
- Gender
- Your terms and conditions of employment
- Details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and us, your CV

- Information about your remuneration, including entitlement to benefits such as healthcare, pensions and insurance cover
- Your bank account details, driving licence details and national insurance number
- Information about your marital status, next of kin, dependants and emergency contacts
- Information about your nationality and entitlement to work in the UK
- Information about any criminal record
- Details of your schedule of work, days and working hours, and attendance at work
- Details of leave you take including holiday, sick absence, family leave and sabbaticals, and the reasons for the leave
- Details of any disciplinary or grievance procedures you have been involved in, including any warnings issued to you and related correspondence
- Assessments of your performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence
- Information about medical or health conditions, including whether you have a disability for which we need to make reasonable adjustments
- Equal opportunities monitoring information including information about your ethnic origin

We collect the above information in a variety of ways. For example: data might be collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during your employment such as benefit nomination forms or information you input into the Company's HR management system; from correspondence with you or your advisors, medical practitioners; or through interviews, meetings or other assessments. We may also collect personal data about you from third parties, such as references supplied by former employers, background check providers, or credit reference agencies and information from criminal records checks permitted by law.

How long we keep your data

We will hold your personal data for the duration of your employment. Some of your data is held after the end of your employment if:

- The law requires us to hold it for longer in which case we will hold it for the period the law requires
- For management information purposes and comparisons with prior periods

The relevant retention periods for each set of data are set out below:

SET OF INFORMATION	RETENTION PERIOD
Personal contact details	Deleted at the end of the financial year following the sixth anniversary of leaving the Company. Employee name and NI no. will be retained
Remuneration details (bank details, salary, commission/bonus, NI No, tax code etc)	Bank details deleted once final payment made. All other records kept for six years after leaving
Personal details (DOB, gender, nationality, passport details, marital status, disability information, immigration status)	Delete details at the end of the financial year following the sixth anniversary of leaving the Company
Next of kin contact details	Delete on leaving employment
Employee Details (job details, hours of work, work patterns, holiday entitlement, sickness records)	Retain start/leave date, job title, part/full time information for future references and record of employment. All other detail deleted after six years. Sick and accident absence information retained indefinitely in case of personal injury claim
Employment contact details (work email, telephone, equipment held)	Deleted on leaving employment
Performance information (probationary review, performance appraisals, disciplinary and grievance records, training records)	Delete 6 years after leaving employment
Contractual information (terms and conditions, JD, CV, offer letter)	Delete 6 years after leaving employment

Where we store your data

Data will be stored in a range of different places including in your personnel file (in hard copy or electronic format, or both), in our HR management system and in other IT systems including our email system. All information you provide to us is stored on our secure servers. Where we have given you (or where you have chosen) a password which enables you to access certain systems, you are responsible for keeping this password confidential. We ask you not to share your password with anyone.

The data that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). It may also be processed by staff operating outside the EEA working for us or for one of our suppliers or a service provider who may host our websites and store personal information on our behalf. By submitting your personal data, you agree to this transfer, storing and processing. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy.

Who has access to your data

Your information may be shared internally, including with members of the HR, finance, your line manager, senior managers and IT staff if access to the data is necessary for performance of their roles.

We share your data with third parties to obtain pre-employment references from other employers or referees you supply to us, obtain employment background checks from third-party providers and obtain

necessary criminal records checks from the Disclosure and Barring Service if applicable. We may also share your data with third parties in the context of a sale of some or all the business. In those circumstances, the data will be subject to confidentiality arrangements.

We also share your data with third parties who process data on our behalf in connection with payroll, HR management systems, the provision of benefits and the provision of occupational health services.

Your contact details may be shared with other companies with whom we do business in the ordinary course of business.

We will only disclose your personal information to government bodies and law enforcement agencies to comply with any legal obligation, or to protect the rights, property or safety of our staff, our company or others.

Your rights

As a data subject, you have several rights in relation to your personal data.

Subject access requests

You have the right to make a subject access request. If you make a subject access request, we will tell you:

- Whether or not your data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from you
- To whom your data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers
- How long your personal data is stored (or how that period is decided)
- Your rights to rectification or erasure of data, or to restrict or object to processing your data
- Your right to complain to the Information Commissioner if you think we have failed to comply with your data protection rights
- Whether or not we carry out automated decision-making and the logic involved in any such decision-making

We will also provide you with a copy of the personal data undergoing processing. This will normally be in electronic form if you have made a request electronically, unless you agree otherwise.

If you want additional copies, we will charge a fee based on the administrative cost of providing the additional copies.

To make a subject access request, you should send the request to the Managing Director, John@patersonsimons.com . In some cases, we may need to ask for proof of identification before the request can be processed. We will inform you if we need to verify your identity and any documentation we require.

We will normally respond to a request within a period of one month from the date it is received. In some cases, such as where we process large amounts of the individual's data, we may respond within three

months of the date the request is received. We will write to you within one month of receiving the original request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, we are not obliged to comply with it. Alternatively, we can agree to respond and will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which we have already responded. If you submit a request that is unfounded or excessive, we will notify you this is the case and whether we will respond to it.

Other rights

You have several other rights in relation to your personal data. You can require us to:

- Rectify inaccurate data
- Stop processing or erase data which is no longer necessary for the purposes of processing
- Stop processing or erase data if your interests override our legitimate grounds for processing data (where we rely on our legitimate interests as a reason for processing data)
- Stop processing or erase data if processing is unlawful
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether your interests override our legitimate grounds for processing data

To ask us to take any of these steps, you should send the request to our Managing Director, John@patersonsimons.com

Individual responsibilities

You are responsible for helping us keep your personal data up to date. You should let us know if data provided to us changes, for example if you move house or change your bank details you should update the Company's online HR management system or speak directly to our payroll administrator who will be happy to help you.

You may have access to the personal data of other employees, of our customers and clients during your employment, contract, volunteer period, internship or apprenticeship with us. Where this is the case, we rely on you to help meet our data protection obligations to employees, customers and clients. You have a duty of confidentiality as outlined in the terms and conditions of your contract.

If you have access to personal data, you are required:

- To access only data you 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 our 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 devices that are used for work purposes

Failure to observe these requirements and your duty of confidentiality may amount to a disciplinary offence, which will be dealt with under our disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

What if you do not provide personal data

You have some obligations under your employment contract to provide the Company with data, in particular, you 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. You may also have to provide us with data to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, must be provided to enable us to enter a contract of employment with you. If you do not provide other information, this will hinder our ability to administer efficiently the rights and obligations arising as a result of the employment relationship.

Security

We take the security of your data seriously. We have put in place security procedures and technical and organisational measures to safeguard your personal information against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

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

Data breaches

If we discover there has been a breach of HR-related personal data which poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of discovery. We will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals there has been a breach and provide them with information about its likely consequences and the mitigation measures we have taken.

Changes to policy

This policy is available in our shared drive along with the Employee Handbook. If we change our privacy policies and procedures, we will post the changes to the drive.