POLICY IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION

MAY 25, 2018

PAYCORP INVESTMENTS (PTY) LTD

Table of contents

Policy prepared by	Group Legal & Compliance
Approved by Board/management on	
Policy was implemented on	25 May 2018
Next review date	

Purpose of the General Data Protection Regulation 2016 ("GDPR")

The GDPR is a regulation in EU law and lays down rules relating to the protection of natural persons with regards to the processing of personal data and rules relating to the free movement of personal data. The GDPR therefore protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

Key terms

Personal data and data subject	any information relating to an identified or identifiable natural person ('data subject')
Identifiable natural person	one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Controller	This is a person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Processor	This is a "person, public authority agency or any other body which processes personal data on behalf of the controller".

Principles of the GDPR

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

- "processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

What information does the GDPR apply to?

Personal data	This is **"**any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".
Sensitive personal data	The GDPR refers to sensitive personal data as "special categories of personal data" as set out in Article 9. These categories are broadly the same as those in the DPA, but there are some minor changes. For example, 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 (see Article 10).

Who has responsibility for personal information?

Everyone that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

The following people however have key areas of responsibility:

Board of Directors	Ultimately responsible for ensuring the company meets its legal obligations.
Data protection officer	Responsible for: • Keeping the board updated about data protection responsibilities, risks and issues. • Reviewing all data protection procedures and related policies, in line with an agreed schedule. • Arranging data protection training and advice for the people covered by this policy. • Handling data protection questions from staff. • Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
IT manager	Responsible for: • Ensuring all systems, services and equipment used for storing data meet acceptable security standards. • Performing regular checks and scans to ensure security hardware and software is functioning properly. • Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
Marketing manager	Responsible for: • Approving any data protection statements attached to communications such as emails and letters. • Addressing any data protection queries from journalists or media outlets like newspapers. • Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

Protecting personal information

Appropriate technical and organisational measures will be implemented to protect personal data. These measures take into account, inter alia, the purpose of the processing, the state of the technology and the implementation costs.

Training and acceptance of responsibilities

All staff, volunteers, contractors, suppliers and other people who have access to any kind of personal data will be given copies of all relevant policies and procedures during their induction process and/or the initial engagement of the relationship for handling personal data and will be expected to adhere to all policies and procedures.

Policy review

This policy will be reviewed at least annually and it will also be reviewed in response to changes in relevant legislation, contractual arrangements, good practice or in response to an identified failing in its effectiveness. A current version of this document will be made available to all members of staff and will be published as and when changes are made.

Should you require further assistance, please contact: Group Legal: Omesha Moodley on +27 11 566 5066 or email OmeshaM@paycorp.co.za.