STELLENBOSCH UNIVERSITY

(hereinafter "the University", "SU")

Data Privacy Regulation

Type of document	Regulation
Accessibility	General (external and internal)
Date of implementation	1 March 2019
Date of revision / frequency of revision	Annually
Previous revisions	None
Owner of these regulations	Rector and Vice-Chancellor, as statutory Information Officer
Institutional functionary responsible for these regulations	Vice-Rector: Strategy and Internationalisation
Date of approval	5 February 2019
Approved by	The Rectorate
Keywords	personal information, privacy

1. INTRODUCTION

South Africa has enshrined the right to privacy within the South African Bill of Rights (Constitution of the Republic of South Africa, 1996) and has given effect to that right through the Protection of Personal Information Act (4 of 2013) ("POPIA"). The University is committed to protecting the privacy of our students, employees, and partners, in line with POPIA and related South African legislation, global leading practices, and our commitment to good institutional governance. This regulation:

- articulates Stellenbosch University's institutional stance on privacy; and
- clarifies POPIA's principles within Stellenbosch University's institutional context and values.

2. IMPLEMENTATION OF THIS REGULATION

This regulation applies to all:

- University students (both full-time and part-time) and staff (both permanent and temporary), members of institutional statutory bodies, and third party suppliers and vendors; and
- processes that include the processing of personal information, including but not limited to institutional business processes and academic (teaching and learning, research) processes.

Process owners, in line with institutional governance goals and leading corporate governance practices[1], must, within 18 months of the implementation of this regulation, both:

- apply the principles discussed in this regulation in the analysis, design, and execution of any process that includes the processing of personal information;
- explain and document how the principles have been applied; and
- for processes where third parties are involved in the processing of personal information, ensure that the third parties are contractually obligated to apply and explain the principles within this regulation.

[1] Including the King IV Report on Corporate Governance for South Africa 2016.

Laws are not static and the South African judiciary makes allowance for nuance and context. Thus, to support the implementation of this regulation, the Division for Information Governance must make itself reasonably available to process owners and assist them with the interpretation, application, and implementation of this regulation within their processes.

3. DEFINITIONS

'**Data subject**', as defined in POPIA, means the person to whom personal information relates. Data subjects may include, but are not limited to:

- prospective students;
- applicants;
- students;
- alumni;
- research participants;
- employees;
- employment candidates;
- visitors; and
- members of the public.

'**Personal information**', as defined in POPIA, means information relating to an identifiable, living individual or identifiable, existing company, including, but not limited to:

- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person; and
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

A '**Process**' is a collection of practices influenced by the institution's policies and procedures that takes inputs from a number of sources (including other processes), manipulates the inputs and produces outputs (such as products, services, or research findings)[2].

[2] Adapted from ISACA (2012) COBIT 5 *A Business Framework for the Governance and Management of Enterprise IT*.

'**Process owner**' is the individual accountable for the performance of a process in realising its objectives, driving process improvement, and approving process changes[1]. Process owners include, but are not limited to, researchers, academics, and the line management of PASS environments.

'**Processing**', as defined in POPIA means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information including:

- the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- disseminations by means of transmission, distribution, or making available in any other form; or
- merging, linking, as well as restriction, degradation, erasure, or destruction of information.

4. PURPOSE OF THIS REGULATION

This regulation, through clarifying foundational principles that give effect to the right to privacy, establishes and enables an institutional framework for the processing of personal information that positions respect for data subjects, transparency, accountability, and auditability at its core.

5. AIM OF THIS REGULATION

This regulation:

a) articulates Stellenbosch University's institutional stance on privacy;
b) supports efforts to give effect to the constitutional right to privacy within Stellenbosch University; and
c) supports the management of risks and opportunities surrounding personal information processing.

6. REGULATION PRINCIPLES

POPIA's definition of processing establishes a phased lifecycle for personal information. When considered alongside international legislation[3], this regulation positions four distinct phases within the lifecycle:

Phase	Activities
Preliminary	Planning and design activities that take place before actual processing of personal information.
Collection and Creation	Collection, receipt, creation, recording of personal information.
Utilisation	Organisation, collation, storage, securing, updating or modification, access, retrieval, alteration, consultation or use, dissemination, merging, linking, restriction, degradation of personal information.
Disposal	Erasure or destruction of personal information.

Though process owners must apply all of the principles of protecting personal information throughout the entire lifecycle, this regulation establishes, by phase, when the application of (or the articulation of the application of) a principle is most pertinent.

<u>Phase 1: Preliminary</u>

[3] Including the European Union's General Data Protection Regulation.

Principle 1: Privacy by design

Process owners must give effect to the right to privacy by design within their processes before processing starts. Process owners must thus consider privacy and the protection of personal information during the analysis and design of their processes. Specifically, process owners must, during the design of a new process or review and analysis of an existent process:

- conduct a privacy impact assessment to determine the lawfulness of and to identify and evaluate risks associated with the proposed processing of personal information;
- use the outcomes of the assessment to identify and design appropriate and reasonable measures within their processes to mitigate identified risks (which may include halting a process determined as unlawful); and
- document the outcomes of the assessment and how it informed the design of the process.

Principle 2: Secure by design and by default

Process owners must, utilising the outcomes of the privacy impact assessment, identify, design, implement, and document reasonable technical, organisational, and procedural information security and cyber security measures within their processes to ensure the confidentiality, integrity, and availability of personal information.

Phase 2: Collection and Creation

Principle 3: Minimal processing

Process owners must ensure that their processes do not collect more personal information than is necessary or relevant to the process.

Principle 4: Accuracy

Decisions made on inaccurate information may expose the institution, process owner, and data subject to unnecessary risk or harm. Process owners must take reasonable measures to ensure the accuracy of any collected personal information. Where reasonably possible, process owners must ensure that their processes collect personal information directly from data subjects.

Principle 5: Notification

Process owners must take reasonably practicable steps to notify data subjects of any personal information processing.

Principle 6: Consent

Any consent to the processing of personal information, according to POPIA, must be “voluntary, specific, and an informed expression of will in terms of which permission is given for the processing of personal

information." If consent is the basis for the processing activity, data subjects must be able to freely withdraw consent.
Consent is not always necessary, practical, or desirable for every potential process. Consent should only be used as a justification to process personal information if no other grounds exist. If the processing of personal information is required to conclude or perform in terms of a contract or to comply with legislation, obtaining consent is never appropriate, because the data subject will not be able to withdraw the consent.

Process owners must thus determine the need for consent during the design of their process (i.e. as part of the privacy impact assessment). If process owners identify a need to capture consent, such consent processes must align with the provisions of POPIA.

Phase 3: Utilisation

Principle 7: For specific purposes

Process owners must ensure that any processing of personal information must align with the original specified and documented purpose for collecting the personal information as specified in the privacy notice or consent procedures (see principles 5 and 6).

Some further processing of personal information may be allowable under law when such processing aligns with the original specified purpose for collecting the personal information. Within the context of Stellenbosch University, such further processing may still be subject to research ethics approval and/or institutional gatekeeper permission.

Principle 8: Access

Process owners must ensure that their processes give effect to all data subject rights. This includes giving data subjects access to mechanisms that allow them:

1. access to their personal information;
2. to change or correct their personal information; and
3. to have their personal information deleted if the information is inaccurate, irrelevant or if Stellenbosch University is no longer authorised to have it (see principle 10 for more detail).

Principle 9: Breach notification

POPIA expects Stellenbosch University to have procedures in place to detect, report, investigate, and contain personal information breaches. The University already has existent breach procedures in place. Where reasonably possible, process owners must ensure that their processes align with the institutional breach procedures.

Where process owners cannot reasonably align their processes with the institutional procedures (such as in specific research projects), they must still establish breach procedures aligned with the outcomes of their privacy impact assessment (see principle 1). For research projects, process owners should address this

requirement through the research ethics approval and/or institutional gatekeeper permission processes (see principle 7).

Phase 4: Disposal

Principle 10: Defensible disposal

Process owners should not keep personal information for longer than is required. POPIA considers the storage and retention of personal information as processing of personal information (see definitions). Long-term storage may also expose the institution, the process owner, and the data subjects to unnecessary risk. Process owners must ensure the proper disposal of a record or personal information as soon as reasonably practicable after achieving the purpose for which the information was originally collected (see principle 7) through:

- archiving records with vital or historical value as per the Stellenbosch University Records Management Policy; or
- destruction, deletion, or de-identification of a record or personal information as per the Stellenbosch University Records Management Policy.

7. NON-COMPLIANCE WITH THIS REGULATION

Failure to apply and explain the principles within this regulation to processing of personal information may render the University or the individuals, involved with processing, non-compliant with South African privacy-related legislation. This non-compliance may lead to fines and claims against Stellenbosch University and/or the individuals involved under South African legislation. Non-compliance may further expose the University to significant reputational harm and data subjects to unnecessary risk and harm.

Based on the nature of the non-compliance, Stellenbosch University may execute its information breach procedures.

Stellenbosch University may take disciplinary action against staff or students for non-compliance with this regulation. Stellenbosch University may take action, as allowed by contractual agreement or relevant legislation, against members of institutional statutory bodies and third party suppliers and vendors for non-compliance with this regulation.

8. CONTROL OVER THIS REGULATION

The Rector and Vice-Chancellor owns these regulations as statutory Information Officer. S/he is ultimately accountable for all processing of personal information within Stellenbosch University and thereby responsible for the existence, implementation, monitoring of compliance, and reporting compliance and non-compliance of this regulation to the University's Council and Rectorate.

The Vice-Rector: Strategy and Internationalisation, supported by the Division for Information Governance, serves as curator of these regulations. S/he is responsible for the formulation, approval, maintenance and revision, and communication and release of these regulations. This includes monitoring and accounting for changes in the applicable legislations.

9. RELATED DOCUMENTATION

- Stellenbosch University: Information Management Policy
- Stellenbosch University: Institutional Breach Procedure
- Stellenbosch University: Manual in terms of section 14 and 51 of the Promotion of Access to Information Act 2 of 2000
- Stellenbosch University: Policy for Responsible Research Conduct at Stellenbosch University
- Stellenbosch University: Records Management Policy
- Stellenbosch University: Regulations for recruiting Stellenbosch University persons as research participants and for conducting research on Stellenbosch University-held personal and institutional information
- Universities South Africa: POPIA Code of Conduct for South African Universities
- Universities South Africa: EU GDPR Guidelines for South African Universities

ANNEXURE A: MAPPING OF REGULATION PRINCIPLES TO THE POPIA CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

POPIA establishes eight conditions for the lawful processing of personal information. The table below summarises how, in developing the principles, the University has considered the eight conditions:

POPIA Condition	**Principle(s)**
Accountability	Through establishing this regulation, the Rector has established the accountability and responsibility structures for the processing of personal information within the University.
Processing Limitation	Privacy by Design; Minimal Processing; Accuracy, Notification, and Consent
Purpose Specification	Privacy by Design; Minimal Processing; For Specific Purposes; Defensible Disposal
Further Processing Limitation	Privacy by Design; For Specific Purposes; Defensible Disposal
Information Quality	Privacy by Design; Accuracy; Access
Openness	Privacy by Design; Notification
Security Safeguards	Secure by Design; Breach Notification
Data Subject Participation	Access