Stellenbosch
UNIVERSITY
IYUNIVESITHI
UNIVERSITEIT

Privacy Regulation

forward together
sonke siya phambili
saam vorentoe

Contents

Privacy Regulation


Privacy

Stellenbosch University Privacy Regulation

Type of document:	Regulation
Purpose:	To articulate the Stellenbosch University stance and understanding of privacy-related legislation; to articulate Stellenbosch University staff and student privacy-related responsibilities.
Approved by:	Rectorate
Date of approval:	25 May 2022
Date of implementation:	1 October 2022
Date of next revision/frequency of revision:	Biennially
Previous revisions:	2019
Regulation owner[1]:	Rector & Vice-Chancellor (as statutory Information Officer)
Regulation curator[2]:	Deputy Information Officer
Keywords:	Privacy, personal information, data protection
Validity:	The English version of this regulation is the operative version, and the Afrikaans version is the translation.

[1] Regulation Owner: Head(s) of Responsibility Centre(s) in which the regulation functions.
[2] Regulation Curator: Administrative head of the division responsible for the implementation and maintenance of the regulation.

1. Introduction

South Africa has enshrined the right to privacy within the South African Bill of Rights (The Constitution of the Republic of South Africa (Act 108 of 1996)) and has given effect to that right through the Protection of Personal Information Act (Act 4 of 2013) ("POPIA"). Stellenbosch University is committed to protecting the privacy of our students, employees, and partners, in line with POPIA and related South African legislation, international legislation when applicable, 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. 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.

'Operator', as defined in POPIA, means a person who process personal information for a responsible party in terms of a contract of mandate, without coming under the direct authority of that party.

'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.

'Privacy impact assessment', also sometimes referred to as 'data protection impact assessment' or 'personal information impact assessment', is a process designed to describe personal information processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal information by assessing them and determining the measures to address them. This definition was adapted from European Union's *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.*

'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.

'Responsible party', as defined in POPIA, means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

3. Purpose of the regulation

The purpose of this regulation is to promote an enabling institutional environment wherein personal information is managed in a manner that supports the University in giving effect to the right to privacy.

4. Aims of the regulation

Through this regulation, the University aims to support the implementation of a coordinated, multi-disciplinary, and integrated approach towards managing personal information.

5. Scope and application

This regulation applies to:

- all Stellenbosch University information curators;
- all Stellenbosch University students (both full-time and part-time) and staff (both permanent and temporary), members of institutional statutory bodies, and to the extent applicable or required, third-party collaborators, suppliers, contractors, service providers, and vendors;
- all personal information processed within, by, or for Stellenbosch University; and
- all processes that include the processing of personal information, including but not limited to institutional business processes and academic (teaching and learning, research) processes.

Any reference to personal information in this regulation also refers to personally identifiable information and personal data. This enables the application of the regulation principles in the broadest sense, regardless of differences in terminology by subject, legislation, or jurisdiction.

This regulation forms part of Stellenbosch University's broader information management framework. Refer to the framework for related policies and regulations, details on core concepts, such as information curators, and additional definitions.

6. Regulation principles

POPIA is a principles-based piece of legislation. This regulation articulates Stellenbosch University's understanding of those principles within the University's context. When considering a conflict between POPIA, as amended from time to time, and this regulation, POPIA shall be considered the valid guiding document.

Stellenbosch University's information curators must apply the following principles to any processing of personal information within their environments. Stellenbosch University information curators must document and be able to explain the application of these principles on any processing of personal information. Through this approach, information curators, within their environments, must formalise the privacy-related guardrails that enable the responsible processing of personal information in day-to-day operations.

The Division for Information Governance provides the enabling training, support, and tools for our information curators. Information curators can find more details about these services at www.sun.ac.za/privacy.

6.1 Information curators must recognise, understand, and respond appropriately to the value of information.

6.1.1. All information has value. Before processing personal information, or as soon as reasonably possible for existent processes, information curators must conduct a privacy impact assessment to recognise and understand the value of personal information processed within their environments.

6.1.2. Information follows a lifecycle, starting with collection or creation, then usage and storage, and finally disposal of information. Information curators must identify and document all processes associated with any personal information processed within their environment. This includes noting the sources of personal information, the processing activities, through to the retention and disposal of personal information.

6.1.3. Taking the value and lifecycle of the personal information into account, information curators must design, implement, and test controls to protect the personal information processed within their environments.

6.2 Information curators must recognise, understand, and respond appropriately to the justifications for the lawful processing of personal information.

6.2.1 There must be a legal basis for any processing of personal information. POPIA positions several possible justifications[3] for the lawful processing of personal information. For each processing activity, before processing personal information or as soon as reasonably possible for existent processes, information curators must identify and document the justification they are relying on and the reason for relying on that justification.

6.2.2 When a third party is involved in the processing of personal information, information curators must ensure that the appropriate agreements must be in place. Such agreements must clearly identify the responsible parties involved, operators involve, privacy-related responsibilities of all parties, and the justification for the processing of personal information.

6.3 Information curators must ensure that personal information processing is kept to the minimum required to meet our goals.

6.3.1 The lawfulness of personal information processing depends on the extent to which the processing may infringe on an individual's right to privacy. Such infringements will be justified if there is no less intrusive way to achieve the goal of the processing.

6.3.2 Information curators must ensure that personal information is only processed when it is adequate to fulfil the purpose of the processing activity.

6.3.3 Information curators must ensure that personal information is only processed when it is relevant to fulfil the purpose of the processing activity.

[3] Personal information may be processed (see section 11 of POPIA for full details):
- to conclude or perform in terms of a contract;
- to comply with an obligation imposed by law;
- to protect a legitimate interest of the data subject;
- to ensure proper performance of a public law duty by a public body;
- to ensure the legitimate interest of the responsible party or of a third party; or
- with the consent of the data subject or a competent person where the data subject is a child.

6.4 Information curators must ensure the confidentiality, quality, and availability of personal information.

6.4.1 Information curators must design, implement, and test controls to prevent the unauthorised disclosure of personal information.

6.4.2. Information curators must design, implement, and test controls to ensure the accuracy and completeness of personal information over its entire lifecycle.

6.4.3 Information curators must design, implement, and test controls to ensure the continuing availability of personal information over its entire lifecycle.

6.5 Information curators must ensure transparency in personal information processing.

6.5.1 Information curators must ensure that individual data subjects are aware of what we do with their personal information, their rights as data subjects, and the options available to them regarding their personal information.

6.6 All University staff, students, members of institutional statutory bodies, and third-party suppliers, must be able to identify and respond to potential information breaches.

6.6.1 All students, staff, members of institutional statutory bodies, third-party suppliers, and vendors have a duty to report potential information breaches.

6.6.2 The regulation owner(s), supported by the regulation curator(s), must ensure the design, implementation, and testing of procedures for the reporting, analysis, investigation, and containment of potential information breaches.

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 or international 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 act, 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 & Vice-Chancellor, as statutory information officer, owns these regulations. They are ultimately accountable for all processing of personal information within Stellenbosch University and thereby accountable for the existence, implementation, monitoring of compliance, and reporting compliance and non-compliance of this regulation to the University's Council and Rectorate. The Rector & Vice-Chancellor may designate deputy information officers as responsible for the execution of the above tasks, in addition to any other relevant tasks or duties as defined by the South African Information Regulator.