UNIVERSITIES SOUTH AFRICA

EU GDPR GUIDELINES FOR SOUTH AFRICAN UNIVERSITIES

TABLE OF CONTENTS

1. THE GUIDELINE IN CONTEXT

Worldwide there is an increased focus on privacy legislation. The privacy laws that are most relevant to South African universities right now, are the European Union[1] General Data Protection Regulation (EU GDPR), and the Protection of Personal Information Act (POPIA).

Universities South Africa (USAf) has launched a project to draft an Industry Code of Conduct for public universities in terms of the POPIA. A Code gives the industry the opportunity to decide on principles to govern the lawful processing of personal information given the features of the industry. The aim of the Code is to help the industry become POPIA compliant. However, the POPIA won't be in effect until the President publishes an effective date, and according to the Information Regulator, the date should be published during the first half of 2018. Universities will have at least one year from that date to become compliant.

The POPIA is based on the new European Union General Data Protection Regulation (the EU GDPR), which comes into force on 25 May 2018 and, as is the case with many data protection laws, its reach will extend far beyond the EU. Therefore, there is an immediate need to assist universities to determine whether they have to comply with the EU GDPR and that is why USAf has commissioned this guideline.

This guideline provides you with the questions you need to answer to determine whether the GDPR applies to your university. There are two possible ways in which the EU GDPR could become relevant for a South African university:

- The EU GDPR could apply directly. If this is the case, the South African university could be fined for non-compliance by the European authorities.
- A European partner organisation may require in a contract that the South African university must comply with the EU GDPR. If this is the case, the European partner can hold the South African university responsible for non-compliance in terms of the contract, but the European authorities will not be able to enforce it directly against the South African university. Hence, we refer to an indirect application.

Both scenarios will be discussed separately.

The status of this guideline
The application of the EU GPDR is very context specific, which is why this document is just a guideline and does not constitute legal advice.

1 The United Kingdom is leaving the EU in March 2019. Whether the EU GDPR will continue to apply in the UK post Brexit is still uncertain. However, the UK government has indicated that it will be adopting the equivalent of the EU GDPR.

2. A STEP BACK: WHAT IS THE POPIA?

The purpose of the POPIA is to:

- give effect to the constitutional right to privacy by safeguarding personal information,
- balance the right to privacy against other rights, such as the right to access to information,
- regulate the way in which personal information must be processed, and
- establish an Information Regulator to ensure that the rights protected by the POPIA are respected and that those rights are promoted and enforced.

The POPIA defines personal information as any information that relates to an identifiable, living individual or an existing business ('juristic person'). This includes the information a university may have of students, staff members, service providers, contractors, suppliers, applicants, and members of the public.

Here are some examples:

Identifiers such as: a name, identity number, student number, staff number, account number, customer number, company registration number, tax number, photos, videos, or any other unique information that can be used to identify a person.

Demographic information such as: race, gender, sex, pregnancy, marital status, national or ethnic or social origin, colour, sexual orientation, age, physical or mental health or wellbeing, disability, religion, conscience, belief, culture, language, and birth.

Contact details such as: physical and postal addresses, email addresses, telephone numbers, online identifiers (e.g. a person's twitter handle), and location information.

Financial information such as: bank and other account numbers, bank statements, salary information, financial statements, applications for financial assistance, and applications for bursaries.

Usernames and passwords.

Background information such as: education, financial, employment, medical, criminal, or credit history.

Biometric information: this refers to techniques of identification that are based on physical, physiological, or behavioural characterisation such as blood typing, fingerprinting, DNA analysis, retinal scanning, and voice recognition.

Someone's **opinions**, **views,** and **preferences**.

Private or confidential correspondence sent by a person and any further correspondence that would reveal the contents of the original correspondence.

Views or opinions about a person (such as interview notes and trade references).

This information can generally be found on computers, phones, in filing cabinets, on forms (application forms, registration forms, procurement forms, HR forms), call centre recordings, CCTV footage, the internet, etc.).

In order to achieve its purpose of protecting personal information and privacy, the POPIA regulates:

- who is responsible for compliance (particularly where multiple organisations are using personal information),
- the way personal information is collected or created,
- what information must be disclosed to a person about how their information is used,
- how personal information is managed (this includes the sharing of information, information quality, and retention and destruction rules),
- information security,
- access to information (internally and externally), and
- sharing personal information across borders.

The purpose of the EU GDPR is very similar to that of the POPIA because the POPIA was based on earlier versions of the EU GDPR. For South African universities this means that where data is shared between Europe and South Africa, both the EU GDPR and the POPIA may apply. The use of 'may' in this context is intentional. Unfortunately, there are some common misconceptions about the application of the EU GDPR. The purpose of this guideline is to assist South African universities to accurately identify instances where the rules of both the EU GDPR and the POPIA are relevant.

3. TYPICAL EXAMPLES OF SA AND EU DATA EXCHANGES

The following scenarios are typical instances in which a South African university comes into contact with data from the EU. We will use these examples throughout the guideline to illustrate how to determine whether the EU GDPR applies.

Example 1: European citizens study at a South African university

There are many European citizens enrolled at South African universities. Some of them may be registered here, others may just be visiting as part of an exchange programme with their home university. There are also European citizens who enrol for online courses and who might never set foot in South Africa.

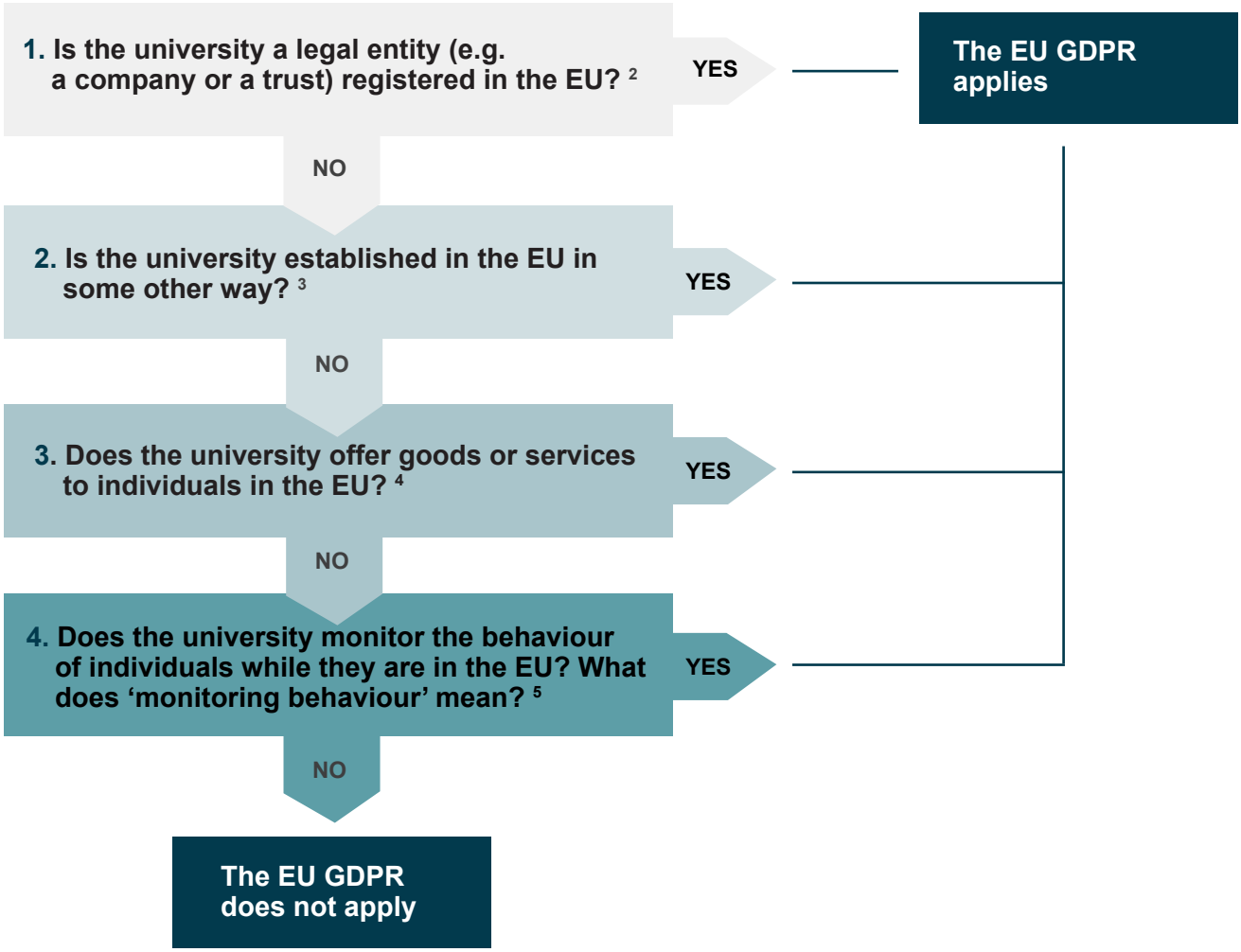
Example 2: The use of research data of European citizens

Universities share research data, and a South African university is given access to data stored in Europe. In some instances a South African university may gather and store research data about Europeans.

When will the EU GDPR apply directly to a South African public university? These four questions will help you determine whether the EU GDPR applies to your university directly. **If you answer yes to any one of the questions, it is likely that the EU GDPR applies.**

Example 3: Alumni who live in Europe

Many Universities have alumni who reside in the EU. Some universities may even have alumni associations that are based in EU countries.



2 Recital 22 and article 3(1) of the EU GDPR. The recital in EU legislation are explanations of the rules contained in the articles.
3 Recital 22 and article 3(1). The recital in EU legislation are explanations of the rules contained in the articles.
4 Many sources incorrectly state that the goods or services must be offered to European residents. This is not correct, because residency is not required. Instead, the question is whether the individual is in the EU when the goods or services are offered.
5 Recital 24 and article 3(2)(b).

1. The GDPR will apply to all data processing undertaken by this legal entity.

2. What does ‘established’ mean?

The test that the European courts have used in the past is very flexible, making it difficult to distil into a checklist. The test is whether the university exercises ‘any real and effective activity’ – through ‘stable arrangements’ in the EU.[6]

Here are some examples from court cases:

- The organisation has a representative in the EU. That representative can be a single individual, an agent, sales office, branch, or subsidiary.
- The organisation has a website in the language of a European country, (other than English).
- The organisation has equipment in Europe.
- The organisation has a European postal address.

3. Many universities offer courses worldwide, but that doesn’t mean that the EU GDPR will apply. Once again, whether or not the EU GDPR applies will be determined on a case by case basis. The mere fact that courses can be accessed in the EU is not enough.

If it does not, the question is whether that university foresees that its activities will reach individuals in the EU. Factors typically considered are whether these services are offered in an EU language (other than English), whether payment can be made in an EU currency, or whether the university mentions customers located in the EU in its publications.

4. It includes tracking individuals in the EU on the internet or elsewhere to create a profile of them, or to analyse their preferences, behaviour, and attitudes. In data protection circles this kind of activity is referred to as ‘profiling’. Profiling takes place when a university uses automated processes (technology in other words) to analyse personal data to learn about, and predict, an individual’s performance at work, financial status, health, personal preferences, interests, reliability, behaviour, location, and movement.

6 Wletimmo v NAIH (-230/140)

Let's apply these questions to our examples:

Example 1: Europeans study at a South African university.

Unless a South African university also has a campus in the EU or is established there in some other way through a typically long term or permanent 'stable relationship' (questions 1 and 2), simply having European students will not trigger the application of the EU GDPR unless Europeans are being specifically targeted (question 3).
Even e-learning courses are often not targeted at a specific population group.

In cases were a South African university has an exchange programme with an European organisation, the EU GDPR will not apply as the services provided to the student by the South African university are not being delivered in the EU.

Example 2: The use of research data of European citizens.

Here too, you must answer the first three questions, but even if they indicate that the EU GDPR does not apply, the enquiry should be taken further. It may be that, for research purposes, a South African university is specifically monitoring individuals while they are in the EU – an activity to which the rules of the
EU GDPR apply.[7]

Example 3: Alumni who live in Europe.

If the university is represented by an alumni association in Europe, who assists the university by keeping in contact with the alumni in that country, the EU GDPR applies directly to the association because they are established in the EU (question 1). The EU GDPR may also apply to the SA University if there is a 'stable arrangement' between the association and the university (question 2). If the university is not represented by an alumni association and is just gathering the information from alumni while they are in Europe questions 3 and 4 must be applied. This means that if the university is offering goods or services in the EU to those alumni or if the university is tracking the alumni while they are in the EU then the EU GDPR will apply.

7 Recital 23 and article 3(2)(a).

4. THE EU GDPR APPLIES, BUT TO WHAT EXTENT?

This discussion is limited

A full discussion of the application of the EU GDPR is outside the scope of this guideline. The intention is to provide South African universities with some guidance regarding what is required of universities that are primarily based outside of the EU.

4.1 The application of the EU GDPR may be limited

The extent to which the EU GDPR applies to a South African university depends on how the EU GDPR was triggered.

Reason why the GDPR was triggered	The extent to which the GDPR applies
The South African university has a legal entity registered in the EU or is otherwise established there. (Questions 1 and 2)	The EU GDPR will apply to all of the processing activities undertaken in the context of the activities of that establishment.
The South African university is specifically targeting individuals in the EU (e.g. for distance learning). (Question 3)	The EU GDPR will apply to the relevant processing activities. **NB:** The EU GDPR will only apply to the processing done in order to deliver the service to the individuals in the EU, not to all of the processing activities of the South African university.
The South African university monitors the behaviour of individuals while they are in the EU. (Question 4)	The EU GDPR will apply to the relevant monitoring activities. **NB:** The EU GDPR will only apply to the monitoring of individuals while they are in the EU, and not to all monitoring or researching activities.

It is crucial that South African universities establish exactly which processing activities are subject to the EU GDPR. In many, if not most, cases the EU GDPR will only apply to specific processing activities.

4.2 The EU GDPR and the POPIA are similar

If a South African university finds itself in a position where it has to comply with the EU GDPR, the cost of running separate POPIA and EU GDPR programmes could be significant. Due to the considerable similarities between the two legislative regimes, it is advisable to take an integrated approach. POPIA compliance should always advance EU GDPR compliance and vice versa[8].

8 While the overarching approach as well as the substance of the two pieces of legislation is similar, they are not identical. In such instances, the principle which best protects a data subject's privacy should be adopted.

A comparison of the United Kingdom Information Commissioner's Office's (ICO) 12-step approach to the EU GDPR with the POPIA illustrates this principle:

ICO's recommended step	Does the POPIA require it too?
Awareness Universities must ensure that decision makers and key people know that the law is changing.	Yes. It is a requirement in terms of the draft POPIA Regulations that the university must ensure that employees and student employees receive POPIA training.
Know your information Document what personal data the university holds, where it came from, and who you share it with. In other words, universities should do a personal data audit.	Yes. The POPIA requires that all processing of personal information must be documented. More importantly, it is impossible to do a POPIA compliance programme without knowing what personal information the university has and what it does with it.
Privacy notices Universities should review their current privacy notices and ensure that they make the necessary changes in time for GDPR implementation. The European Commission has published draft guidelines on transparency. At a minimum the information must be easily accessible and easy to understand. Crucially, the Commission has affirmed an established principle of plain language drafting. Universities must identify the intended audience, assess the average member of that audience's level of understanding, and continuously check that the information is tailored to the needs of the actual audience.	Yes. The POPIA places extensive notification obligations on universities. The key principle is that people should not be surprised by what their personal information is used for. A privacy notice is also known as a privacy policy which is usually hidden behind a URL in the footer of a website. It needs to come out of hiding. Using plain language when you talk about privacy and personal information is key if you want to win trust.
Individuals' rights Universities must ensure that their procedures cover all the rights individuals have, including when and how to: ☐ give people access to personal data ☐ change or correct personal data ☐ delete personal data	Yes. The POPIA also requires that people have the right to access, change or correct, and delete their personal information unless one of the exceptions applies.
Access requests Universities should update their procedures and plans for when people request access to their personal data. This is necessary, because the GDPR will change the timeframes within which access has to be granted.	Yes. The POPIA interacts with an existing piece of legislation, the Promotion of Access to Information Act (PAIA). It has not changed PAIA much, but the Information Regulator will now be tasked with enforcing it. Universities also need to dust off their PAIA manuals and review them to determine whether they comply with the POPIA. The POPIA and PAIA do not prescribe a specific timeframe within which access has to be granted. It must just be reasonable.
Legal processing Universities must identify the purposes for which data are used and whether they can justify those purposes (justifications are listed in the GDPR). These purposes must be documented and explained in the university's privacy notice.	Yes. The POPIA contains a virtually identical requirement. The most common justifications are that personal information must be processed to fulfil a contractual obligation or where other legislation requires the university to process personal information to comply.

Consent Universities should review how they seek, record, and manage consent and whether any changes need to be made. Valid consent in terms of the GDPR must be: • freely given, • specific, • informed, • unambiguous, and • given by a statement or a clear affirmative action[9]. The European Commission has published draft guidelines on consent. Here are some of the highlights: • People must be given a real choice and control. Consents cannot be asked on a 'take it or leave it' basis. If the person cannot refuse or withdraw the consent without a negative effect, it is not freely given. • In many cases public authorities will probably not be able to rely on consent, because there will often be a clear imbalance of power. This imbalance also occurs in the employment context. Employers must find other ways to justify their activities (in most instances it will be authorised by labour legislation). • It is problematic to exchange free services for consent to use personal data for a non-essential purpose such as behavioural advertising. In other words, consent should not be used as a *quid pro quo* for additional services. • If consent is asked for more than one purpose, people should be free to agree to some, but not others. The consents must not be bundled into one, it must be granular.	Consent also features strongly in the POPIA. In many instances, universities will be able to comply with the principles of POPIA by obtaining consent from data subjects. For instance, in principle, personal data must be collected directly from the individual unless they have given the university consent to collect it from somewhere else. Virtually every principle in the POPIA is qualified in this fashion. The important question will be when consent will be considered valid. In the POPIA consent is defined as 'any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information'. It is similar to the GDPR which means that we can be guided by how the requirements for valid consent have been interpreted in the EU. **The myth of consent** Universities are often advised that they need consent to process personal information. That is 100% untrue and also bad practice, because those consents are asked on a take-it-or-leave-it basis. If the person says no, they cannot have the product or access the service. This consent is questionable from a legal point of view. The European Commission has stated that 'if consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given.' In any event, research has shown that this kind of 'consent' infuriates people and erodes their trust in the university. Most processing activities are justified because they are required to fulfil a contract (e.g. sending exam results) or legislation (e.g. collecting information about a person's race in terms of the Employment Equity Act). There are other justifications too. Consent should only be obtained as a last resort.
Children Universities must consider whether they need to put a system in place to verify individuals' ages and to obtain parental or guardian consent for processing activities involving child data. A child is anybody under the age of 14.	Yes. The POPIA also contains very specific requirements for the processing of child personal information, but the relevant age in South Africa will be 18. Around 90% of the time, the POPIA requires parental or guardian consent.
Data breaches Universities must make sure that they have the right procedures in place to detect, report, and investigate personal data breaches.	Yes. The POPIA requires breach monitoring and response policies and procedures. Not having this in place has sunk many a business.

9 Both POPIA and the EU GDPR has special provisions on consent for scientific research which allow for 'broad consent' as defined in the Department of Health's Ethics in Health Research: Principles, processes and structures. Both POPIA and the EU GDPR has special provisions on consent for scientific research which allow for 'broad consent' as defined in the Department of Health's Ethics in Health Research: Principles, processes and structures.

Data protection by design and privacy impact assessments Universities should think about how to ensure that all current processing activities and future (new) processing activities go through a privacy impact assessment. The ICO has a terrific code of practice on privacy impact assessments and the latest guidance from EU authorities.	Yes, but not in so many words. The POPIA requires that all processing activities should be assessed, but privacy by design or privacy impact assessments are not mentioned in so many words. It is impossible to ensure lasting POPIA compliance without them, but privacy impact assessments can be complex and it requires experience to accurately gauge the level of risk a particular activity poses to the university.
Data protection officers Universities should designate someone to take responsibility.	Yes. The POPIA provides that the heads of private organisations are automatically the Information Officer of the organisation. Of course, the Vice-Chancellor cannot actually do the work, so the POPIA also allows for the designation of Deputy Information Officers. Universities need Deputy Information Officers and privacy officials (sometimes called privacy stewards or champions) in each business area. Experience has shown that, if POPIA compliance does not end up in a number of people's job descriptions, POPIA compliance will not happen.
International If the university operates in more than one EU member state, it should determine the lead data protection supervisory authority.	The POPIA does not contain an equivalent provision, because the Act only applies to South Africa. It does contain provisions on the cross-border transfer of personal information. The bottom line is that the level of protection has to remain at the POPIA levels even when the information is sent somewhere else. This will be the case if the country has adequate data protection legislation or if an agreement or binding rules to ensure compliance has been put in place.

5. WHAT IF THE EU GDPR IS MADE APPLICABLE BY MEANS OF A CONTRACT WITH A EUROPEAN ORGANISATION?

Even if the EU GDPR does not apply to the South African university directly, it does not mean that the EU GDPR will not affect it at all. If the university has relationships with organisations in the EU, the EU GDPR will have an influence on that university.

If a South African university has agreements or relationships with EU based organisations and this involves the university receiving information of persons located in the EU, the transfer of that information will be subject to the EU GDPR. EU based organisations may only send personal data of persons located in the EU to non-EU organisations[10] if:

1. they are based in a jurisdiction which is deemed to provide adequate levels of data protection;[11] or
2. if appropriate safeguards are put in place between the organisation sending and the one receiving the information (e.g. a data protection contract based on prescribed model clauses or binding corporate rules);[12] or
3. one of the exceptions applies.

10 Recitals 108 and 110 and article 47(1) to (3) of the EU GDPR deals with binding corporate rules.
11 Recital 106 to 107, articles 45(3) to (5) and 93(2) to (3) of the EU GDPR. Currently they are: Andorra, Argentina, Canada (for organisations that are subject to Canada's PIPEDA law), Switzerland, the Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay, and the US (for organisations that are certified to the EU-US Privacy Shield).
12 Recital 59 to 60 and articles 26(2) to (4) and 31(2) of the Directive and recitals 81 and 180 to 109 and articles 28(6) to (8), 46(2)(c), 57(1)(j), 57(1)(r) and 93(2) of the EU GDPR deals with model clauses.

The exemptions to provide adequate levels of data protection are:

1. If the data subject explicitly consents to the transfer to South Africa despite being informed that their data may not be protected.[13]
2. If the transfer is necessary for the performance of a contract between the data subject and the EU-based organisation, or for the implementation of pre-contractual measures taken at the data subject's request.
3. If the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the EU-based organisation and another natural or legal person.
4. The transfer is necessary for important reasons of public interest.
5. The transfer is necessary for the establishment, exercise, or defence of legal claims (e.g. the EU data is required in an active court case).
6. The transfer is necessary to protect the vital interests of the data subject or of other persons (this is limited to actual life or death situations, e.g. there is a medical emergency).
7. The transfer is made from a register which is open to the public or available upon request (this does not justify the transfer of the entire register).
8. There are compelling legitimate interests.

For these exceptions to apply, the transfer of the data to South Africa must be necessary for the purpose on which the exception is based and it must only happen occasionally. If the data transfer takes place regularly, it is often an indication that there is a stable relationship between the EU organisation and the South African university which means that the exceptions do not apply.

Until the POPIA comes into force, South Africa will not be deemed to have adequate levels of protection. This means that South African universities will have to establish whether one of the exemptions apply or they must sign an agreement in which they undertake to apply the EU GDPR to the data transferred by the EU-based organisation.

It will always be better for a South African university to argue that one of the exemptions apply than to sign a contract in which it undertakes to comply with the EU GDPR. However, because the exemptions are difficult to apply, the EU-based organisation will in most instances require that the South African university sign a data protection agreement. The European Commission has approved a set of model clauses[14] that EU organisations must use.

13 See the Article 29 Data Protection Working Party *Guidelines on Consent under Regulation 2016/679*.

14 https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en
The current model clauses were drafted based on and approved under Directive 95/46/EC (the legislation that the GDPR will be replacing on 25 May 2018). It is expected that the Commission will update or replace the existing model clauses. The impact of these updates remains to be seen.

The SA university:

1. may only process personal data on the EU organisation's instructions
2. must implement the technical and organisational security measures specified by the EU organisation
3. will promptly notify the EU organisation about
    - any legally binding request for disclosure of personal data by law enforcement authorities unless otherwise prohibited;
    - an accidental or unauthorised access (data breach); and
    - any request received directly from the data subject without responding to that request
4. may not engage with a subcontractor without prior written consent from the EU organisation
    - where the SA university engages a subcontractor to carry out processing for the Data Exporter, the same contract which is applicable to the Data Importer and the Data Exporter will apply to the subcontractor; and
    - the SA university may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
5. must delete or return all personal information to the EU organisation at the end of the service contract
6. must at the request of the EU organisation submit its data-processing facilities for an audit of the data processing activities covered by the contract

What should a SA university do before signing such an agreement?

- Investigate whether one of the exemptions applies. If this is the case, try to convince the EU organisation that the data protection agreement is not necessary.
- Identify exactly which processing activities are affected by the data protection agreement. Never sign an agreement which requires that all processing activities must be EU GDPR compliant. It is not a requirement.
- Ask the EU organisation to specify exactly which 'technical and organisational security measures' are required.
- Specify instances where it will not be possible to delete or return personal information at the end of the agreement. Remember that South African laws may require that you retain records.

6. NEED ASSISTANCE?

If you require assistance, please contact Ms Jana van Wyk by email: jana@usaf.ac.za.

Universities South Africa (USAf) is an association of South Africa's public universities. The organisation's primary mandate is to support its 26 members in achievement of their core functions of teaching and learning, research and community engagement, and to contribute to creating an environment where universities can thrive and prosper, and contribute to South Africa's development.