KEU Underwriting Managers Protection of Personal Information Act Policy

Foreword

In the information we offer customers the means to be always connected. This requires data to be collected and processed. When storing and transmitting data, we must ensure a high level of Protection of Personal Information and data security. That goes for information pertaining to our customers, prospects, business partners and employees. Because Protection of Personal Information is people protection.

Our top priority is to ensure universally applicable standards for handling personal data. For us, protecting the personal rights and privacy of each and every individual is the foundation of trust in our business relationships.

The policy sets an applicable Protection of Personal Information and security standard for our company. We have established seven Protection of Personal Information principles – among them transparency, data economy and data security – as our guideline.

Our managers and employees are obligated to adhere to the Corporate Protection of Personal Information Policy and observe their local Protection of Personal Information laws. As the Information Officer for Protection of Personal Information, it is my duty to ensure that the rules and principles of Protection of Personal Information at KEU are followed around the world.

Contents

I. Aim of the Protection of Personal Information Policy

II. Scope and amendment of the Protection of Personal Information Policy

III. Application of national laws

IV. Principles for processing personal data

1. Fairness and lawfulness
2. Restriction to a specific purpose
3. Transparency
4. Data reduction and data economy
5. Deletion
6. Factual accuracy; up-to-date data
7. Confidentiality and data security

V. Reliability of data processing

1. Customer and partner data
    - 1.1 Data processing for a contractual relationship
    - 1.2 Data processing for advertising purposes
    - 1.3 Consent to data processing
    - 1.4 Data processing pursuant to legal authorization
    - 1.5 Data processing pursuant to legitimate interest
    - 1.6 Processing of special personal information
    - 1.7 Automated individual decisions
    - 1.8 User data and internet

2. Employee data

    - 2.1 Data processing for the employment relationship
    - 2.2 Data processing pursuant to legal authorization
    - 2.3 Collective agreements on data processing
    - 2.4 Consent to data processing
    - 2.5 Data processing pursuant to legitimate interest
    - 2.6 Processing of special personal information
    - 2.7 Automated decisions
    - 2.8 Telecommunications and internet

Contents continued

VI. Transmission of personal data

VII. Contract data processing

VIII. Rights of the data subject

IX. Confidentiality of processing

X. Processing security

XI. Protection of Personal Information control

XII. Protection of Personal Information incidents

XIII. Responsibilities and sanctions

XIV. Chief Officer of Corporate Protection of Personal Information

XV. Definitions

I. Aim of the Protection of Personal Information Policy

As part of its social responsibility, KEU is committed to compliance with the Protection of Personal Information Act and Regulations. This Protection of Personal Information Policy applies to KEU and is based on globally accepted, basic principles on Protection of Personal Information. Ensuring Protection of Personal Information is the foundation of trustworthy business relationships and the reputation of KEU as an attractive employer.

The Protection of Personal Information Policy provides one of the necessary framework conditions for cross-border data transmission. It ensures the adequate level of Protection of Personal Information prescribed by the Protection of Personal Information Act (and Regulations) and the national laws for cross-border data transmission, including in countries that do not yet have adequate Protection of Personal Information laws.

II. Scope and amendment of the Protection of Personal Information Policy

This Protection of Personal Information Policy applies to KEU.

The Protection of Personal Information Policy extends to all processing of personal data. In countries where the data of legal entities is protected to the same extent as personal data, this Protection of Personal Information Policy applies equally to data of Juristic entities. De-identified data, e.g. for statistical evaluations or studies, is not subject to this Protection of Personal Information Policy.

This Protection of Personal Information Policy can be amended in coordination with the Information Officer for the Protection of Personal Information under the defined procedure for amending policies. The amendments will be reported immediately to KEU using the process for amending policies. Amendments that have a major impact on compliance with the Protection of Personal Information Policy must be reported annually to the Protection of Personal Information authorities that issue approval for this Protection of Personal Information Policy as Binding Corporate Rules.

The latest version of the Protection of Personal Information Policy can be accessed with the data privacy information at KEU 's website: www.keu.co.za.

III. Application of national laws

This Protection of Personal Information Policy comprises the internationally accepted data privacy principles without replacing the existing national laws. It supplements the national data privacy laws.

The relevant national law will take precedence in the event that it conflicts with this Protection of Personal Information Policy, or it has stricter requirements than this Policy. The content of this Protection of Personal Information Policy must also be observed in the absence of corresponding national legislation. The reporting requirements for data processing under national laws must be observed.

KEU is responsible for compliance with this Protection of Personal Information Policy and the legal obligations. If there is reason to believe that legal obligations contradict the duties under this Protection of Personal Information Policy, the relevant person must inform the Information Officer for the Protection of Personal Information. In the event of conflicts between national legislation and the Protection of Personal Information Policy, KEU will work with the relevant person to find a practical solution that meets the purpose of the Protection of Personal Information Policy.

IV. Principles for processing personal data

1. Fairness and lawfulness

When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner.

2. Restriction to a specific purpose

Personal data can be processed only for the purpose that was defined before the data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation.

3. Transparency

The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be aware of, or informed of:

» The identity of the Responsible Party
» The purpose of data processing
» Third parties or categories of third parties to whom the data might be transmitted

IV. Principles for processing personal data continued

4. Data limitation and data economy

Before processing personal data, you must determine whether and to what extent the processing of Personal data is necessary in order to achieve the purpose for which it is undertaken. Where the purpose allows and where the expense involved is in proportion with the goal being pursued, de-identified / anonymized or statistical data must be used. Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by national law.

5. Deletion

Personal data that is no longer needed after the expiration of legal or business process-related periods must be deleted. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.

6. Factual accuracy; up-to-dateness of data

Personal data on file must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

7. Confidentiality and data security

Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organisational and technical measures to prevent unauthorised access, illegal processing or distribution, as well as accidental loss, modification or destruction.

V. Reliability of data processing

Collecting, processing and using personal data is permitted only under the following legal bases. One of these legal bases is also required if the purpose of collecting, processing and using the personal data is to be changed from the original purpose.

1. Customer and partner data

1.1 Data processing for a contractual relationship

Personal data of the relevant prospects, customers and partners can be processed in order to establish, execute and terminate a contract. This also includes advisory services for the partner under the contract if this is related to the contractual purpose. Prior to a contract – during the contract initiation phase – personal data can be processed to prepare bids or purchase orders or to fulfill other requests of the prospect that relate to contract conclusion. Prospects can be contacted during the contract preparation process using the information that they have provided. Any restrictions requested by the prospects must be complied with. For advertising measures beyond that, you must observe the following requirements under 1.2.

1.2 Data processing for advertising purposes

If the data subject contacts KEU to request information (e.g. request to receive information material about a product), data processing to meet this request is permitted. Customer loyalty or advertising measures are subject to further legal requirements. Personal data can be processed for advertising purposes or market and opinion research, provided that this is consistent with the purpose for which the data was originally collected. The data subject must be informed about the use of his/her data for advertising purposes. If data is collected only for advertising purposes, the disclosure from the data subject is voluntary. The data subject shall be informed that providing data for this purpose is voluntary. When communicating with the data subject, consent shall be obtained from him/her to process the data for advertising purposes. When giving consent, the data subject should be given a choice among available forms of contact such as regular mail, e-mail and phone (Consent, see 1.3).

If the data subject refuses the use of his/her data for advertising purposes, it can no longer be used for these purposes and must be blocked from use for these purposes. Any other restrictions from specific countries regarding the use of data for advertising purposes must be observed.

1.3 Consent to data processing

Data can be processed following consent by the data subject. Before giving consent, the data subject must be informed in accordance with IV.3. of this Protection of Personal Information Policy. The declaration of consent must be obtained in writing or electronically for the purposes of documentation.

In some circumstances, such as telephone conversations, consent can be given verbally. The granting of consent must be documented.

V. Reliability of data processing continued

1.4 Data processing pursuant to legal authorization

The processing of personal data is also permitted if national legislation requests, requires or allows this. The type and extent of data processing must be necessary for the legally authorised data processing activity, and must comply with the relevant statutory provisions.

1.5 Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary for a legitimate interest of KEU. Legitimate interests are generally of a legal (e.g. collection of outstanding receivables) or commercial nature (e.g. avoiding breaches of contract). Personal data may not be processed for the purposes of a legitimate interest if, in individual cases, there is evidence that the interests of the data subject merit protection, and that this takes precedence. Before data is processed, it is necessary to determine whether there are interests that merit protection.

1.6 Processing of highly sensitive data (special personal information)

Highly sensitive personal data can be processed only if the law requires this or the data subject has given express consent. This data can also be processed if it is mandatory for asserting, exercising or defending legal claims regarding the data subject. If there are plans to process highly sensitive data, the Information Officer must be informed in advance.

1.7 Automated individual decisions

Automated processing of personal data that is used to evaluate certain aspects (e.g. creditworthiness) cannot be the sole basis for decisions that have negative legal consequences or could significantly impair the data subject. The data subject must be informed of the facts and results of automated individual decisions and the possibility to respond. To avoid erroneous decisions, a test and plausibility check must be made by an employee.

1.8 User data and internet

If personal data is collected, processed and used on websites or in apps, the data subjects must be informed of this in a privacy statement and, if applicable, information about cookies. The privacy statement and any cookie information must be integrated so that it is easy to identify, directly accessible and consistently available for the data subjects.

V. Reliability of data processing continued

If use profiles (tracking) are created to evaluate the use of websites and apps, the data subjects must always be informed accordingly in the privacy statement. Personal tracking may only be effected if it is permitted under national law or upon consent of the data subject. If tracking uses a pseudonym, the data subject should be given the chance to opt out in the privacy statement. If websites or apps can access personal data in an area restricted to registered users, the identification and authentication of the data subject must offer sufficient protection during access.

2. Employee data

2.1 Data processing for the employment relationship

In employment relationships, personal data can be processed if needed to initiate, carry out and terminate the employment agreement. When initiating an employment relationship, the applicants' personal data can be processed. If the candidate is rejected, his/her data must be deleted in observance of the required retention period, unless the applicant has agreed to remain on file for a future selection process. Consent is also needed to use the data for further application processes or before sharing the application.

In the existing employment relationship, data processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorised data processing apply.

If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding (national) laws have to be observed. In cases of doubt, consent must be obtained from the data subject.

There must be legal authorisation to process personal data that is related to the employment relationship but was not originally part of performance of the employment agreement. This can include legal requirements, collective regulations with employee representatives, consent of the employee, or the legitimate interest of the company.

2.2 Data processing pursuant to legal authorisation

The processing of personal employee data is also permitted if national legislation requests, requires or authorises this. The type and extent of data processing must be necessary for the legally authorised data processing activity, and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the employee that merit protection must be taken into consideration.

V. Reliability of data processing continued

2.3 Collective agreements on data processing

If a data processing activity exceeds the purposes of fulfilling a contract, it may be permissible if authorised through a collective agreement. Collective agreements are pay scale agreements or agreements between employers and employee representatives, within the scope allowed under the relevant employment law. The agreements must cover the specific purpose of the intended data processing activity, and must be drawn up within the parameters of Protection of Personal Information legislation.

2.4 Consent to data processing

Employee data can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily. Involuntary consent is void. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In certain circumstances, consent may be given verbally, in which case it must be properly documented. In the event of informed, voluntary provision of data by the relevant party, consent can be assumed if national laws do not require express consent. Before giving consent, the data subject must be informed in accordance with IV.3. of this Protection of Personal Information Policy.

2.5 Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary to enforce a legitimate interest of KEU. Legitimate interests are generally of a legal (e.g. filing, enforcing or defending against legal claims) or financial (e.g. valuation of companies) nature.

Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the employee merit protection. Before data is processed, it must be determined whether there are interests that merit protection.

Control measures that require processing of employee data can be taken only if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The justified interests of the company in performing the control measure (e.g. compliance with legal provisions and internal company rules) must be weighed against any interests meriting protection that the employee affected by the measure may have in its exclusion, and cannot be performed unless appropriate.

The legitimate interest of the company and any interests of the employee meriting protection must be identified and documented before any measures are taken. Moreover, any additional requirements under national law (e.g. rights of co-determination for the employee representatives and information rights of the data subjects) must be taken into account.

V. Reliability of data processing continued

2.6 Processing of special personal information

Special personal information can be processed only under certain conditions. Special personal information is data about racial and ethnic origin, political beliefs, religious or philosophical beliefs, union membership, and the health and sexual life of the data subject. Under national law, further data categories can be considered highly sensitive or the content of the data categories can be filled out differently. Moreover, data that relates to a crime can often be processed only under special requirements under national law.

The processing must be expressly permitted or prescribed under national law. Additionally, processing can be permitted if it is necessary for the responsible authority to fulfill its rights and duties in the area of employment law. The employee can also expressly consent to processing. If there are plans to process special personal information, the Information Officer must be informed in advance.

2.7 Automated decisions

If personal data is processed automatically as part of the employment relationship, and specific personal details are evaluated (e.g. as part of personnel selection or the evaluation of skills profiles), this automatic processing cannot be the sole basis for decisions that would have negative consequences or significant problems for the affected employee. To avoid erroneous decisions, the automated process must ensure that a natural person evaluates the content of the situation, and that this evaluation is the basis for the decision. The data subject must also be informed of the facts and results of automated individual decisions and the possibility to respond.

2.8 Telecommunications and internet

Telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by the company primarily for work-related assignments. They are a tool and a company resource. They can be used within the applicable legal regulations and internal company policies. In the event of authorised use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed if applicable.

There will be no general monitoring of telephone and e-mail communications or intranet/internet use. To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to the KEU network that block technically harmful content or that analyse the attack patterns. For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be logged for a temporary period. Evaluations of this data from a specific person can be made only in a concrete, justified case of suspected violations of laws or policies of KEU. The evaluations can be conducted only by investigating departments while ensuring that the principle of proportionality is met.

VI. Transmission of personal data

Transmission of personal data to recipients outside or inside KEU is subject to the authorisation requirements for processing personal data under Section V. The data recipient must be required to use the data only for the defined purposes.

In the event that data is transmitted to a recipient outside KEU to a third country, this country must agree to maintain a Protection of Personal Information level equivalent to this Protection of Personal Information Policy. This does not apply if transmission is based on a legal obligation.

VII. Contract data processing

Data processing on "Behalf" means that a provider is hired to process personal data, without being assigned responsibility for the related business process. In these cases, an agreement on Data Processing on "Behalf" must be concluded with external providers. The client retains full responsibility for correct performance of data processing. The provider can process personal data only as per the instructions from the client. When issuing the order, the following requirements must be complied with; the department placing the order must ensure that they are met.

1. The provider must be chosen based on its ability to cover the required technical and organisational protective measures.

2. The order must be placed in writing. The instructions on data processing and the responsibilities of the client and provider must be documented.

3. The contractual standards for Protection of Personal Information provided by the Information Officer must be considered.

4. Before data processing begins, the client must be confident that the provider will comply with the duties. A provider can document its compliance with data security requirements in particular by presenting suitable certification. Depending on the risk of data processing, the reviews must be repeated on a regular basis during the term of the contract.

5. In the event of cross-border contract data processing, the relevant national requirements for disclosing personal data abroad must be met. In particular, personal data from South Africa can be processed in a third country only if the provider can prove that it has a Protection of Personal Information standard equivalent to this Protection of Personal Information Policy. Suitable tools can be:

   a. Agreement on EU standard contract clauses for contract data processing in third countries with the provider and any subcontractors.

   b. Participation of the provider in a certification system accredited by the EU for the provision of a sufficient Protection of Personal Information level.

VII. Contract data processing continued

c. Acknowledgment of binding corporate rules of the provider to create a suitable level of Protection of Personal Information by the responsible supervisory authorities for Protection of Personal Information.

VIII. Rights of the data subject

Every data subject has the following rights. Their assertion is to be handled immediately by the responsible unit and cannot pose any disadvantage to the data subject.

1. The data subject may request information on which personal data relating to him/her has been stored, how the data was collected, and for what purpose. If there are further rights to view the employer's documents (e.g. personnel file) for the employment relationship under the relevant employment laws, these will remain unaffected.

2. If personal data is transmitted to third parties, information must be given about the identity of the recipient or the categories of recipients.

3. If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented.

4. The data subject can object to the processing of his or her data for purposes of advertising or market/opinion research. The data must be blocked from these types of use.

5. The data subject may request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.

6. The data subject generally has a right to object to his/her data being processed, and this must be taken into account if the protection of his/her interests takes precedence over the interest of the responsible party owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.

   Additionally, every data subject can assert the rights under III. Para. 2, IV., V., VI., IX., X and XIV Para. 3 as a third-party beneficiary if a company that has agreed to comply with the Data Protection Policy does not observe the requirements and violates the party's rights.

IX. Confidentiality of processing

Personal data is subject to data secrecy. Any unauthorised collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorised to carry out as part of his/her legitimate duties is unauthorised. The “need to know” principle applies. Employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities.

Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorised persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.

X. Processing security

Personal data must be safeguarded from unauthorised access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical and organisational measures to protect personal data must be defined and implemented. These measures must be based on the state of the art, the risks of processing, and the need to protect the data (determined by the process for information classification).

In particular, the responsible department can consult with its Information Security Officer (ISO) and Protection of Personal Information coordinator. The technical and organisational measures for protecting personal data are part of Corporate Information Security management and must be adjusted continuously to the technical developments and organisational changes.

XI. Protection of Personal Information control

Compliance with the Protection of Personal Information Policy and the applicable Protection of Personal Information laws is checked regularly with Protection of Personal Information audits and other controls. The performance of these controls is the responsibility of the Information Officer, the Protection of Personal Information coordinators, and other company units with audit rights or external auditors hired. The results of the data protection controls must be reported to the Information Officer. KEU’s management must be informed of the primary results as part of the related reporting duties. On request, the results of Protection of Personal Information controls will be made available to the responsible Protection of Personal Information authority. The responsible Protection of Personal Information authority can perform its own controls of compliance with the regulations of this Policy, as permitted under national law.

XII. Protection of Personal Information incidents

All employees must inform their supervisor, Protection of Personal Information coordinator or the Information Officer immediately about cases of violations against this Protection of Personal Information Policy or other regulations on the protection of personal data.

The manner responsible for the function or the unit is required to inform the responsible data protection coordinator or the Information Officer immediately about data protection incidents.

In cases of

- » improper transmission of personal data to third parties,
- » improper access by third parties to personal data, or
- » loss of personal data the required company reports must be made immediately so that any reporting duties under national law can be complied with.

XIII. Responsibilities and sanctions

Management staff are responsible for ensuring that organisational, HR, and technical measures are in place so that any data processing is carried out in accordance with Protection of Personal Information.

Compliance with these requirements is the responsibility of the relevant employees. If official agencies perform Protection of Personal Information controls, the Information must be informed immediately.

The relevant executive bodies must inform the Information Officer as to the name of their Protection of Personal Information coordinator. Organisationally speaking, in agreement with the Information Officer, this task can be performed by a Protection of Personal Information coordinator for multiple companies or plants. The Protection of Personal Information coordinators are the contact persons on site for Protection of Personal Information. They can perform checks and must familiarise the employees with the content of the Protection of Personal Information policies. The relevant management is required to assist the Information Officer and the Protection of Personal Information coordinators with their efforts.

The departments responsible for business processes and projects must inform the Protection of Personal Information coordinators in good time about new processing of personal data. For data processing plans that may pose special risks to the individual rights of the data subjects, the Information Officer must be informed before processing begins. This applies in particular to extremely sensitive personal information / data. The managers must ensure that their employees are sufficiently trained in Protection of Personal Information.

Improper processing of personal data, or other violations of the Protection of Personal Information laws, can be criminally prosecuted in many countries and result in claims for compensation of damages. Violations for which individual employees are responsible can lead to sanctions under employment law.

XIV. Information Officer

The Information Officer, being internally independent of professional orders, works towards the compliance with national and international Protection of Personal Information regulations. He / she is responsible for the Protection of Personal Information Policy, and supervises its compliance. The Information Officer is appointed by the Management of KEU.

The Protection of Personal Information coordinators shall promptly inform the Information Officer of any Protection of Personal Information risks.

Any data subject may approach the Information, or the relevant Protection of Personal Information coordinator, at any time to raise concerns, ask questions, request information or make complaints relating to Protection of Personal Information or data security issues. If requested, concerns and complaints will be handled confidentially.

If the data coordinator in question cannot resolve a complaint or remedy a breach of the Policy for Protection of Personal Information, the Information Officer must be consulted immediately.

Decisions made by the Information Officer to remedy Protection of Personal Information breaches must be upheld by the management of the company in question. Inquiries by supervisory authorities must always be reported to the Information Officer.

Contact details for the Information Officer and staff are as follows:

info@keu.co.za

XV. Definitions

» Data is anonymised if personal identity can never be traced by anyone, or if the personal identity could be recreated only with an unreasonable amount of time, expense and labour.

» Consent is the voluntary, legally binding agreement to data processing.

» Protection of Personal Information incidents are all events where there is justified suspicion that personal data is being illegally captured, collected, modified, copied, transmitted or used. This can pertain to actions by third parties or employees.

» Data subject under this Protection of Personal Information Policy is any natural person or juristic person, whose data can be processed.

» Special personal information / Highly sensitive data is data about racial and ethnic origin, political opinions, religious or philosophical beliefs, union membership or the health and sexual life of the data subject. Under national law, further data categories can be considered highly sensitive or the content of the data categories can be structured differently. Moreover, data that relates to a crime can often be processed only under special requirements under national law.

» Personal data is all information about certain or definable natural or juristic persons. A person is definable for instance if the personal relationship can be determined using a combination of information with even incidental additional knowledge.

» Processing personal data means any process, with or without the use of automated systems, to collect, store, organise, retain, modify, query, use, forward, transmit, disseminate or combine and compare data. This also includes disposing of, deleting and blocking data and data store media.

» Processing personal data is required if the permitted purpose or justified interest could not be achieved without the personal data, or only with exceptionally high expense.

» Responsible party is the legally independent company of KEU, whose business activity initiates the relevant processing measure.

» A sufficient level of Protection of Personal Information in third countries is acknowledged by the Information Regulator if the core of personal privacy, as unanimously defined, is adequately ensured. When making its decision, the Information Regulator accounts for all circumstances that play a role in data transmission or a category of data transmission. This includes the opinions under national law and relevant applicable professional standards and security measures.

» Third countries under the Protection of Personal Information Policy are all nations outside the Republic of South Africa. This does not include countries with a Protection of Personal Information level that is considered sufficient by the Information Regulator.

» Third parties are anyone apart from the data subject and the Responsible party.

» Transmission is all disclosure of protected data by the responsible party to third parties.