THE ERGUIDEONLINE PRIVACY STATEMENT

1. POLICY STATEMENT

Everyone has rights with regard to how their personal information is handled and protected. In order to carry out its business and provide its services, The ERGuide Online (Pty) Ltd (hereafter referred to as ERGuide Online) may collect, store and process personal information about:

- Employees;
- Customers;
- Consumers;
- Service Providers/Suppliers; and;
- Business Contacts.;

ERGuide Online recognises the need to treat this information in an appropriate and lawful manner. ERGuide Online is committed to complying with its obligations in this regard in respect of all personal information it handles and in order to maintain the confidence of ERGuide Online's customers, service providers/suppliers, business contacts and employees.

Protection of Personal Information Act no. 4 of 2013 (POPIA) and regulations (2018) relates to identifiable, living, natural persons and identifiable, existing, juristic persons. The General Data Protection Regulation (GDPR) only relate to European Citizens information (Natural persons). There might also be other privacy legislation that might be applicable if ER GUIDE ONLINE operates in another country.

The types of information that ERGuide Online may be required to handle include details of current, past and prospective employees, service providers/suppliers, customers, consumer information and other business contacts that ER GUIDE ONLINE communicates with. The information includes name, address, email address, date of birth, ID/Passport numbers, phone numbers, private and confidential information and special personal information. In addition, ERGuide Online may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law.

The information which may be held on paper, electronic format or other media and is subject to certain legal safeguards specified in the POPIA and the GDPR of the European Parliament as well as other applicable acts and regulations. POPIA and GDPR imposes restrictions on how ERGuide Online may collect and process the information.

The policy may be amended from time to time. Any breach of this policy will be taken seriously and may result in disciplinary action up to and including dismissal.

2. DEFINITIONS OF TERMS USED IN THIS POLICY

POPIA Definitions

Data Subject for the purpose of this policy includes all living, identifiable natural or juristic persons whom about ERGuide Online holds personal information or special personal information.

Operator means a person who processes personal information for a responsible part in terms of a contract or mandate, without coming under direct authority of that party.

Personal Information means information relating to an identifiable, living, natural or juristic person. Personal information can be factual (ID/Passport numbers, name, addresses, phone numbers, email addresses, etc.) or it can be an opinion (such as a performance appraisal.)

Processing means any operation or activity, 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;
- dissemination 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 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.

Special Personal Information means information about an individual that pertains to racial or ethnic origins, political, religious or philosophical beliefs, health or sexual life, trade union membership or political persuasion, biometric information or criminal behaviour (to the extent that such criminal behaviour relates to the alleged commission by a date subject of an offence or any proceedings in respect of any offense allegedly committed by a data subject. Special Personal Information can only be processed under strict conditions and will usually require the express written consent of the person concerned.

GDPR Definitions

Personal data means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

3. PURPOSE AND SCOPE OF THE POLICY

This policy sets out ERGuide Online the general rules and the important legal conditions that must be satisfied in relation to the collecting, obtaining, handling, processing, storage, transportation and destruction of identifiable personal and special personal information.

It also describes the Privacy Compliance Framework and Information Governance in more detail.

All employees of ERGuide Online are bound by this policy.

4. PRIVACY COMPLIANCE FRAMEWORK

4.1 BACKGROUND

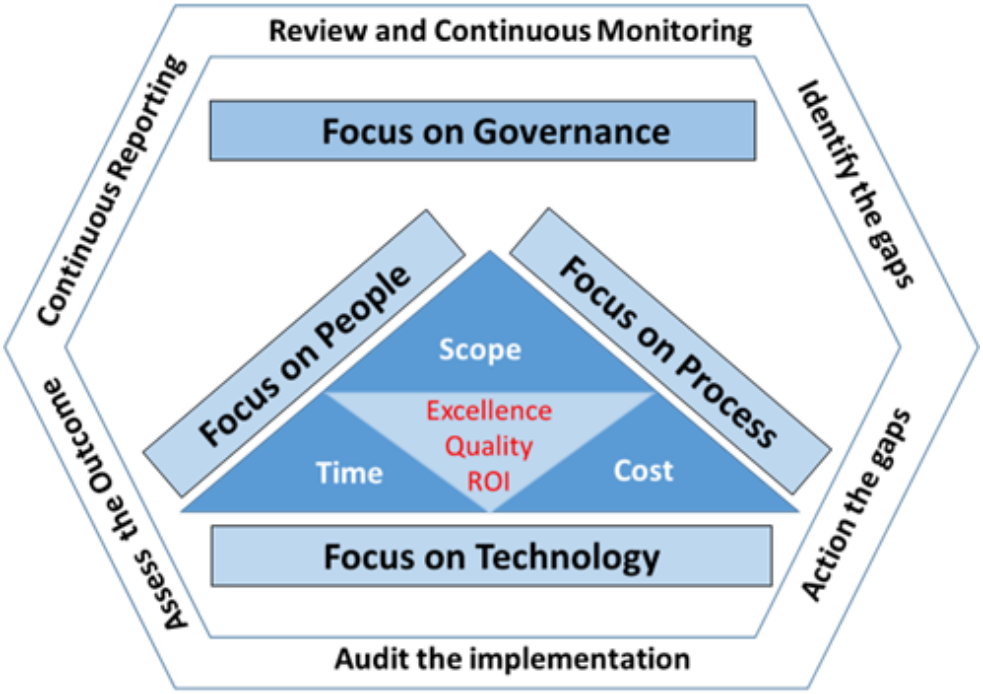
To ensure compliance with the requirements of Privacy legislation such as POPIA and GDPR it is important to know the focus areas that need to be addressed to be compliant.

The main focus areas are:

- Governance;
- People;
- Process; and
- Technology

4.2 PRIVACY COMPLIANCE FRAMEWORK

The privacy compliance framework is depicted in **Picture 1**. And described in more detail below



Picture 1

4.2.1 Focus on Governance

One of the most important areas in any business is taking accountability for the actions and implementing good corporate governance.

The focus on governance means that the organisation will establish an Information Governance Committee (IGC) and other structures to ensure that compliance is not a once-off process and that continued management of Information processes will take place.

4.2.2 Focus on Process

Another important area in any business is putting the processes in place to ensure that Personal Identifiable Information (PII) is processed is in line with relevant legislation.

This will include performing a Personal Information Impact Assessment (PIIA) and also developing and implementing the needed policies and procedures and other control measures to ensure compliance with the relevant privacy legislation.

4.2.3. Focus on People

Most of the information security breaches involves people in one way or the other. It is important to ensure that management and employees (full and part-time) is made aware of their responsibilities in relation to processing Personal Identifiable Information (PII).

Management and Employees must undergo Privacy and Information Security training at least annually. All new employees must be trained within 3 months from joining the company.

4.2.4 Focus on Technology

Implementing technology with the appropriate security safeguards is crucial. The technology part includes the software, hardware and data specific requirements. This also

includes where Personal Identifiable Information (PII) is processed, stored and destructed. It is important to appoint a specialist in IT to set up and deal with the technology part. This can be done in-house or by outsourcing the IT function.

4.2.5 Review and Audit

4.2.5.1 Review and Continuous Monitoring

The following should be reviewed and monitored on a regular basis, that:

- The Governance Process are functioning as intended and that there have been regular Information Governance Committees (IGC);
- The processes been reviewed on a regular basis and that all the policies and procedures have been reviewed and updated at least annually;
- That the other control measures that have been implemented are functioning as intended and that they are adequate and effective;
- The management and employees have been made aware and kept aware of how to process Personal Identifiable Information (PII) and that the privacy awareness campaign have been developed and implemented;
- The technology areas have undergone vulnerability assessments and where applicable that penetration testing been done. The technology area also includes information security management.

4.2.5.2 Identify the gaps

On a regular basis gap (weaknesses) should be identified and actions to mitigate the gaps should be recorded in the Privacy Implementation Action Plan.

The gaps (weaknesses) should be prioritised and an accountable person should be identified to address the gaps (weaknesses).

There should also be a due date set when the gaps (weaknesses) should be addressed.

4.2.5.3 Action the gaps

The gaps (weaknesses) should be actioned as per the Privacy Implementation Action Plan.

A specific responsible person should be identified that would co-coordinate or perform an action and a due date to complete the action should also be set.

Where there is a specific due date the progress to address the gaps (weaknesses) should be reported to the Information Governance Committee.

4.2.5.4 Audit the implementation

It is important to review if the implementation of the controls to address the gaps (weaknesses) have been made successful.

The ideal is to get someone that was not involved in the implementation to review the implementation. Where there is not someone with the knowhow or skills inhouse this can be insourced from independent auditors.

4.2.5.5 Assess the outcome

Assess the outcome of the “audit” and determine if there is any action needed. Where the gap (weakness) has been addresses it would be noted. Where there is additional work required it should be added to the Privacy Implementation Action Plan.

4.2.5.6 Continuous Reporting

It is important to continuously report the status of Information Management to the Information Governance Committee and at least on a quarterly basis to the Board of Directors.

4.2.6 Project Management

During the implementation of privacy processes in the organisation, project principles of scope, time and cost is important to consider.

5. INFORMATION GOVERNANCE

5.1 INFORMATION OFFICER

The responsibilities of the Information Officer in terms of the Protection of Personal Information Act (POPIA) No. 4 of 2013 include:

- the encouragement of compliance (e.g. awareness and training) by the organisation taking into consideration ALL the conditions for the lawful processing of personal information;
- ensuring compliance by the organisation with the provisions of POPIA;
- dealing with requests in relation to POPIA to the organisation for instance, requests from Data Subjects to update or view their personal information;
- working with the Information Regulator in relation to investigations; and
- designation and delegation of relevant duties to deputy information officers.

The responsibilities of the Information Officer have **been expanded upon** in the **regulations** that relate to the Protection of Personal Information Act that was issued on the 14th of December 2018, the Information Officer must ensure that:

- a compliance framework is developed, implemented, monitored and maintained;
- a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
- a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);
- internal measures are developed together with adequate systems to process requests for information or access thereto; and
- internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.

5.2 INFORMATION GOVERNANCE MANAGEMENT COMMITTEE

The Information Governance Management Committee has the following responsibilities:

Strategic

The oversight of the full information lifecycle for both structured and unstructured information;

- Endorsement of information policies and procedures in relation to information management (including principles);
- Assists with ensuring compliance with the Protection of Personal Information (POPIA and GDPR (where applicable)) which include the following:
    - The security and integrity of data/information held by, or on behalf of the organisation;
    - The dissemination of the organisation's data/information to third parties;
    - Information and data confidentiality and availability;
    - Information and data quality (completeness, accuracy and updating);
    - Information sharing arrangements with other parties;
    - Retention and Destruction of information practices;
    - Document Management (including digitisation); and
    - Discussing and identifying the areas where consent will be needed in relation to processing of personal information.
- Assists with the Integration of people, technologies, information and processes across the organisation;
- Identify and rate the information risks and provide input to the organisation's enterprise-wide risk management process;
- Review that there is proactive monitoring of data/information breach incidents and the response to these incidents;
- Review and provide oversight to ensure that the information architecture supports confidentiality, integrity and availability of information;
- Endorsement of information-related strategies and roadmaps;
- Prioritisation of information-related initiatives;
- Establishing information-related metrics and oversight of results;
- Direct efforts to resolve issues in relation to information management;
- To assist with advice on the leverage of information to sustain and enhance the organisation's intellectual capital; and
- Review and assess the actions taken to monitor the effectiveness of information management and how the outcomes were addressed.

Operational

- Establishing structures needed to support information governance in the organisation;
- Delegation of authorities for implementation of decisions;
- Coordination of information management responsibilities across the organisation ensure complete coverage of the information lifecycle;
- Making the organisation aware of the Information Governance structures and its roles and responsibilities.
- Promoting good information management practices and publishing the names of the Information Asset Owners (IAO's) for easy reference so they can be notified of particular issues relating to their domain; and
- Training and mentoring of IAOs to enable them to fulfil their roles.

6. INFORMATION PROCESSING PRINCIPLES

6.1 PROTECTION OF PERSONAL INFORMATION ACT (POPIA)

ERGuide Online fully supports and complies with the eight principles of the POPIA which are summarised below:

Accountability – a responsible party must ensure that the Information Processing Principles are complied with.

Process Limitation – personal information must be processed lawfully and in a reasonable manner.

Purpose Specification – personal information shall be obtained/processed for specific lawful purposes.

Further Processing Limitation - personal information shall be obtained for no longer than is necessary for the purpose/s for which it was collected.

Information Quality - personal information must be complete, accurate, not misleading and kept up to date.

Openness – personal information may only be processed by a responsible party who has taken reasonable steps to notify the data subject.

Security Safeguards – personal information must be kept secure.

Data Subject Participation – a data subject has the right to request the responsible part to confirm, free of charge, whether or not the responsible party holds personal information about him as well as the description of the personal information held by responsible party.

6.1.1 ACCOUNTABILITY

The Act is intended not to prevent the processing of personal information, but to make sure that a responsible party ensures that the information Processing Principles as set out in POPIA and all the measures that give effect to the principles are complied with.

The data subject must be told who the responsible party (in this case, ERGuide Online) and the purpose for which personal information is to be processed by ERGuide Online.

ERGuide Online has developed a Privacy Policy which is available at ERguide Online premises and is also accessible online at www.erguide.co.za This policy outlines ERGuide Online's commitment to privacy.

6.1.2 PROCESS LIMITATION

For personal information to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the responsible party or the party to whom the personal information is disclosed. When special personal information is being processed, in most cases the data subject's explicit consent to the processing of such special personal information will be required.

A responsible party must collect personal information directly from the data subject unless information is in a public record, the data subject has consented, or the collection of personal information doesn't prejudice the legitimate interest of the data subject, or

collection is necessary to: avoid prejudice to laws, to comply with the collection of revenue (South African Revenue Services Act nr 34 of 1997), proceedings in a court, interest of national security or to maintain the legitimate interests of the responsible party.

Where ERGuide Online processes personal information as a responsible party, the data subject should be informed of such, as well as the purpose for which the personal information is being processes by ERGuide Online and stating whom the personal information may be disclosed or transferred. ERGuide Online has drafted a Terms of Use agreement which is found online at www.erguide.co.za which explicitly outlines how ERGuide Online may use a person's information.

6.1.3 PURPOSE SPECIFICATION

Personal information may only be processed for a specific and lawful purpose or for any other purpose specifically permitted by POPIA, and steps must be taken to ensure that the data subject is aware of the purpose of the collection of the personal information. This means that personal information must not be collected for one purpose and then used for another or retained for any longer than is necessary for achieving the purpose for which the information was collected.

Personal information should only be collected to the extent it is required for the specific purpose notified to the data subject. Any personal information which is not necessary for that purpose should be collected at the first place.

If it becomes necessary to change the purpose for which the personal information is processed, the data subject must be informed of the new purpose before any processing occurs. Any employee personal information collected by ERGuide Online is used for ordinary Human Resources purposes. Where there is a need to collect employee personal information for another purpose, ERGuide Online will notify the employee of this and where it is appropriate and practicable, will get the employee's consent prior to such processing.

Where ERGuide Online collect personal information directly from a data subject the personal information collected and processed by ERGuide Online (i.e. ID number, proof of address, etc.) will only be used for the required purpose.

6.1.4 FURTHER PROCESSING LIMITATION

Personal information should not be kept longer than is necessary for the purpose. For guidance in relation to a particular personal information retention period an employee should contact ERGuide Online. ERGuide Online has various legal obligations to keep certain employee and student data for a specified period of time as well as company invoices. In addition, ERGuide Online may need to retain personal information for a period of time to protect its legitimate interest.

ERGuide Online will not use the personal information for any other purpose that it has received the information in the first place.

6.1.5 INFORMATION QUALITY

Personal information must be complete, accurate, and kept up to date. Personal information which is incorrect or misleading is not accurate and steps should be taken to

check the accuracy of any personal information at the point of collection and at regular intervals afterwards.

Inaccurate or out-of-date personal information should be destroyed. Employees should ensure that they notify their manager/human resources of any relevant changes to their personal information so that it can be updated and maintained accurately. Examples of relevant changes to personal information would include a change of cellular number, surname, address, etc.

All personal information which is in paper form should be destroyed only by shredding. If the personal information is on an electronic medium, ERGuide Online must ensure that a reputable service provider destroys the personal information so that there is no future record of the information on the medium and must obtain an undertaking from the applicable service provider in this regard.

6.1.6 OPENNESS

Personal information may only be processed by ERGuide Online if ERGuide Online has notified the data subject. ERGuide Online obtains information from legitimate sources.

In the case where ERGuide Online works directly with a data subject, ERGuide Online will take reasonable, practicable steps to ensure that the data subject is aware of the following:

- What information is being collected and where it is not collected from the data subject, the source of the information;
- The full name and addresses of ERGuide Online;
- The purpose of which the information is being collected;
- Whether supplying the personal information to ERGuide Online is voluntary or mandatory;
- The consequences of failure to provide the information;
- The applicable law authorising or requiring the collection of the information;
- The right to lodge a complaint against the Information Regulator: and
- Any further information such as recipient or category of recipients of information, nature of information, existence of the right of access and the right to rectify information collection.

6.1.7 SECURITY SAFEGUARDS

ERGuide Online and its employees must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal information, and against the accidental loss of, or damage to, personal information.

POPIA requires ERguide Online to put in place procedures and technologies to maintain the security of all personal identifiable information. Personal Information may only be transferred to an operator if the operator has agreed to comply with those procedures and policies or has adequate security measures in place.

Refer to ERGuide Online's Information Security and related policies for further information concerning ERGuide Online security safeguards.

The following must be maintained to ensure the following:

Confidentiality – that only people who are authorised to use the personal information can access it. ERGuide Online will ensure that only authorised persons have access to an employee's personnel file and any other personal or special information held by ERGuide Online. Employees are required to maintain the confidentiality of any personal information and/or special personal information that they have access to.

Integrity – that proper security safeguards are in place to ensure that the maintenance of, and the assurance of, the accuracy and consistency of information/data in maintained over its entire life cycle.

Availability – that authorised users should be able to access the personal information if they need it for an authorised purpose.

Examples of Security Procedures at ERGuide Online include:

- Secure lockable desks and Cupboards – desks and cupboards should be kept locked if they hold confidential personal identifiable information of any kind;
- Methods of Disposal – paper documents should be shredded. CD-ROMs and USB keys should be physical destroyed when they are no longer required;
- Equipment – data users should ensure that individual computer monitors do not show confidential information to passers-by and that they log off from their computer when it is left unattended; and
- User Management – any access to the ERGuide Online database is logged by ERGuide Online through a username and password system. Any changes/updates/uploads to the system are constantly tracked.

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, ERGuide Online or any third-party processing personal information under the authority of ERGuide Online, must notify the information regulator and the data subject.

Notification to a data subject must be in writing and communicated to the data subject in at least one of the following ways:

- Mailed to the data subjects last known physical or postal address;
- Sent by email to the data subjects last known email address;
- Placed in a prominent position on the website of ERGuide Online;
- Published in the news media; or
- As directed by the information regulator.

The notification referred to above must provide sufficient information to all the data subject to take protective measures against the potential consequences of the security compromise including:

- A description of the possible consequences of the security compromise;
- A description of the measures that ERGuide Online intends to take or has taken to address the security compromise;
- A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
- If known to ERGuide Online the identity of the unauthorised person who may have accessed or acquired the personal information.

6.1.8 DATA SUBJECT PARTICIPATION

A formal request from a data subject for information that ERGuide Online holds about them, must be made in writing accompanied with adequate proof of identification (in most instances, a certified copy of the individual's ID or passport and proof of residence).

Any employees who receive a written request in respect of data held by the Company should forward it to the Information Officer immediately.

For any individual requesting personal information will go to the relevant employee who will process the request. The employee will then request a certified copy of the individual's ID or passport as well as proof of address. Once received, the employee will then be authorised to release the personal information to the individual. The employee must:

- Record the request in the request register /system;
- Safely store the certified copy of the ID and passport either in a file in a locked cupboard (if in paper format) or online in an encrypted folder which cannot be accessed by unauthorised personnel. Storage of these documents should be kept for one year, after which they must be properly destroyed.

Any employee dealing with telephone enquiries should be careful about disclosing any personal information held by ERGuide Online over the phone. In particular the employee should:

- Check the identity of the caller to ensure that information is only given to a person who is entitled to that information – this can be accomplished by confirming: ID number, date of birth, address, cell phone number etc.
- Suggest that the caller put their request in writing if the employee is not sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified. In these circumstances, the employee should also request a certified copy of the ID/passport of the individual.
- Refer the request to their manager for assistance in difficult situations. No employee should feel forced to disclose personal information.
- Where a request has been made in terms of this section and personal information is communicated to the data subject must be advised of their right to request the correction of the information.

6.2 GENERAL DATA PROTECTION REGULATION (GDPR)

ERGuide Online fully supports and complies with the six principles of the GDPR which are summarised below:

Principle 1: Lawfulness, fairness and transparency

The personal information of the European citizens will be processed "lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')"

Principle 2: Purpose limitation

The personal information of the European citizens will be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')"

Principle 3: Data minimisation

The personal information of the European citizens will be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)”

Principle 4: Accuracy

The personal information of the European citizens will be “accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’)”

Principle 5: Storage Limitation

The personal information of the European citizens will be “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’)”

Principle 6: Integrity and Confidentiality

The personal information of the European citizens will be “processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

7. REVIEW OF POLICY

ERGuide Online will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives on at least an annual basis and more frequently if required, taking into account changes in the law and organisational or security changes.