|  |  |  |
| --- | --- | --- |
| S. Alderson Emergency Medical Training (Pty) Ltd | ***POPI COMPLIANCE***  ***(10 Protection Principles)*** | Doc. No POLICY  Rev. No.: 0 |
| Prepared by:  C. Alderson  **Quality Management Representative** | Approved by:  S. Alderson  **CEO** | Date:  2021/06/01 |

**POPI COMPLIANCE**

**1. ACCOUNTABILITY**

The **Information Officer** must ensure compliance. The Information Officer is required to **audit the processes used to collect, record, store, disseminate and destroy personal information:** in particular, ensure the integrity and safekeeping of personal information in your possession or under your control. The Information Officer must take steps to prevent the information being lost or damaged, or unlawfully accessed.

**2. PURPOSE SPECIFICATION**

The **Information Officer** must **define the purpose of the information gathering and processing:** personal information must be collected for a specific, explicitly defined and lawful purpose that is related to a function or activity of the company concerned.

**3. PROCESSING LIMITATION**

• Is done in a reasonable manner that does not infringe the privacy of the data subject.

• Must be adequate, relevant and not excessive given the purpose.

• Must have obtained consent or necessity, if consent, it must be *Voluntary, Specific, Informed*.

• Would prejudice lawful purpose, or • Information is contained in public record.

• religious or political beliefs

• race or ethnic origin

• trade union membership

• political opinions

• health, sexual life • criminal behaviour.

The **Information Officer** must ensure **processing is lawful** and:

Data subject consent is required - ***BUT NOT*** if;

What is “**Special Personal Information**”?

**4. TAKE STEPS TO NOTIFY THE ‘DATA SUBJECT’**

• the name and address of the company processing their information,

• he or she must be informed as to whether the provision of the information is voluntary or mandatory.

•The individual whose information is being processed has the right to know this is being done and why. **The data subject must be told;**

**5. FURTHER PROCESSING LIMITATION - (LIMIT THE PROCESSING PARAMETERS)** To assess whether further processing is permitted - Ask the following:

• Is there a valid relationship between the purposes?

• What is the nature of information?

• What are the consequences for data subject?

• The manner in which information was collected?

• Are there any contractual rights between the parties?

• If information is received via a third party for further processing, this further processing must be compatible with the purpose for which the data was *initially* collected.

**6. INFORMATION QUALITY**

• Complete

• Accurate

• Not misleading; and

• Updated where necessary

• Information being collected

• Purpose for which information is collected

• Whether the supply of information is voluntary or mandatory

• The consequences of failure to provide information

• Any particular law that applies

Once POPI is FULLY enacted and a Regulator established, organisations processing personal information will have to notify the Regulator about their actions.

AND

**The Responsible Party must take reasonable steps to notify the data subject of:**

***You will only need to notify once, not each instance of processing, but if processing is different than initially notified, you are required to notify within 1 year.***

**7. ACCOMMODATING DATA SUBJECT REQUESTS**

POPI allows data subjects to make certain requests, *free of charge*, to organisations holding their personal information. For instance, the data subject has the right to know the identity of all third parties that have had access to their information. A data subject can also ask for a record of the information concerned.

**8. SECURITY**

• Loss, damage or unauthorised access

• Unlawful access to or processing of personal information

• Identify all reasonably foreseeable internal and external risks

• Establish and maintain appropriate safeguards against the risks

• Regularly verify that the safeguards are adequately implemented

• Ensure the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards

• The Operator must treat information confidentially

• The Responsible Party must ensure that the operator establishes and maintains appropriate security safeguards

• *ALL* processing by an operator must be governed by a written contract

• In the event of security breaches, the Responsible Party must notify the Regulator and the data subject

The Information Officer is required to *secure the integrity of personal information* by taking appropriate, reasonable technical and organisational measures to prevent;**must take all reasonable measures to; oversee an Operator who processes data on his/her behalf.**

Responsible Party must be aware;

**9. RETAIN RECORDS FOR REQUIRED PERIODS**

• Personal information must be destroyed, deleted or ‘de-identified’ as soon as the purpose for collecting the information has been achieved.

• However, a record of the information must be retained if an organisation has used it to make a decision about the data subject. The record must be kept for a period long enough for the data subject to request access to it.

**10. CROSS BORDER DATA TRANSFER**

There are restrictions on the sending of personal information out of South Africa as well as on the transfer of personal information back into South Africa. The applicable restrictions will depend on the laws of the country to whom the data is transferred or from where the data is returned, as the case may be. The Responsible Party must institute a written protocol to cover these aspects.