Ameli Inyangu & Partners | Advocates
Nimble • Personal

Important data protection principles for businesses that handle personal data from their customers

By Geoffrey E. Odongo

From time to time businesses will find themselves handling information relating to identifiable natural persons who are their customers (referred to as personal data) in order to transact in goods or services.

The Data Protection Act, No. 24 of 2019 sets out the rights of data subjects together with the obligations of persons that have possession of their personal data by regulating the processing of such personal data. The word **processing** in this regard is a technical term covering a wide range of actions and which the Act defines as follows:

"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:

1. *Collection, recording, organization, structuring*
2. *Storage adaptation or alteration*
3. *Retrieval, consultation or use*
4. *Disclosure by transmission, dissemination or otherwise making available*
5. *Alignment or combination, restriction, erasure or destruction"*

Some of the principles businesses will be required to carefully consider when handling personal data are as follows:

1. The lawfulness, fairness and transparency principle

I. **Lawfulness** means that a person processing personal data must identify and document a legal basis or legitimate ground entitling him to perform any operation with the personal data. Such grounds are diverse and could include collection of the personal data by an employer in order to fulfil his obligations under an employment contract or where a business collects the personal data as part of the steps at the data subject's request before entering into a contract

II. **Fairness** requires that personal data is handled in ways that people disclosing the data would reasonably expect and not used in ways that have unjustified adverse effects on the data subjects.

III. **Transparency** refers to clarity to the data subject from whom the personal data is collected regarding its collection and the manner in which it will be used. Transparency also requires that any information and communication relating to the processing of the personal data is easily accessible and understandable by the data subject.

2. The purpose limitation principle

This principle requires personal data to be collected for specified, explicit and legitimate purposes. Meaning that the personal data should not be processed in a manner that is incompatible with the initial purpose disclosed to the data subject. Hence be clear from the outset why it is you are collecting the personal data and what it is you intend to do with it. Specify this in your privacy information disclosed to your individual customers so they are able to make an informed decision on whether they are happy to share the details you request.

Update your documentation and privacy information to individuals by ensuring that where you plan to use or disclose personal data for any purpose that is additional to or different from the original purpose, the new use is compatible with your original purpose disclosed to your customer. If not, get specific consent from your customer for the new purpose.

Regarding compatibility, the general rule is that if the new purpose is very different from the original purpose or would be unexpected, or would have an unjustified impact on the individual then it is unlikely to be compatible with your original purpose. However, to decide whether a new purpose is compatible with your original purpose you should take into account the following:

I. Any link between your original purpose and the new purpose.
II. The context in which you originally collected the personal data, e.g., is it particularly sensitive.
III. The possible consequences for individuals of the new processing

Whether there are appropriate safeguards, e.g., encryption or pseudonymisation.

3. The data minimization principle

This principle requires that personal data be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. This means that you identify the minimum amount of personal data that you need to fulfil your purpose and you hold no more than that much information. You must not collect personal data on the off chance that it might be useful in the future. Meaning that for you to hold information for a foreseeable event that may never occur provided you can justify it.

4. Integrity and confidentiality principle

This principle requires personal data to be processed in a manner that ensures appropriate security of the data including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures. The security measures in place should take into account matters such as the likelihood and severity of the risk to individuals if your security is breached.

Note that the appropriate security does not just depend on your circumstances but principally on the data you are processing and the risks posed. In order to enhance security the following fundamental security concepts need to be considered namely:-

I. Minimization of personal data collected
II. Managing, limiting and controlling access to personal data
III. Resilience of processing systems and service and ability to restore availability and access to personal data
IV. Regular testing of effectiveness of measures implemented

5. Accuracy principle

Every reasonable step must be taken to ensure that data is accurate, its source is clear and where data is

6. The storage limitation principle

This principle requires that personal data is kept in a form which permits identification of data subjects for no longer than is necessary. You should therefore not retain personal data in case it is needed in the future, or if there is a small possibility that it might be needed. Personal data should only be archived where your company still needs to hold the information otherwise it should be deleted. In this regard, you should come up with a retention period for the personal data that is justifiable. You should therefore periodically review the data you hold and erase or anonymise it when you no longer need it.