

---

# HIPSSA Project

**Support for Harmonization of the ICT Policies  
in Sub-Sahara Africa,  
Second Mission - Namibia**

## **PRESENTATION OF THE DRAFT DATA PROTECTION LEGISLATION FOR NAMIBIA**

**Samson Muhapi,**  
ITU National Legal Expert on Data Protection



---

# SUMMARY

1. What is **data protection**?
2. **Glossary/definitions**
3. The **10 Principles** of personal data protection
4. **Your rights** as a citizen
5. How and when can you **enforce your rights**?
6. The role of the Data Protection Authority



Committed to connecting the world



# 1. What is data protection?

- In the information society, there are numerous organisations and institutions collecting more and more information about individuals.
- We all disclose personal information, voluntarily (credit cards, edgars cards, etc.) or not (NSA, crime, medical records), to a multitude of organisations. Here are examples:



# Examples

- local or government authorities (permits, licences, municipal rates/taxes);
- MoF -tax authorities (tax returns);
- doctors and pharmacies (consultations and prescriptions);
- health insurance funds (claims/medical aid);
- banks (loan applications and credit card statements);

# Examples cont.....

- supermarkets (loyalty cards and lotteries);
- mobile phone operators, post and telecommunication services (telephone communications);
- sports clubs, cultural and leisure organisations (membership cards);
- or simply when browsing the Internet, or even spending the afternoon shopping because of the recordings of surveillance systems (CCTV).

# Cont....

- Due to modern computing techniques, this data can now be exploited more easily and in a variety of ways, either by the State and its authorities, by companies and professionals, or by clubs and associations.
- The proposed Legislation aims to establish the correct balance between the information society and the protection of privacy.



# Cont....

- Harmonisation of national data protection legislation within the SADC Member States is an essential step towards removing obstacles to the free circulation of data within the single market. The SADC Model Law on Data Protection aims to establish, throughout SADC, the same level of protection of rights and freedoms of individuals with regard to the processing of personal data. The Model Law will also lift restrictions on the flow of personal data within the SADC Region, while imposing strict conditions limiting the circulation of information





# Cont.....

- The building of personal profiles which reveal our life style and consumer habits is becoming a common practice (surveys, customer cards, Internet, etc).



Committed to connecting the world





---

# Cont.....

- Whether data is collected or recorded, consulted or disclosed to third parties, there are real and constant risks for the identifiable person, resulting from this accumulation and exploitation of personal data.



Committed to connecting the world



## Cont.....

- However, loss of control over your personal data and unwarranted intrusion into your private life are not inevitable. The **Model Law** which transposes a SADC protocol relating to data protection affords you certain rights. The law aims at protecting the privacy of individuals (and so even the interest of corporate bodies) with regard to the processing of their personal data by third parties.



Committed to connecting the world



## Cont.....

- However, loss of control over your personal data and unwarranted intrusion into your private life are not inevitable. The **Model Law** which transposes a SADC protocol relating to data protection affords you certain rights. The law aims at protecting the privacy of individuals (and so even the interest of corporate bodies) with regard to the processing of their personal data by third parties.

## Cont....

- The authorities, companies, professionals, associations and other organisations who collect, record, use and disclose personal data cannot do so without restrictions.
- They must notify the identifiable person (“data subject”) and inform them of the purpose of what the law calls “the processing of personal data”.



Committed to connecting the world



---

## Cont.....

- This processing must be limited to what is necessary and proportionate to the aims stipulated at the outset.
- Data must therefore always be used in accordance with strict rules, under the supervision of the DPA.
- To ensure transparency, any filing system must previously be either declared or authorised (depending on the type of data and processing).



Committed to connecting the world



---

# Cont.....

- The legislation on the protection of personal data does not only apply to computer files, but covers every kind of medium (paper files, audio and video recordings).
- The protection of privacy is a fundamental right, just like the inviolability of the home, the confidentiality of correspondence and freedoms of opinion and expression.

# GLOSSARY OF TERMS USED

- **PERSONAL DATA (Sec. 1)**
- Any information of any kind, regardless of its form, including sound and image, relating to an identified or identifiable person. An identifiable natural person ("data subject") or legal person (company) is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, genetic, mental, cultural, social or economic identity.



Committed to connecting the world





---

# Glossary

- **PROCESSING OF PERSONAL DATA**
- Any operation or set of operations performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of data.

# Glossary

- **Personal Data Filing System**
- Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
- **Data Controller**
- The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

---

# Glossary

- **PURPOSE**
- **Sec 15 of the Data Protection Bill**
- The objective chosen before instigating the processing, which serves to determine the operations to be performed to achieve it (or try to achieve it) and to determine the data undergoing these operations. Several vague objectives may not be gathered under one purpose. Determination of the purpose or linked purposes of the processing is a key to evaluating the legitimacy of the processing.

---

# Glossary

- **DATA SUBJECT'S CONSENT**
- **Sec 18 of the Draft Bill**
- Any explicit, unequivocal, freely given, specific and informed expression of the data subject's will by which the data subject or his legal, judicial or statutory representative agrees to the personal data being processed.



Committed to connecting the world



# Glossary

- **INTERCONNECTION**
- Any form of processing which involves connecting data processed for one purpose with data processed for identical or related purposes by one or more other controllers.



Committed to connecting the world



# THE 10 PRINCIPLES (COMMANDMENTS) OF PERSONAL DATA PROTECTION

- Those who process personal data concerning other people must comply with the following principles:



Committed to connecting the world



# 1: THE PRINCIPLE OF LEGITIMACY

- The processing of personal data is allowed only if there is a legitimate reason to justify it (**Sec. 15** of the Draft). Anyone who wants to process data concerning you must ask for your consent beforehand.
- Data processing is also permitted if it is essential in order to fulfil a contract, a task in the public interest or a legal obligation, or to protect your life.



Committed to connecting the world





---

# Legitimacy

- the processing can be legitimate if there is a justified interest, provided the processing of your data has only a minimal effect on your privacy.



Committed to connecting the world



# Legitimacy

- This **first criterion** (**legitimacy**) is used to determine whether the processing is legal/lawful. It answers the question of when *can your data be requested and used*.
- The next principles describes the rules that must be observed when processing data. They will answer the question of how your data can be processed.



Committed to connecting the world



# 2: THE PRINCIPLE OF PURPOSE

- The use of your personal data (including images and sounds) must be rigorously confined to a purpose which has been **explicitly determined** beforehand (**Sec. 15**).
- The collection, recording and use of your personal data are strictly limited to what is necessary to achieve the aims specifically declared in advance by the authority, agency, company, association, professional or self-employed worker involved.



Committed to connecting the world



# Example

- Following an accident at work, your employer tries to find out about your state of health from your GP. Thinking she is doing the right thing in reassuring him, the doctor's assistant provides information on the doctor's diagnosis.
- In doing so, she is transgressing the purpose for which the medical practice holds this information, i.e. in order to provide health care. (Think about the doctor/patient or lawyer/client professional relationship.)

# Cont....

- These users cannot disclose the data to other organisations or people, unless it is needed to accomplish the same aims.



Committed to connecting the world



# 3: THE PRINCIPLES OF NECESSITY AND PROPORTIONALITY

- The principle of proportionality ensures that the processing of your personal data is limited to cases where there is a direct connection with the initial purpose of the processing.



Committed to connecting the world



# Necessity and proportionality

- The information must not only be useful, but also **necessary** to whoever is processing your data. The data being processed must not be excessive in relation to the aim pursued (**Sec. 14 of the Draft DPA**).



Committed to connecting the world





# Example

- When booking a table at a restaurant by telephone, the manager of the establishment asks you to supply your credit card number.
- **This information should be regarded as excessive in relation to the aim being pursued, which is only to arrange available tables.**

# 4: THE PRINCIPLE OF THE ACCURACY OF DATA

- As inaccurate or incomplete information can harm the person to whom it relates, every effort must be made to ensure the data being processed is correct and up-to-date. If this is not the case, the personal data must be rectified or erased (**Sec. 13 of the Draft DPA**).



Committed to connecting the world



# Accuracy

- The law also protects you against any negative decision automatically taken about you by a computer, without you being able to put forward your personal point of view.
- **Sec. 13:**
- The data controller must ensure that personal data processed is:
  - (a) adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed;

# Accuracy

- (b) accurate and, where necessary, kept up-to-date;



Committed to connecting the world



# Example

- You are applying to your bank for a personal loan to buy some furniture. After submitting your application via the Internet, you immediately receive a negative reply from your bank which refuses to grant you the requested loan. It transpires that no bank adviser has been involved, but that your application has been assessed using a software which evaluated your request upon pre-established ratios and statistics.*



Committed to connecting the world



# Solution

- In this event, you have the right to insist on your application to be re-examined on the basis of an interview with your bank adviser who should listen to your argument.
- During this interview, you might point out, for example, that your financial situation has recently improved thanks to an inheritance. It could even be possible that the figures used were incorrect or that there was a mix-up with a debt-ridden person of the same name.

# 5. THE PRINCIPLE OF FAIRNESS

- **Sec 14 of the DPA**
- Your personal data must be collected, recorded, used and communicated fairly, and with your knowledge.
- Also, your data must be erased or rendered anonymous as quickly as possible. Subsequent use of your personal data for purposes other than those stipulated from the outset, is prohibited as a rule.





# Example

- *Pick n Pay supermarket offers you a loyalty card to give you special discounts on your shopping or an end-of-year rebate. As you subsequently pass through the checkout, the contents of your basket are recorded and used to build a consumer profile, which will be monitored on a regular basis.*



Committed to connecting the world



# Result

- If this is done without your knowledge, and if you weren't informed about it when signing up, the principle of fairness has been violated.



Committed to connecting the world



# 6. THE PRINCIPLE OF SECURITY AND CONFIDENTIALITY (Sec. 26)

- Your personal data must be processed in a confidential manner and stored in safe forms and places.
- In the event of non-compliance with this principle, the person who processes your data assumes personal responsibility. This includes the individual behaviour of employees, and contracts entered into with subcontractors (suppliers for instance) as well as the choice of technical equipment (in terms of computer security).



Committed to connecting the world



# Example

- *You want to change your mobile phone network. However, having looked at your application, the sales consultant of the company you have just chosen refuses to accept you as a new client. This person, who used to work as a sales agent for your LEO (previous GSM operator), refers to a dispute over a bill which you had with the first company.*



Committed to connecting the world



# Issues

- By allowing its sales agents to obtain information from its accounts department, your previous GSM operator failed to ensure that personal information on its clients could only be accessed by those employees really needing it for their work.
- So, was the staff properly warned against the temptations of misusing client-related data? How was the sales agent able to bring a client file from his old employer to his new employer? Was the file stolen?

- Solution....
- Whatever the case, the security measures and internal organisation of the company were inadequate in terms of maintaining the confidentiality of personal data. The management which failed in its legal obligations, as well as the unscrupulous employee are to blame for this breach.



# 7. THE PRINCIPLE OF TRANSPARENCY

- The law guarantees that you can obtain the information you need about the processing operations performed on your personal data and gives you the opportunity to exercise personal control. Anyone who wants to process your personal data must notify you when the data is collected or in the event of your data being communicated to third parties.



Committed to connecting the world





# Cont....

- You have the right to request details of the personal information on record and about its use, you also have the right to demand that any data not processed in accordance with the law be deleted.
- The registration of all databases with the Data Protection Authority contributes to transparency. The public register of the processing of personal data will be accessible via its website



# Example

- *Seeing that you have been in a state of exhaustion for a long time, your GP suggests having your blood analysed to determine the causes of your fatigue. The blood sample is taken by an external laboratory, which sends the results of this analysis to your doctor. It turns out that an HIV test has been done without your knowledge.*

# Remark

- This constitutes a breach of the principles of transparency and loyalty. You should also think of the consent requirement, the purpose requirement, legitimacy, etc.



## 8. PARTICULARLY SENSITIVE INFORMATION IS SUBJECT TO EVEN MORE STRINGENT PROTECTION

- The processing of personal information which reveals your opinions and beliefs, or which relates to your state of health or your sex preferences, including your genetic data, is prohibited, apart from a few exceptions which are enumerated in a restrictive way in the law.

---

# Cont.....

- Moreover, the processing of this type of data must, in principle, be explicitly authorised by the Data Protection Authority.



# Example

- *At a job interview, the company's Human Resources Manager to whom you are presenting yourself asks you what you think about financing retirement and the respective views of the political parties on this subject. He also makes it known to you that he keeps a list of employees who are members of trade unions.*



---

# Solution

- Gathering this kind of information (sensitive data) is normally prohibited by the law.



Committed to connecting the world





# 9. SURVEILLANCE (VIA AUDIO, VIDEO, DATA) OF IDENTIFIABLE PEOPLE IS STRICTLY LIMITED BY LAW

- An authorisation from the DPA is required before using technical means for monitoring people, particularly by video camera, electronic tracing, etc. Personal data gathered in this way can only be processed under certain very specific circumstances enumerated by the law.



Committed to connecting the world



---

# Example

- *Your telephone conversations are recorded by the company you work for, without you having been told beforehand.*



Committed to connecting the world



# Solution

- This is contrary to the principle of transparency. Furthermore, the employer requires authorisation from the DPA, which is responsible for verifying the legitimacy and proportionality of such a practice.



# 10. USE OF YOUR PERSONAL DATA FOR ADVERTISING OR MARKETING PURPOSES REQUIRES YOUR PERMISSION

- You may object to the use of your personal data for commercial purposes at any time. Direct marketing using modern means of communication (SMS, e-mail, etc) is in principle prohibited if you haven't given your consent.



Committed to connecting the world



# Example

- *Being assailed with junk mail, you require the business stores and commercial companies to stop sending this mail. It turns out that the company sending the personalised mailings is sponsor to your sports club from whom it received your address as well as the database of all the club members. The club should not have communicated its file of recordings concerning its members as the information contained is only meant to be used to manage the club and organise its activities.*



# Remark

- This unlawful misuse of the purpose for which the personal data was given is a breach of data protection law as well as an offence that is subject to punishment.



Committed to connecting the world



---

# Advertising, marketing, etc

- The law aims to ensure transparency in the processing of your personal data and encourages a certain amount of self-help from each data subject. It confers rights which allow you to personally check on what is happening to your data.





# Data Protection Authority

- Sec 3 to 12
- Establishment of the Authority, Board, qualifications, vacation of office, etc.
- Data Protection Authority is the independent supervisory authority which upholds the rights of individuals and ensures these are respected by both private persons and public authorities.
- To be in line with the SOE's Act.



---

# END

- Comments
  - Samson N Muhapi
    - National Law Expert: Data Protection
  - Pria Chetty
    - International Law Expert: Data Protection

---

# END OF BILL

- Comments

- Samson N Muhapi

- National Law Expert: Data Protection

- Pria Chetty

- International Law Expert: Data Protection



Committed to connecting the world

