'creating a level playing field'

Cyber & Data Protection Baseline Assessment Of Zimbabwean Enterprises

Report prepared by:
Research and Development Department (R&D)
Postal & Telecommunications Regulatory Authority of Zimbabwe (POTRAZ)

Executive Summary

93% aware of Cyber Act

62.5% organisations did not have Data Protection Officers

99% of organisations confirmed their processing of one or more of the categories of 'personal information' as specified in Cyber and Data Protection Act Chapter 12:07

80% of organisations, across sectors, stored personal data for periods exceeding five years and

91% of these organisations had minimum data retention periods explicitly defined in their policies

95% had antivirus and malware protection software, 88% had firewalls.

93% of the surveyed organisations desired to receive cyber and data protection

Executive Summary

This report presents a summary of the findings of the Cyber and Data Protection Act Baseline Survey that was carried out by POTRAZ Research and Development Department. As "the oil of the digital era", entities that own or obtain access to data have the potential to influence society and the economy. The survey sought to establish the status on the policies, practices, procedures, and governance employed by data controllers in their collection, storage, and use of personal information.

The study incorporated both qualitative and quantitative methodologies to carry out the survey. An online survey was conducted in which ninety-nine (99) organisations responded, and representation from all sectors was addressed in recruiting.

The summary of findings is outlined below:

- Awareness of the Cyber and Data Protection Act was high as 93% of the respondents, across all sectors, were aware of the Cyber and Data Protection Act (Chapter 12:07) which was promulgated in 2021.
- Insights from the survey supported the application of the Act across sectors as well as the need for extensive enforcement. 99% of organisations within the identified sectors confirmed their processing of one or more of the categories of 'personal information' as specified in Cyber and Data Protection Act Chapter 12:07; and 84% of the organisations also admitted to the processing of information through automated means.
- Some organisations did not obtain consent from data subjects before the processing of personal data in violation of the Cyber and Data Protection Act Chapter 12:07. 70% and 63% of surveyed organisations confirmed that they obtained consent from data subjects before processing sensitive and non-sensitive information respectively.
- 23% of the organisations who claimed to obtain consent revealed that they attained consent verbally from data subjects, which is not in compliance of the Act, particularly for sensitive information.
- 62.5% organisations did not have Data Protection Officers (DPOs). Only 37.5% of organisations who processed personal information confirmed that they had appointed Data Protection Officers (DPOs). The financial services sector had the largest proportion of organisations who had appointed Data Protection Officers.
- Most of the organisations who had not appointed DPOs did not have any intensions to do so. 72% of the surveyed organisations highlighted that they did not have any plans of appointing a DPO, with only 28% confirming such intentions.
- Furthermore, the few organisations with intentions to appoint a DPO were not in a hurry to do so. 60% expected to appoint a DPO after a period exceeding twelve (12) months. Only 7% expected to appoint a DPO within a period of three months.
- The study revealed that most organisations have never conducted a data protection impact assessment as reflected by 80% of the surveyed organisations. A correlation analysis reflected that organisations with DPOs were more likely to conduct data protection impact assessments than those without.
- Most of the organisations stated that they had security practices, policies and procedures to protect personal information. For example, 95% had antivirus and malware protection software, 88% had firewalls. Moreso, 88% of the organisations had internal non-disclosure policies which prohibited unlawful access to and or disclosure of personal data.
- The study revealed that 80% of organisations, across sectors, stored personal data for periods exceeding five years and 91% of these organisations had minimum data retention periods explicitly defined in their policies.
- The proportion of organisations that transferred data outside the country was low as only 13% of the surveyed organisations confirmed the transfer of personal data outside the country. A sector-by-sector analysis shows that the postal and courier sector, financial service sector and the NGO sector had the largest proportion of such entities.
- The study revealed a high demand for cyber and data protection training as 93% of the surveyed organisations desired to receive cyber and data protection training from POTRAZ, the designated Data Protection Authority in Zimbabwe.

This report provides a more detailed analysis of these and other findings as well as recommendations to remedy identified gaps.

Table Of Contents

List Of Tables

List Of Figures

1. Research Background

1.1 INTRODUCTION

The world's transition from the industrial to the information era has emphasized the importance of data and the dangers associated with its misuse. Consequently, it is crucial to have data protection regulations in place to safeguard the privacy of data subjects everywhere. Although the right to privacy is typically a right that is guaranteed by the constitution, it has become somewhat brittle due to the complexity of modern technology, leaving personal data in the hands of data controllers who may or may not have due consideration for this fundamental right. The rise of the internet over the past few decades has also had a profound effect on privacy and the protection of data, necessitating the promulgation of cyber and data protection legislations globally.

In Zimbabwe, the Cyber and Data Protection Act [Chapter 12:07] was promulgated in 2021. The objective of this Act is to increase cyber security to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives, and data subjects. The Act also aims at creating a technology driven business environment, technological development, and lawful use of technology. The Postal and Telecommunications Regulatory Authority of Zimbabwe is the designated Data Protection Authority in Zimbabwe, according to the Cyber and Data Protection Act (Chapter 12:07). The Authority regulates the way personal information may be processed by promoting and enforcing fairness to processing of data, among other functions. This baseline survey provides an analysis of the data protection ecosystem across various economic sectors in Zimbabwe.

1.2 PROBLEM STATEMENT

Baseline data on the data protection ecosystem is pertinent for implementation of the Cyber and Data Protection Act (Chapter 12:07) by POTRAZ. A baseline study was yet to the conducted by POTRAZ as implementation of the Act commenced in 2023. The unavailability of comprehensive data limits industry contextualisation in the implementation of the Act. This also means the absence of an evidence base on which to measure future progress or inform corrective action. It is against this backdrop that the survey was conducted.

1.3 OBJECTIVES OF THE STUDY

The study sought to achieve the following objectives:

1. To assess the level of awareness of the Cyber and Data Protection Act by organisations in Zimbabwe.
2. To evaluate the processing of personal information by organisations across sectors in Zimbabwe.
3. To identify existing policies, programs and security measures employed by organisations in Zimbabwe to ensure cyber security and data protection.
4. To evaluate the fulfillment of obligations with respect to the meeting rights of data subjects in Zimbabwe.
5. To determine the present status of the data protection personnel in the ecosystem in terms of complement and qualifications.
6. To assess organizational needs and demand for cyber and data protection training in Zimbabwe.

The Postal and Telecommunications Regulatory Authority of Zimbabwe is the designated Data Protection Authority in Zimbabwe, according to the Cyber and Data Protection Act (Chapter 12:07). The Authority regulates the way personal information may be processed by promoting and enforcing fairness to processing of data, among other functions. This baseline survey provides an analysis of the data protection ecosystem across various economic sectors in Zimbabwe.

1.4 RESEARCH QUESTIONS

The specific research questions were as follows:

1. What is the level of awareness by data controllers on the following:
    - Cyber and Data protection Act?
    - POTRAZ's designation as the Data Protection Authority?
2. What are the prevalent types of personal information processed by organisations?
3. Which policies, programs and security measures are employed by organisations to ensure cyber security and data protection?
4. To what extent are provisions currently in place to afford data subjects their rights as per the Cyber and Data Protection Act?
5. (a) What is the proportion of organisations that have appointed Data Protection Officers? (b) How qualified are the Data Protection Officers?
6. What is the scope and level of demand for cyber and data protection training by organisations?

1.5 SIGNIFICANCE OF STUDY

This survey plays a significant role in establishing priority areas for implementation of the Cyber and Data Protection Act [Chapter 12:07]. The baseline survey plays a pivotal role in establishing existing policies, programmes and security measures put in place by data controllers to protect personal and sensitive data they collect and process. In addition, the survey helps identify gaps for remedy as well as benchmarks on which future progress will be measured.

1.6 SCOPE OF THE RESEARCH

The baseline survey covered corporate players, academic institutions and government agencies. These data controllers were categorized into nine (9) categories/sectors namely Telecommunications, Postal and Courier Services, Financial Services, Health, Education, Non-Governmental Organisations, Tourism and Hospitality, Government Agencies and Retailers. It was mainly focused on registered organisations which collect and process personal and sensitive information in the process of doing their businesses. The unit of measurement was an enterprise with a minimum of thirty employees as per data controller thresholds specified in the draft Data Protection Regulations. the survey targeted head offices for organisations and not individual branches.

2. Research Methodology

2.1 INTRODUCTION

This section highlights the research approach and techniques used in the survey. These include research design, inclusion criteria, sample design, survey instrument design, data processing, analysis and reporting, ethical considerations as well as other survey implementation processes.

2.2 RESEARCH DESIGN

The mixed methods approach was used, combining qualitative and quantitative methods to effectively answer the research questions. The collection of data from multiple sources, across different industries, also facilitated triangulation of findings.

2.3 SAMPLING STRATEGY

Quota sampling was employed to select respondents from different economic sectors. Each sector would represent a stratum with similar characteristics. The team would contact organisations within selected economic sectors and seek their consent for participation in the survey. Electronic questionnaires were provided to consenting organisations for submission within a period of two weeks.

2.4 INCLUSION CRITERIA

The baseline survey covered organisation, institutions and agencies across nine key data-intensive sectors of the economy i.e., telecommunications, postal and courier, financial services, health, education,

tourism and hospitality, retailers, government agencies as well as Non-Governmental Organisations. The unit of measurement was an enterprise; this implies that the survey targeted head offices for organisations and not individual branches. The survey also targeted organisations with a minimum of thirty (30) employees as per data controller thresholds specified in the draft Data Protection Regulations.

Participation was not compulsory but voluntary, with consent requested and anonymisation guaranteed in all instances. Details used within sector's inclusion and exclusion criteria are outlined in table 1 below:

Table 1: Inclusion and Exclusion Criteria

SECTOR	INCLUSION CRITERIA	EXCLUSION CRITERIA
Telecommunications	• Licensed by POTRAZ. • Willing to participate in the survey.	• Not licensed by POTRAZ. • Unwilling to consent.
Postal and Courier Services	• Registered with POTRAZ. • Willing to participate in the survey.	• Not registered with POTRAZ. • Unwilling to participate.
Finance	• Registered Banks. • Registered Micro-Finance Companies. • Insurance Companies. • Willing to participate in the survey.	• Not registered. • Unwilling to participate.
Health	• Registered public/private hospitals, clinics and pharmacies. • Willing to participate in the survey.	• Not registered. • Unwilling to participate.
Education/Academia	• Universities. • Polytechnical Colleges. • Teachers' Colleges. • Willing to participate in the survey.	• Not registered. • Unwilling to participate.
Government Agencies	• Parastatals. • Local Authorities. • Ministries. • Willing to participate in the survey.	• Unwilling to participate.
Non-Governmental Organisations (NGOs)	• Registered to operate in Zimbabwe. • Willing to participate in the survey.	• Not registered • Unwilling to participate.
Retailers	• High market share. • Registered with the Companies Act. • Willing to participate in the survey.	• Low market share. • Not registered. • Unwilling to participate.
Tourism and Hospitality	• High market share. • Registered with the Companies Act. • Willing to participate.	• Low market share. • Not registered. • Unwilling to participate

2.5 SURVEY INSTRUMENT

The survey instrument was a questionnaire that was developed by the Research and Development team and approved by the Data Protection Unit (DPU). It was administered electronically. Table 2 outlines the

thematic areas of the questionnaire.

Table 2: Questionnaire Modules

MODULE	THEMES
Administrative Data	**ORGANISATIONAL PROFILE** • Sector • Number of employees etc.
Section A	**GENERAL**: • Awareness of Cyber & Data Protection Act • Type of personal and sensitive data collected and stored • Data subjects' consent • Data subjects` rights
Section C	**GOVERNANCE** • Appointment Data Protection Officer/s (DPOs) • Qualifications of the DPOs • Data Protection Impact Assessments
Section D	**DATA PROTECTION PRACTICES** • Security policies and procedures • Data storage • Incidence of data breaches • Transfer of data beyond borders
Section E	**CAPACITY BUILDING** • Training needs • Training frequency

The questionnaire had open-ended as well as closed-ended questions. Open ended questions were useful in soliciting descriptive information from the respondents and complementing the quantitative information.

2.6 DATA COLLECTION, PROCESSING & ANALYSIS

The questionnaires were administered using the Microsoft forms online platform. This proved effective in terms of managing costs and time. Extensive quality control measures were put in place to ensure the validity and reliability of the data collected. Skip routines and consistency checks were effectively applied to facilitate automatic flagging of any inconsistent responses. This ensured that respondents rectify inconsistencies before proceeding to the next modules of the questionnaire.

Data cleaning was done in Excel using logical syntax. Excel, SPSS and Power Bi were used for data analysis. Measures of central tendencies were computed to aid insights from the data collected. Data was presented in pie charts, bar graphs, tables to show patterns, and in narrative summaries to interpret data from quantitative methods. Cross-tabulations and Chi-square tests were also carried out to establish relationships between variables. Content analysis was applied in analysing qualitative data gathered using open-ended questions.

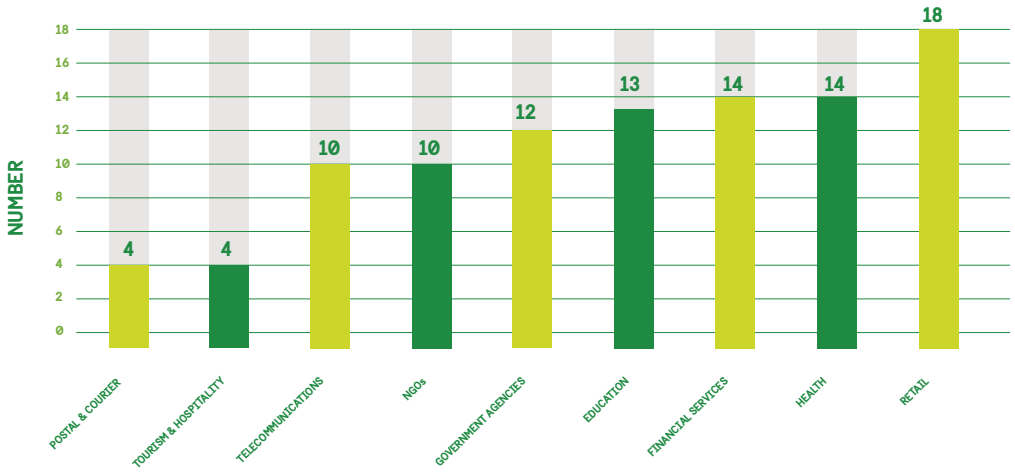
2.7 ETHICAL CONSIDERATIONS

Principles of informed consent and voluntary participation were followed in the administration of the survey. This was in cognisance of the fact the research was not a compliance audit but an exploratory assessment. Privacy and confidentiality of research participants were also ensured as data was sufficiently anonymized and pseudonymized. Participants were not subjected to any form of harm or liable to any penalties emanating from their disclosures in this research.

2.8 ATTAINED SAMPLE SIZE

Ninety-nine (99) entities responded to the questionnaire. All the nine targeted sectors were represented as follows:

Figure 1: Profile of Respondents



It is important to note that only registered organisations were surveyed, and the unit of measurement was an enterprise, not individual branches. Furthermore, only organisations with a minimum of thirty (30) employees were requested to participate and participation was voluntary.

3. Research Findings

3.1 INTRODUCTION

This chapter presents and discusses the baseline survey findings. The findings are presented in themes that are derived from the research questions. The qualitative and quantitative data gathered from the survey were analyzed using the Statistical Package for Social Scientists (SPSS) and Power BI. It explains how the analysis of both quantitative and qualitative data was conducted to augment each other and ensure the reliability of the findings. Content analysis was adopted for qualitative data gathered using open-ended questions.

3.2 GENERAL AWARENESS

3.2.1 AWARENESS OF THE CYBER AND DATA PROTECTION ACT

Awareness of the Cyber and Data Protection Act is high amongst organisations in Zimbabwe. 93% of the respondents, across all sectors, were aware of the Cyber and Data Protection Act which was promulgated in 2021. A detailed analysis by sector shows 100% awareness by players in the telecommunications sector, tourism and hospitality sector and across government agencies as shown in the table below.

Table 3: Awareness of the Act by Sector

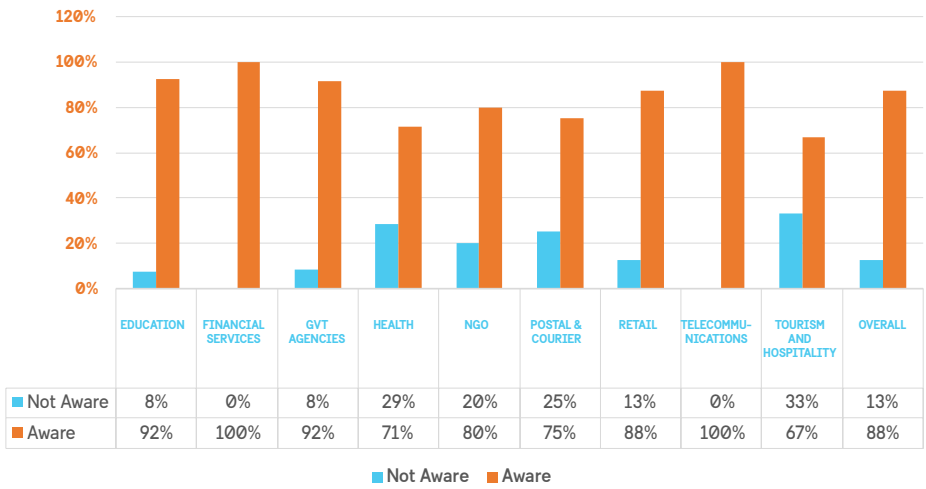
NO		Have you ever heard of the Cyber and Data Protection Act		Average
		YES	YES	
Sector	Education	8%	92%	100%
	Financial services	0%	100%	100%
	Government agencies	0%	100%	100%
	Health	14%	86%	100%
	NGO	0%	100%	100%
	Postal and courier	50%	50%	100%
	Retail	13%	88%	100%
	Telecommunications	0%	100%	100%
	Tourism & Hospitality	0%	100%	100%
Total		7%	93%	100%

It was surprising to note the high proportion of players in the postal and courier sector who were unaware of the Act. This points to the need for sensitisation of data controllers.

3.2.2 AWARENESS OF THE DATA PROTECTION AUTHORITY

Some of the organisations who were aware of the promulgation of the Cyber and Data Protection Act were unaware of the substantive aspects of the Act, particularly POTRAZ`s designation as the Data Protection Authority in Zimbabwe. An analysis of awareness of POTRAZ`s designation as the Data Protection Authority in Zimbabwe by sector is shown in Figure 2 below:

Figure 2: Awareness of the DPA

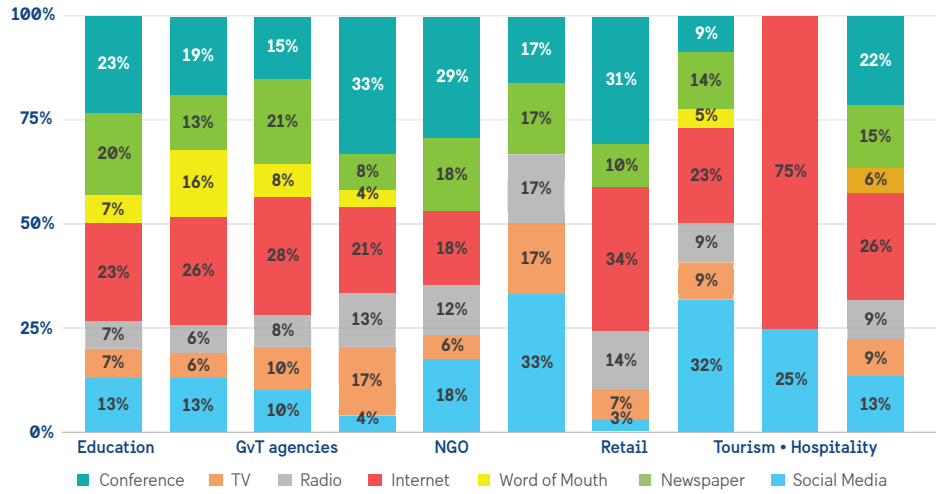


As shown above, organisations in the Telecommunications and Financial Services sectors were more aware, since they all had 100%. Tourism and Hospitality and Health sectors had largest numbers of respondents who were not aware with 33% and 29% respectively.

3.2.3 SOURCE OF INFORMATION

Social media platforms and the general Internet were the most popular sources of information about the Cyber and Data Protection Act. Conferences were also a popular source of information, particularly for organisations in the postal and telecommunications sectors. A sectoral analysis is shown in Figure 3 below:

Figure 3: Source of Information by Sector

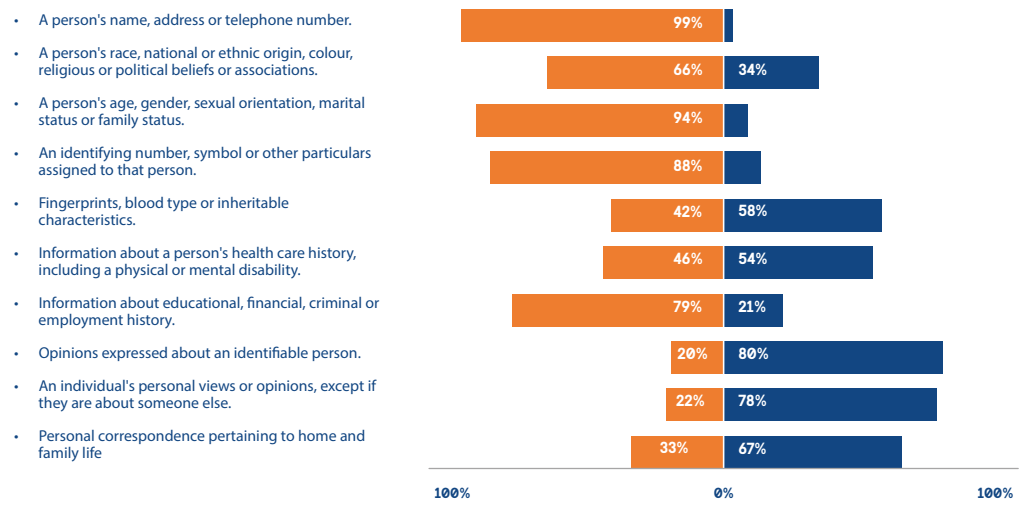


As shown above, awareness through the radio and television was low, this tallies with findings from the data subjects awareness survey. This can be explained by the current lack of data protection content on these platforms. Conferences were a popular source of information for telecommunications as well as postal and courier players. This is probably because the Act and other data protection matters were discussed in other POTRAZ workshops and forums.

3.3 PROCESSING OF PERSONAL INFORMATION

The research showed that all organisations within the identified nine sectors, process one or more of the categories of 'personal information' as specified in Cyber and Data Protection Act Chapter 12:07. The most processed personal information pertains personally identifiable data such as name, address and telephone number as shown in Figure 2 below:

Figure 2: Personal Information Processed by Data Controllers



Furthermore, 84% of the organisations also admitted to the processing of information through automated means. This information supports the general relevance and application of the Act across sector as well as the need for extensive enforcement.

3.3.1 REASONS FOR PROCESSING PERSONAL INFORMATION.

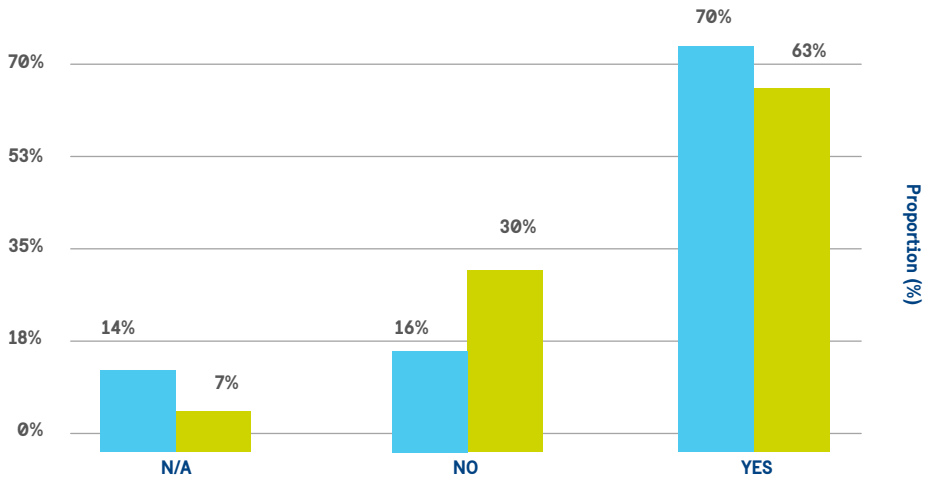
Content analysis was applied to open ended questions that prompted respondents to fill in reasons why they hold personal information. The study established that the main reason for the processing of personal information by organisations across all sectors was to comply with regulatory requirements. These include applicable Know Your Customer/Customer Due Diligence requirements by regulators across sectors.

Organisations also cited the need to facilitate various employment and personnel matters as a major reason for the processing of personal information. These include payroll administration as well as the processing of social security, insurance and fiscal requirements. The nature of some industries also requires players to collect personal information in the discharge of mandates e.g., health, education, tourism and hospitality amongst others.

3.4 OBTAINING CONSENT FROM DATA SUBJECTS

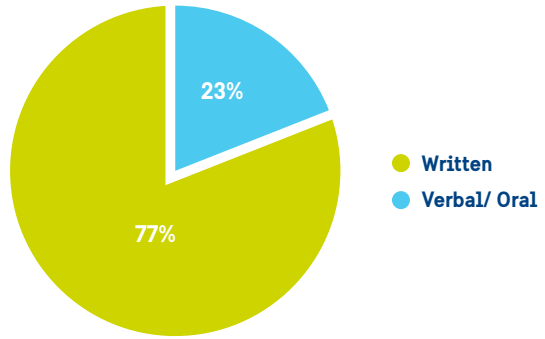
According to the Cyber and Data Protection Act, information may only be processed if the data subject or a competent person, where the data subject is a child, consents to the processing of such data. This applies to sensitive and non-sensitive data, as defined by the Act. Organisations were asked whether they obtain consent from data subjects before the processing of their information and the results are summarised in Figure 3 below:

Figure 3: Obtaining Consent



As shown above, 70% and 63% of surveyed organisations confirmed that they obtain express consent from data subjects before processing their sensitive and non-sensitive information respectively. Some organisations did not obtain consent from data subjects in violation of the Cyber and Data Protection Act Chapter 12:07. Of those organisations who obtain consent from data subjects, 77% attain it in written format as shown in Figure 4 below:

Figure 4: Methods of Obtaining Consent

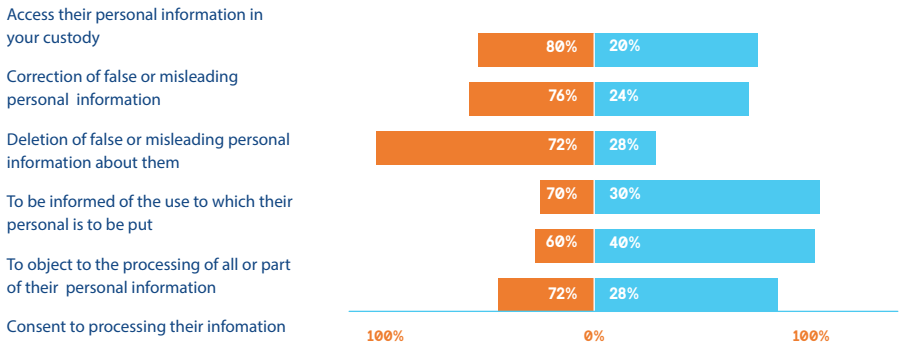


Consent, particularly written consent, is a very important matter in data protection and should be enforced as an obligation of data controllers.

3.5 RIGHTS OF DATA SUBJECTS

Some organisations confirmed that they have some provisions or policies in place to afford data subjects their information rights as shown in Figure 5 below:

Figure 5: Provisions to afford Data Subjects their Rights

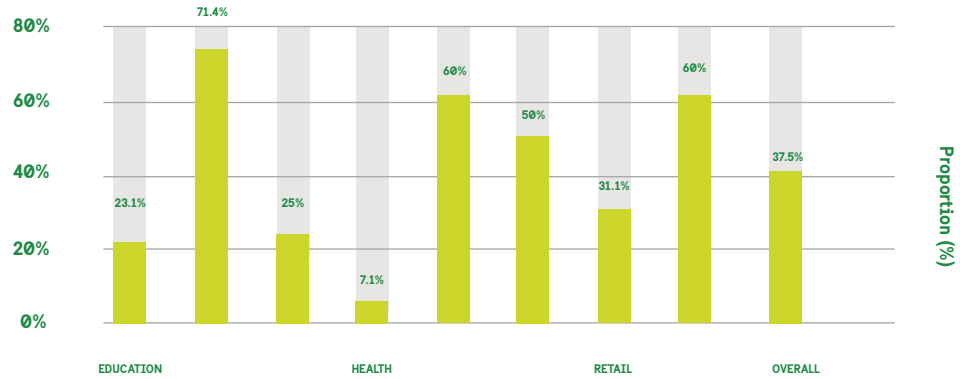


However, it should be noted that having provisions or policies in place does not necessarily imply sufficiency of the implied provisions, actual implementation or compliance with the Act. It is pertinent that Guidelines be developed for adoption and standardised implementation by data controllers.

3.6 APPOINTMENT OF DATA PROTECTION OFFICERS

Most organisations did not have Data Protection Officers. Only 37.5% of respondents who process personal information confirmed that they have appointed Data Protection Officers (DPOs) within their organisations. A sectoral analysis of organisations with DPOs is shown in Figure 6 below:

Figure 6: Proportion of Organisations with DPOs

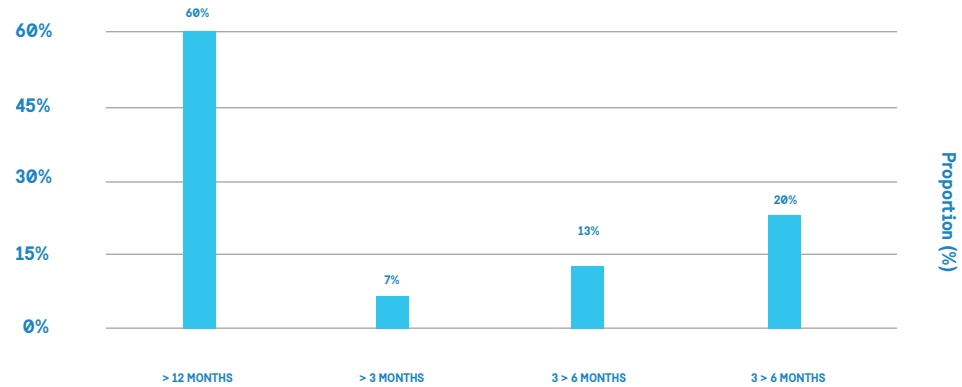


As shown above, the financial services sector had the largest proportion of organisations who have appointed Data Protection Officers, whilst there were none in the surveyed tourism and hospitality entities. There is need for sensitisation of data controllers to ensure compliance with provisions of the Act, such as the appointment of Data Protection Officers by data controllers.

3.7 INTENTION TO APPOINT DPO

Organisations that confirmed that they had not appointed DPOs were further inquired whether they had intentions of appointing a DPO. Responses also show that 72% of the data controllers did not have any plans of appointing a DPO, with only 28% confirming such intentions. However, there was no urgency even for the few 28% who had intensions of appointing a DPO in the future as shown in Figure 7 below:

Figure 7: Anticipated Time to appoint a Data Protection Officer



As shown above, the majority of the few (28%) organisations with intentions to appoint a DPO were not in a hurry to do so as 60% expected to appoint a DPO after a period exceeding twelve (12) months. Only 7% expected to appoint a DPO within a period of three months. This information is broken down by sector in Table 4 below:

Table 4: Anticipated Time to appoint a Data Protection Officer

Sector	>12 months	>3 months	3>6 months	6>12 months
Education	50%	0%	25%	25%
Financial services	50%	0%	0%	50%
Government agencies	0%	50%	0%	50%
Health	100%	0%	0%	0%
NGO	N/A	N/A	N/A	N/A
Postal and courier	N/A	N/A	N/A	N/A
Retail	100%	0%	0%	0%
Telecommunications	67%	0%	33%	0%
Tourism & Hospitality	100%	0%	0%	0%
Overall	**60%**	**7%**	**13%**	**20%**

As shown above, there is no urgency by organisations, particularly those within the health Sector, retail as well as Tourism & Hospital. None of the NGO as well as postal and courier organisations without DPOs had any plans to appoint a DPO.

3.8 QUALIFICATIONS OF APPOINTED DPOs

An analysis of the provided qualifications of the appointed Data Protection Officers from the various sectors shows that all of them are Information Technology/Computer Science professionals. They hold tertiary qualifications in Information Technology and Computer Science and professional certifications such as:

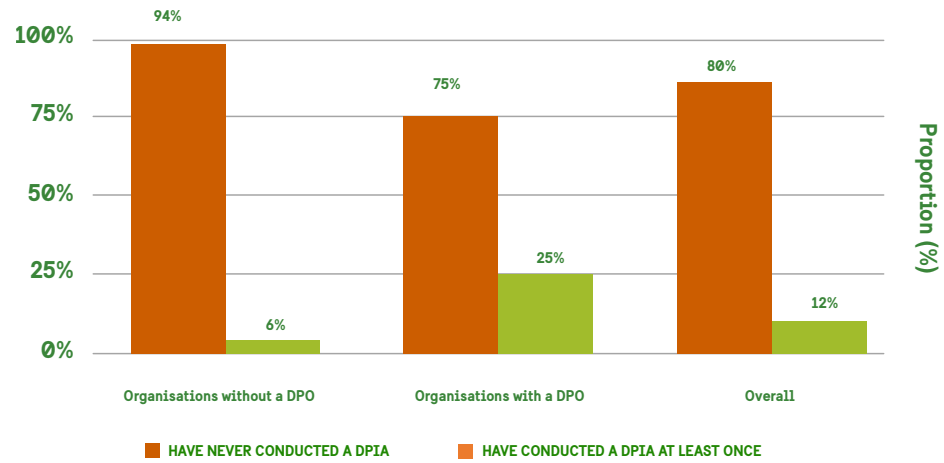
- Certified Information Systems Security Professional (CISSP).
- CISA - Certified Information Systems Audit
- Certified Information Security Manager (CISM)
- Certified In Governance of Enterprise Information Technology (CGEIT)
- Cisco Certified Network Associate (CCNA)
- Cisco Certified Network Professional certification (CCNP)
- Various Cyber Security & Forensics Certifications

The survey also revealed that the number of data protection certified professionals is still low as only one appointed Data Protection Officer had data protection certification. This certification was by the Professional Evaluation and Certification Board (PECB).

3.9 DATA PROTECTION IMPACT ASSESSMENTS

The study revealed that most organisations have never conducted a Data Protection Impact Assessment (DPIA) as reflected by 80% of the respondent organisations. A comparison of the execution of DPIAs by organisations with DPOs and those without DPOs is shown in Figure 8 below:

Figure 8: Data Protection Impact Assessments



The above information implies that the probability of conducting data probability impact assessments is higher in organisations with DPOs than those without. To test this assumption, a Chi-squared test of association was applied at critical value $\alpha = 0.05$ and Fishers exact test on scenario where the expected frequencies are less than or equal to 5. The tested hypotheses were as follows:

: There is no association between having a DPO and best practices in data protection by organisations.

: There is association between having a DPO and best practices in data protection by organisations.

Rejection criteria: We reject the null hypothesis if p-value/fisher's exact < 0.05 and accept the alternative hypothesis. If the p-value is greater, there will be not enough evidence to reject null hypothesis. The results of the tests done are summarised in the table below.

Independence test:

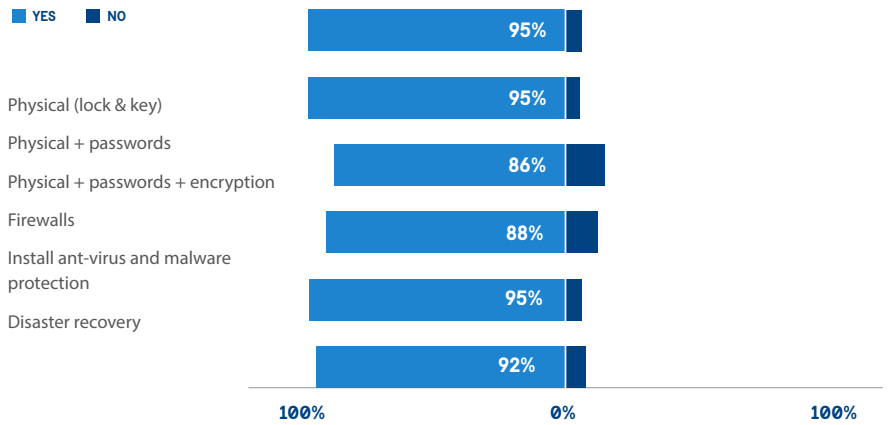
Best Practice		Hava data protection officer		CHI² *p-value* **Fisher's exact*
		YES	NO	
Conduct impact assessments	Yes	9	3	0.009
	No	50	27	

It was noted that the results shows that data protection impact assessments in organisation were associated with the presence of a DPO in each organisation. Hence it is very important to enforce the appointment of DPOs by organisations that process personal information.

3.10 DATA SECURITY CONTROLS

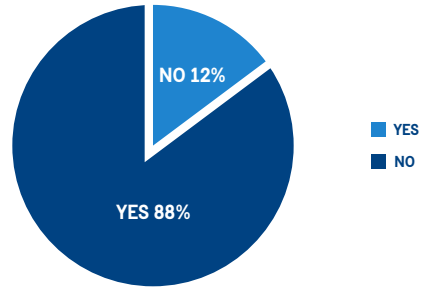
Generally, organisations appreciate the importance of data protection and security. They have various measures in place as summarised in Figure 9 below:

Figure 9: Security Controls



Other respondents stated that they have biometric access control measures in place to protect data from unauthorised access. A large number (88%) of the data controllers also highlighted that they have internal non-disclosure policies which prohibits unlawful access to and or disclosure of personal data.

Figure 10: Internal Non-Disclosure Policies

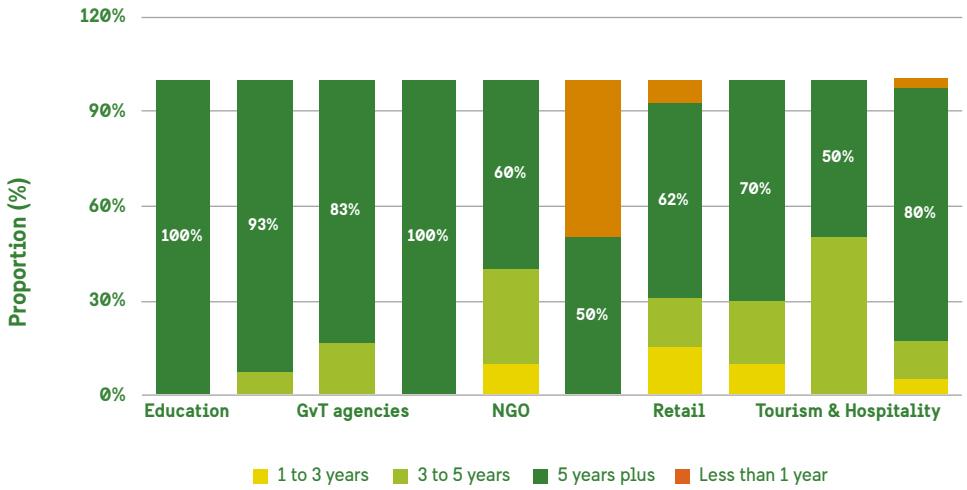


The adoption of non-disclosure policies as well as various security measures is still not 100%. Risk is still prevalent and there is great scope for educations and awareness.

3.11 STORAGE OF PERSONAL INFORMATION

The study revealed that 80% of organisations, across sectors, store personal data for periods exceeding five years and 91% of these organisations have minimum data retention periods explicitly defined in the policies. A sectoral analysis of the average retention periods for personal data is shown in Figure 11 below:

Figure 11: Average Data Retention Periods

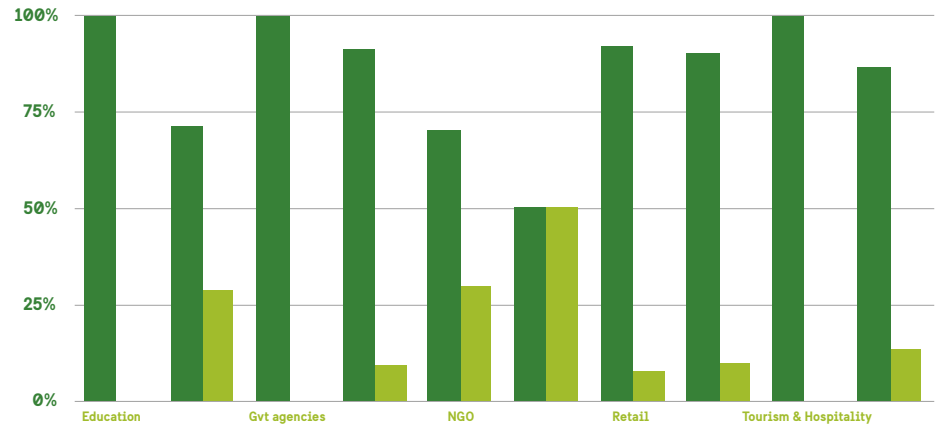


Generally, data is stored for longer periods in the education and health sectors as shown above. There may be need for sector-specific guidelines/rules of personal data retention to ensure that personal data is kept in a form which permits identification of data subjects for no longer than is necessary, or for the purposes for which the personal data are processed. This will ensure that if personal data is no longer necessary, organisations either erase or anonymise it.

3.12 TRANSFER OF DATA OUTSIDE THE COUNTRY

The proportion of organisations that transfer data outside the country is low as only 13% of the surveyed organisations confirmed that they transfer personal data outside the country. A sector-by-sector analysis shows that the postal and courier sector, financial service sector and the NGO sector have the largest proportion of entities that transfer personal data outside the country as shown in Figure 12 below:

Figure 12: Transfer of Data Outside Zimbabwe



Organisations who transfer data outside the country cited several measures that they use to guarantee data protection. These include the establishment of contracts, service level agreements, non-Disclosure agreements with recipients in foreign countries as well as the implementation of various technical security measures. Some organisations particularly NGOs and those in the financial services industry cited that they follow transfer principles of the General Data Protection Regulation (GDPR) i.e., the European Union and the European Economic Area information privacy and security regulation.

3.13 CAPACITY BUILDING

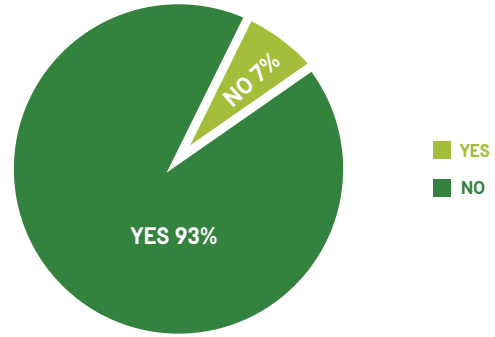
The survey revealed that 57% of organisations provide some form of training on data protection matters to their employees; 43% of organisations do not offer any such training to employees. A sectoral analysis is shown in Table 5 below:

Table 5: Training of Employees on Data Protection

Sector	Not Offered	Offered
Education	69%	31%
Financial services	29%	71%
Government agencies	50%	50%
Health	64%	36%
NGO	0%	100%
Postal and courier	50%	50%
Retail	46%	54%
Telecommunications	30%	70%
Tourism & Hospitality	50%	50%
Total	**43%**	**57%**

The health and education sector processes a lot of personal information, yet these sectors have the lowest proportion of organisations providing some form of data protection training to employees. The forms of training provided to employees by respondent organisations include sending employees to attend data protection workshops, online training courses, providing informational bulletins &newsletters on data protection and cybersecurity issues, inhouse training during orientation/ onboarding etc. It should be noted that this does not substantiate the depth, frequency or reach of the training currently provided. There is need for cyber and data protection training by organisation as 93% highlighted that they wish to be trained by POTRAZ.

Figure 13: Organisations Desirous of Training by POTRAZ



Most organisations stated that they want to be educated on all aspects of the Cyber and Data Protection Act, its application in respective sectors, cyber security, data handling amongst other matters.

4. Conclusion & Recommendations

As personal information is rapidly digitised in the modern era, protecting people's privacy is more important than ever. The digital age demands a comprehensive data protection framework with safeguards on the collection, processing, transmission and storage of data as guided by data protection and privacy principles. The baseline survey revealed several key findings as summarised below:

- **Awareness**

Awareness of the Cyber and Data Protection Act was high as 93% of the respondents, across all sectors, were aware of the Cyber and Data Protection Act (Chapter 12:07) which was promulgated in 2021. However, 13% of those who were aware of the Act were unaware of POTRAZ`s designation as the Data Protection Authority in Zimbabwe.

Processing of Personal Information

Insights from the survey supported the application of the Act across sectors as well as the need for extensive enforcement. 99% of organisations within the identified sectors confirmed their processing of one or more of the categories of 'personal information' as specified in Cyber and Data Protection Act Chapter 12:07; and 84% of the organisations also admitted to the processing of information through automated means. Most processed. The most processed personal information pertains personally identifiable data such as name, address and telephone number.

Obtaining of Consent from Data Subjects

Some organisations did not obtain consent from data subjects before the processing of personal data in violation of the Cyber and Data Protection Act Chapter 12:07. 70% and 63% of surveyed organisations confirmed that they obtained consent from data subjects before processing sensitive and non-sensitive information respectively. 23% of the organisations who claimed to obtain consent revealed that they attained consent verbally from data subjects, which is not in compliance of the Act, particularly for sensitive information.

Appointment of DPOs

62.5% organisations did not have Data Protection Officers (DPOs). Only 37.5% of organisations who processed personal information confirmed that they had appointed Data Protection Officers (DPOs). The financial services sector had the largest proportion of organisations who had appointed Data Protection Officers. 72% of the organisations without DPOs highlighted that they did not have any plans of appointing a DPO, with only 28% confirming such intentions. Furthermore, the few organisations with intentions to appoint a DPO were not in a hurry to do so. 60% expected to appoint a DPO after a period exceeding twelve (12) months. Only 7% expected to appoint a DPO within a period of three months.

Qualifications of DPOs

An analysis of the provided qualifications of the appointed Data Protection Officers from the various sectors shows that all of them were Information Technology/ Computer Science professionals holding various tertiary qualifications in Information Technology and Computer Science as well as professional certifications in Information Systems, Cyber Security & Forensics amongst others. The number of data protection certified professionals was low as only one appointed Data Protection Officer had data protection certification by the Professional Evaluation and Certification Board (PECB).

Security measures, programs and practices.

The study revealed that most organisations have never conducted a data protection impact assessment as reflected by 80% of the surveyed organisations. Most of the organisations stated that they had security practices, policies and procedures to protect personal information. For example, 95% had antivirus and malware protection software, 88% had firewalls. Moreso, 88% of the organisations had internal non-disclosure policies which prohibited unlawful access to and or disclosure of personal data.

Personal Data Retention

The study revealed that 80% of organisations, across sectors, stored personal data for periods exceeding five years and 91% of these organisations had minimum data retention periods explicitly defined in their policies.

- **Transfer of data outside the country**

The proportion of organisations that transferred data outside the country was low as only 13% of the surveyed organisations confirmed the transfer of personal data outside the country. A sector-by-sector analysis shows that the postal and courier sector, financial service sector and the NGO sector had the largest proportion of such entities. Organisations who transfer data outside the country used contracts, service level agreements, non-Disclosure agreements, and various technical security measures to ensure data protection. Some organisations particularly NGOs and those in the financial services industry cited that they followed transfer principles of the General Data Protection Regulation (GDPR) i.e., the European Union and the European Economic Area information privacy and security regulation.

- **Capacity Building**

The survey revealed that 57% of organisations provide some form of training on data protection and cyber security matters to their employees; 43% of organisations did not offer any such training to employees. The study revealed a high demand for cyber and data protection training as 93% of the surveyed organisations desired to receive cyber and data protection training from POTRAZ, the designated Data Protection Authority in Zimbabwe.

Considering these insights from the baseline survey, the following recommendations were made to POTRAZ:

- **Develop DPO Guidelines**

The Cyber and Data Protection Act Chapter 12:07 introduces an obligation of the appointment of Data Protection Officers (DPOs) by data controllers. The survey showed a lack of appreciation on the need to appoint DPOs. There is need for guidelines to assist organisations with determining whether a DPO needs to be appointed, whether they can be externally appointed, the professional qualifications or expertise a DPO should have, their tasks, their potential liability amongst other matters. The guidelines will also help DPOs in understanding the scope of their role.

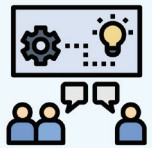
- **Pay Particular Attention to SMEs**

The Small and Medium Enterprise (SME) sector now employs over 60% of Zimbabwe's productive workforce, contributes to over 50% of GDP, and constitutes 70% of business in Zimbabwe according to the National Research and Development Survey on SMEs and Cooperatives carried out in 2019 by the Research Council of Zimbabwe. Given their sheer number and contribution, it is imperative that POTRAZ, as the Data Protection Authority, cultivates a strong relationship with them. The profile of this survey`s respondents shows that a large proportion of data controllers fit into the SME category i.e. business with less than seventy employees and with a turnover of less than US$240 000 or assets less than US$100 000 according to the Women Affairs, Community, Small and Medium Enterprises Development. A huge number of SMEs also process personal and sensitive data hence there is need for specialised trainings for SMEs, publication of guides and instructions for SMEs to help them comply and raising awareness through their associations.

- **Introduce Data Protection Self-Assessment Toolkits**

There is need to introduce digital self-assessment toolkits to help organisations individually assess their compliance with the Cyber and Data Protection Act (Chapter 12:07). The toolkit will help organisations by providing information on compliance gaps and remedies they need to employ make sure the data in their custody is protected and secure. Self-Assessment Toolkits will be a great tool for self-audits, making sure data controllers constantly evaluate their policies, procedures and training.

- **Conduct Implementation Workshops**



The survey revealed that the lack of understanding of the Act is not restricted to private organisations, even some government agencies are found wanting. There may be need for Cyber and Data Protection Act Implementation Workshops targeting business enterprises as well as the public sector. The aim is to sensitise and assure organisations on the impact of the Act, how it can be implemented in a way that enables growth and innovation in business and delivery of public services, new obligations brought about by the Act amongst other issues.

- **Adopt a Fiduciary Model of Data Protection**

The survey revealed that data controllers collect a lot of personal data and retain data for long periods of time. This purports a form of information capitalism, showing information dependence by data controllers and increased vulnerability of data subjects. This creates asymmetry between data subjects and data controllers in terms of information, transparency, power and control. The law recognizes fiduciary relationships for precisely these kinds of situations. As information fiduciaries, data controllers must be obligated with three duties toward their end users: a duty of confidentiality, a duty of care, and a duty of loyalty. They must be held to a strict standard of conduct, and any slight abrogation from the standard constitutes a breach of the duty, attracting penalties. Principles of legitimate interest, based on necessity and proportionality, should also be enforced as the lawful basis for processing of data.

- **Train, Train and Train again**

The findings from this research support the need to have comprehensive and consistent cyber and data protection training. A study by the International Business Machines Corporation (IBM) also revealed that by 95% of cyber security breaches are attributable to human error; hence, if human error was eliminated, 19 out of 20 cyber breaches may not take place at all! POTRAZ as the Data Protection Authority should facilitate training of organisations, directly and indirectly, to improve levels of cyber and data protection. There is a lot of appetite for training as 92% of surveyed organisations were eager to be trained by POTRAZ.

Annexure: Survey Questionnaire

POTRAZ Data Controller Assessment Survey

Questionnaire

JOB NO....

INTRODUCTION

1. The Cyber and Data Protection Act [Chapter 12:07] was promulgated in 2021; The object of this Act is to increase cyber security in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects.
2. The Postal and Telecommunications Regulatory Authority is the designated Data Protection Authority in Zimbabwe, according to the Cyber and Data Protection Act [Chapter 12:07].
3. This survey is intended to provide insights on data protection practices in Zimbabwe and does not constitute a compliance audit in any manner. Hence, we would appreciate your honest responses.
4. Strict Confidentiality is hereby assured.

RESPONDENT DETAILS

Name of Organisation	
Sector	
Number of employees	
Physical Address	
Email	
Contact Number	
Gender	
Completed by:	
Date completed:	

Section A: General

Q1.0 Have you ever heard of the Cyber and Data Protection Act?

YES	
NO	

IF ANSWER IS YES, CONTINUE, IF ANSWER IS NO SKIP FOLLOWING QUESTION

Q1.1 How did you get to know about the Cyber and Data Protection Act?

Radio	
TV	
Word of Mouth	
Social media	
Internet	
Newspaper	
Conferences	
Other Specify……	

Q2.0 The Postal & Telecommunications Regulatory Authority of Zimbabwe is the designated Data Protection Authority in Zimbabwe. Were you aware of this before today?

YES	
NO	

IF YES, CONTINUE TO Q6, IF NO, SKIP

Q2.1 How did you get to know about the Data Protection Authority?

Radio	
TV	
Word of Mouth	
Social media	
Internet	
Newspaper	
Conferences	
Other Specify……	

Q3.0 Does your organisation process the following types of personal information on individuals? This can be staff, clients, and other people. Tick where applicable.

NB: "Processing" refers to any operation or set of operations which are performed upon data, whether by automatic means, such as obtaining recording or holding the data or carrying out any operation or set of operations on data, including (a) organisation, adaptation or alteration of the data; (b) retrieval, consultation or use of the data; or (c) alignment, combination, blocking, erasure or destruction of the data.

	Personal Information	Yes	No
1.	A person's name, address, or telephone number;		
2.	A person's race, national or ethnic origin, colour, religious or political beliefs or associations;		
3.	A person's age, sex, sexual orientation, marital status or family status;		
4.	An identifying number, symbol or other particulars assigned to that person;		
5.	Fingerprints, blood type or inheritable characteristics;		
6.	Information about a person's health care history, including a physical or mental disability;		
7.	Information about a person's health care history, including a physical or mental disability;		
8.	Information about educational, financial, criminal or employment history;		
9.	Opinions expressed about an identifiable person;		
10.	An individual's personal views or opinions, except if they are about someone else		
11.	personal correspondence pertaining to home and family life;		

If you say NO to ALL responses above, STOP Otherwise Continue

Q3.1 Why do you hold personal information in Q1 above?

1----------2----------
----------3----------
----------4----------
----------5----------
----------6----------
----------7----------
----------8----------
----9----------10---------
----------11----------

Q4.0 Does your organisation process any of the above personal information on behalf of another?

YES	
NO	

Q5.0 Does your organisation process the following 'sensitive data' on individuals? i.e., information or any opinion about an individual which reveals or contains the following:

*Tick where applicable:

Sensitive Data	**Yes**	**No**
1. A person's name, address, or telephone number;		
2. racial or ethnic origin;		
3. political opinions;		
4. membership of a political association;		
5. religious beliefs or affiliations;		
6. philosophical beliefs;		
7. membership of a professional or trade association		
8. membership of a trade union		
9. sex life;		
10. criminal educational, financial or employment history		
11. gender, age, marital status or family status;		

If selected NO to ALL responses in the above question, SKIP following question

Q5.1 Why do you hold the "sensitive data" mentioned in Q4 above?

Q6.0 Do you obtain express consent from data subjects before the processing of:

YES	
NO	

Sensitive data

YES	
NO	

Non-Sensitive data

Q7.0 Are there provisions (policies, forms, or any other measures) in place to afford data subjects the following rights:

	YES	**NO**
Access their information in your custody;		
Correction of false or misleading personal information;		
Deletion of false or misleading data about them;		
To be informed of the use to which their personal information is to be put;		
To object to the processing of all or part of their personal information		
Consent to processing their personal information		

Q7.1 If yes kindly explain .....

.....

.....

.....

.....

Q8.0 Do you collect consent from data subjects?

YES	
NO	

Q8.1 How do you collect consent from data subjects?

Verbal	
Written	

Section B: Governance

Q9.0 Do you have a Data Protection Officer?

YES	
NO	

Q10.0 Do they have any data protection qualification?

YES	
NO	

Q10.1 If YES, kindly provide details of the type of qualification/s and awarding institution……

……

……

……

……

Q11.0 If you do not currently have a Data Protection Officer, are you planning to appoint someone?

YES	
NO	

Q11.1 If yes, when do you anticipate this taking place within?

>3 months

3>6 months

6>12 months

>12 months

Q12.0 Have you ever conducted a data protection impact assessment?

YES	
NO	

Section C: Data Practices, Policies And Procedures

Q13.0 Do you subject personal information to automated processing?

YES	
NO	

Q14.0 Do you have security policies and procedures in place?

YES	
NO	

Q14.1 If YES, do you have any of the following?

	Yes	No
Physical (lock & key)		
Physical + passwords		
Physical + passwords + encryption		
Firewalls		
Install anti-virus and malware protection		
Disaster recovery		
Other (explain)……		

Q15.0 How long do you store personal information for?

Less than 1 year	
1 to 3 years	
3 to 5 years	
5 years plus	

Q15.1 Is this in your practice, policies or procedures?

YES	
NO	

Q16.0 Have you ever experienced a data breach relating to personal information?

YES	
NO	

Q16.1 If YES, provide details on how you managed the data breach/es……..

•……
……
……

Q17.0 Do you transfer personal data to third parties outside the country?

YES	
NO	

Q17.1 Where personal data is transferred outside the country, what measures do you use to ensure adequate level of protection is ensured in the country of the recipient or within the recipient international organisation?…… ……
……
……
……
……

Section D: Data Protection Capacity Building

Q18.0 Do you have an internal non-disclosure policy that prohibits unlawful access to and/or disclosure of personal data?

YES	
NO	

Q19.0 Do the employees in your organisation receive training on data protection?

YES	
NO	

Q19.1 If so, please describe the nature of the training given, when it is given and who is responsible for carrying out the training…….. ……
……
……

Q20.0 Would you wish to be considered for the training to be conducted by the Authority?

YES	
NO	

Q20.1 What nature of training are expecting?..... ……
……
……
……
……

THANK YOU