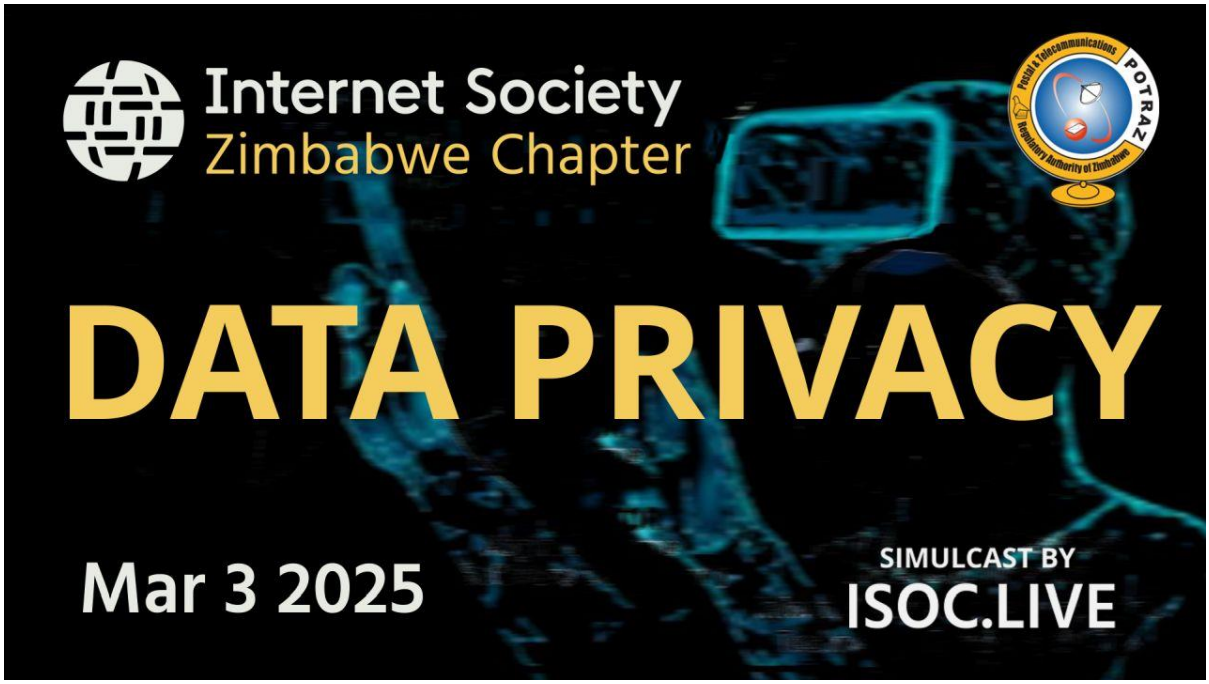

ISOC Zimbabwe - Data Privacy – March 3 2025

Prof. Vusumuzi Maphosa - NUST: Good afternoon colleagues. My name is Vusumuzi Maphosa. I'm the Director of IT at NUST and I'm in Cyber Security Data Protection Privacy Advocacy. I'll be sharing a few tips with you. Thank you.

Abgirl Chigume: Thank you very much, Professor.

For now we have Professor and our representatives from POTRAZ. They'll join us very soon so we can dive right in. Professor, I'll start with you. To set the stage, could you briefly explain what data privacy means and why it's so important in today's digital world, particularly for Zimbabwe?

Prof. Vusumuzi Maphosa - NUST: Thank you. Thank you. Thank you so much. Data has become so pivotal in the fourth industrial revolution and its access determines wealth. It has become the oil of the fourth industrial revolution. If you check top billionaires in the world, I think 70% of the top 10 billionaires in the world, they are in the internet.

Data is now very key and it drives the fourth industrial revolution. Yet, human rights also are now very, very key, especially in protecting private information, sensitive information about individuals. We need to strike a balance between harnessing that data for industrial development and also respecting the privacy and rights of individuals.

Abgirl Chigume: Thank you very much, Professor, on emphasizing on the need for data, since we are in the industrial revolution for technology. I'll get back to you with another question again. What are some of the current trends in data privacy that organizations should be aware of?

Prof. Vusumuzi Maphosa - NUST: Thank you so much for that question, Abigirl. Organizations are supposed to be aware of the new regulatory landscape, right? We know that the government of Zimbabwe has enacted the Cyber and Data Protection Act of 2024 and the statutory instrument 155. These pieces of legislation now, they are now regulating the collection, the processing, the storage of data to ensure that we respect the rights of our data subjects.

Again, there's issues to do with artificial intelligence, which is coming in now, which is disruptive. There are technologies like deepfake, where someone can fake someone's voice, where someone can fake, even do a fake video. We have seen companies losing lots of money through deepfakes. For example, an employee was instructed through a deepfake to transfer 25 million US dollars, right? Where someone faked the CEO's voice and instructed an employee. The employee acted on that and transferred that amount of money.

Then there's another one where an employee also, there was a deepfake of the boss, where they actually fake the video of the boss and the boss called an employee and instructed them to transfer 35 million US dollars into a deepfake's account.

AI is now being used to aid all these people. It is very, very critical for us to understand that this landscape has now changed.

Again, we know that many decisions which are taking place now, they're being driven by AI. We know that AI can do hallucinations. If it has got no answer, it can just create an answer. Some people can take action based on those. It is very, very important for us to understand that.

AI is also being used for phishing attacks, all right? It's actually helping attackers to construct phishing messages, which are now very, very difficult to detect.

We also have to know that we have now adopted remote work, where workers are now working remotely at home, which means that the threat landscape is now increased. Therefore, we need to be aware of these issues.

Even ransomware attacks are now increasing. Therefore, these issues, they threaten our data privacy. We need to be aware of these issues as a nation. I'm glad that POTRAZ has developed legislation and regulations to protect individual privacy.

When people work remotely, how does companies balance between monitoring their privacy and also monitoring their work? These issues, they've come to the fore because of the current trends and organizations are supposed to be aware of these trends.

Abgirl Chigume: Thank you very much, Professor, on touching on the issues of AI, because it's one of the most current trends in Zimbabwe, and everyone is excited to use AI. But the implications and the policies, people are not yet aware. And you've got, like what you mentioned, millions of dollars are being lost due to the issue of not knowing how to use the current technologies.

Thank you very much, Mr. Maphosa.

So, we have been joined by our representatives from POTRAZ. We have Advocate Komborerai Manenji, who just joined in from POTRAZ Data Protection Department. I'm going to give them the floor to explain the data privacy and protection, before we dive into questions, so that we get to have a view and how the regulatory companies are taking it, and how we can navigate, because we've got participants from different companies, from different organizations, wanting to understand how best we can navigate.

I'll give this floor to Mr. Komborerai Manenji, who just joined in.

Thank you very much, Moderator, for the opportunity. If I get your question correctly, you want me to explain data privacy and protection and how companies are navigating compliance. Is that correct?

Advocate Komborerai Manenji - POTRAZ: Yes, yes.

Okay. When you talk about data protection and data privacy, those are two things that cannot be spoken of in the same sentence, because data privacy is a component of data protection. What I mean is that for us to have data protection, you must have what you call data security and data privacy. And if you marry the two together, you then get what you call data protection.

Advocate Komborerai Manenji - POTRAZ: In other words, data protection refers to the systems and the laws and the policies that are put in place to safeguard the processing of personal information. And in line with POTRAZ, you may understand that data protection is regulated through the Cyber and Data Protection Act, 2024.

Instead of navigating compliance, compliance and data protection involves a lot of things. It's something that can be done in a day, or it's something that can be done in a month. It's a lot of work that is involved. But for now, if you read Cyber Act 2024, you understand that there are two main things that companies are supposed to come up with.

The first thing that they're supposed to appoint what you call a data protection officer, who is an individual who is charged with the responsibility of ensuring that an organization is compliant to data protection. And they were supposed to have appointed all the companies by the 12th of December, 2024.

And then the second issue is that companies are supposed to apply for what you call a data controller license. And they're supposed to apply for this license by the 12th of March, 2024, which is only about nine days away from today.

Now, if you apply for a data controller license, we say that the only companies that we have their license approved are those companies that have a licensed or a certified and a trained data protection officer. For that to happen, you also have your DPO licensed and trained.

Now, what is a data controller? A data controller is a person or a company that determines the means of processing personal information. In other words, if a person walks through the gates of your company or through the doors of your company, and you say to them, we want this type of information, those are the only people that are, those are the people that you call a data controller. That will be my answer for now.

And I see that you're recording. You didn't get my concern before you recorded.

For the video, we actually tell our members that we are going to be recording the video. We have asked them before and then we have, that's how we record.

That part I understand. It's okay.

Abgirl Chigume: The next question is how do laws, data protection act and the impact on data privacy practices in Zimbabwe?

Advocate Komborerai Manenji - POTRAZ: I'm not really sure on how to respond to that question, because I don't see that is if the laws do affect data protection in any way.

In actual effect, what I understand is that the current legal framework is a step towards protecting and promoting data protection in Zimbabwe where it's calling upon the lawful processing of personal information of every information that is collected from citizens and data subjects under the law.

For instance, when you talk about processing, we're talking about collection, storing, sharing, and any use of information to be part of, it should be lawful. The law provides, for example, you must have consent or where you cannot seek consent, there are other lawful ways that are applicable to a data subject like contractual obligation, legal obligation.

The law is actually trying to put safeguards around the processing of information to promote data protection. If you then say it affects data protection, then I'm not sure how to answer that question, because like I'm saying, from where I'm sitting, the law is actually in a bid to promote the processing of personal information in Zimbabwe. That would be my answer to that one.

Abgirl Chigume: Okay. Thank you so much, Advocate. I'll give this question to Professor Maphosa. What technologies can help to enhance the data protection and privacy for organizations, since we are talking about organizations so far?

Prof. Vusumuzi Maphosa - NUST: Thank you, Abigirl, for that question. What I can say is that before we deploy technologies, we need to have policies in place. These policies define how we're going to govern data privacy issues.

Again, when organizations are acquiring new technologies or developing new systems, they must consider concepts like privacy by default and privacy by design, meaning that at developmental stage, at acquisition stage, these systems already have privacy in them. Because it is difficult to just acquire some technology, which does not respect privacy issues and expect to change it later.

At the onset, we need to have technologies which have a privacy-embedded data protection embedded in them. There are several organizational and technical measures that organizations can adopt to enhance data protection.

For example, we can start with physical security. Premises where we process this data must be secure. We can have firewalls that prevent unauthorized access. Again, we can have backups to ensure that if anything happens, we have a backup. Because if data is lost, the person who is prejudiced is the data subject. All right. We need to have backups so that if anything happens to that data, if there's a natural disaster, we're able to recover.

Then one thing again, we need to comply with the laws of the land. We need to comply with the Cyber and Data Protection Act. All right. I think the advocate has also highlighted that we need to get licensed. We need to have a DPO.

Then we need to implement technologies like multi-factor authentication, where if someone is accessing a particular resource in our network, we can prove that that person is really who they say they are. We can also have access control, where we restrict access to data because this data could be sensitive data, which if disclosed, individuals can be at risk.

Abgirl Chigume: We can also do role-based access, where for you to access a particular resource, it has to match or align with your role. Then the other thing that we can do is if that data is accessed by someone who's not authorized, they may not be able to make

sense or identify the data subject whose data is about. These are some of the technologies that we can use to enhance data protection. Thank you, Abigirl.

Thank you very much, Professor.

Abgirl Chigume: Advocate, coming back to you, since you talked about us having the data protection officer who is now processing the personal data for individuals. My question to you is, how can individuals better protect their own data privacy online?

Advocate Komborerai Manenji - POTRAZ: Thank you very much. For individuals to be able to protect their own data online, there are very few steps that you need to do. The first thing is that we are in the habit, as data subjects, myself included, that when we go online, we always sign up to sites that we do not understand, or to sites that force us to give our information so that we can be able to access the service, which is not something that you're supposed to do.

For example, you go online and then the site is asking that, can we have your information? Or they say, are we going to be sharing your data with other third parties? Obviously, because sometimes you are desperate to get the service, you're going to agree to the terms and conditions of you giving your information, but sometimes you agree without even understanding who are the third parties who are supposed to, who are going to receive your information.

Now, in data protection we say that, before you tell a data subject that you're going to share the information with third parties, you must define who the third parties are to the data subject under their right to be informed. The first thing is that data subjects do not sign up for anything that you don't understand. If it's possible, seek legal advice and clarification.

The second thing is that always read the terms and conditions of these services that you employ, either physically or even online, and it's your right as a data subject to ask. That also brings another issue that data subjects must be in a habit of understanding their own rights and obligations.

For example, with the right to be informed, they say that before your information is collected, you must be informed of why your information is needed, what information will be used, and who needs your information at that particular time, and who needs your information at that particular time. It's your right that you must enjoy under the law, and no one must take that away from you.

Advocate Komborerai Manenji - POTRAZ: The second is that you must know that you have the right to say you consent to something or you don't consent to something, and it's within your obligation. No one should force the data subject to consent to giving out their information.

The last thing is that they also just must understand the law. The law mainly holds data controllers accountable, but , now if you don't understand that law, how are you able to enforce your own rights under that law? You must understand your rights under the law so as to be able to defend yourself and to protect yourself better as a citizen.

Abgirl Chigume: Thank you so much, Advocate.

On the data controlling part, it's very true, because for other users, even for the ISP providers that we have in Zimbabwe, you just see a message just popping up from an anonymous user, and you don't know who gave that person your number, even your details.

Prof. Vusumuzi Maphosa - NUST: I think I'll move on to Professor Maphosa to say, what practices should organizations adopt to minimize the data they collect and retain?

Thank you so much Abigirl for that question. Organizations are encouraged to collect only data which is necessary for a specific purpose. This reduces the risk of exposure to data subjects.

Prof. Vusumuzi Maphosa - NUST: As the Advocate has said, data controllers by law are supposed to appoint a data protection officer, and the role of the data protection officer is to conduct or oversee the conducting of a data protection impact assessment and also a record of processing activities.

What these frameworks do, they help the organizations to identify the lawful basis for collecting that data. By law, we're not just supposed to collect data if we've got no legal basis, lawful ground for collecting that data. And by conducting those two frameworks, we can identify risks inherent to data subjects in case that data is exposed.

These documents are very, very critical. Number two, we need to simplify our forms again to ensure that we only collect what is essential about our customers, about students, so that in case there is a breach, they are not exposed.

Number three, we need to also train employees on data minimization. I've noted in Zimbabwe that right now, it's a norm that if you lose your national ID, if you lose your passport, you can find it on a public space being displayed. Already, your rights as a data subject are being violated.

We need to train people so they understand. Even in offices that we visit, there is over-collection of data, which is not necessary. If that data is exposed, you as a data subject, you're going to be at risk.

Again, we need to follow industry-based practices and regulatory frameworks. We've got our own CDPA that we need to follow to the dot, and also other frameworks like the

ISO 27701. These are some of the things or practices that organizations can adopt to also minimize data.

Again, in terms of storage, if you are done with a particular service that you're providing, what is the purpose of keeping a data subject's data beyond that period? You are doing a survey. The survey is done. Why must we keep that data? Because by keeping that data beyond that necessary time, you are exposing your data subject.

I think what I can say is that data minimization really is respecting the rights of the data subject to ensure that you just collect just enough for you to process, not more than enough. Because if you collect more than enough, if there is a data breach, then you're exposing the data subjects. Thank you.

Advocate Komborerai Manenji - POTRAZ: Thank you very much, Professor, for answering that question for us. For the next question, I will give it to Advocate. We are looking at the AI. We now have organizations using the data to train models because we now have artificial intelligence in our markets. How can organizations ensure that they use the personal data in an ethical way?

Thank you very much. The answer to that is very simple. Ethics are a matter of principle or rather also a matter of law or a matter of police. Now that we've got the law in Zimbabwe that says the data is supposed to be processed in such a way, for an organization to say that they're processing data ethically, they need to follow what the law says.

Advocate Komborerai Manenji - POTRAZ: If you read section 10, section 11, section 12, and section 13 of the Act, it provides for the lawful basis of processing data in Zimbabwe. If you want to use my information to train an AI model, you need to seek my consent. That's what the law says. Or maybe if there's a law of general application that says that this is supposed to be done, then you can do that.

Also, it's a matter of protection. If you're going to use someone's innovation, someone's writings to train an AI, then it becomes a question of intellectual property. There's always a law that is provided in our jurisdiction. For it to be ethical, just follow the law. What does the law say? You stick to the law, then you're ethical.

Abgirl Chigume: Otherwise, when you do that, you're unethical, and you may issue a suspension so that you're unable to process any information, personal information, because of your failure to follow the law. Also, be reminded that the Act itself provides for some criminal sanctions where you don't follow the law in processing the data. In a nutshell, I'm saying to process the data ethically, follow the law.

Advocate Komborerai Manenji - POTRAZ: Okay, okay. Thank you very much, Advocate. We've got questions from the chat coming in, so I'll just pick any. There's a

question, I'll direct it to you, Advocate. It's saying, does the authority approve globally certified people, for example, PECB, which are globally recognized, assuming certifying should go beyond borders. Is content in use in their curriculum? He's saying it's generally GDPR.

No, we don't approve that one. The only certification that we are approving is when you are trained and certified by POTRAZ and Directors of Technology, because it's a certification that is customized for the Zimbabwean setup.

Advocate Komborerai Manenji - POTRAZ: The other people, we have come with international certifications, and they know that they actually failed the course, not because we are failing them, but because someone comes in and says, I've done GDPR, but because there are always those differences between the GDPR and our own law, you find that sometimes the application is different.

I'll give an example. You understand that, for example, there's a right against automated decision making. In GDPR, it says that if you are automated 100 percent, if your automation makes decisions, always be ready to provide for human intervention after the subject complains. In Zimbabwe, that's not the position. It says that whenever there's an automation, there should be a human intervention at every stage of the automation.

So, obviously, it seems to someone who's just reading, we'll see that it's the same right that's been provided for in both the GDPR and in Zimbabwe, but now the application to the extent that the right is being used is different.

So, for that reason, we want the people who are going to be appointed as data protection officers to be certified of the Zimbabwean certification, so that they can practice according to our interpretation as the Zimbabwean authority.

Abgirl Chigume: How many DPOs are necessary? Like, for example, you have one organization with many entities or branches.

Advocate Komborerai Manenji - POTRAZ: It depends with the amount of work that is involved. You as an organization, you've got the duty to understand, to say that we've got 10 entities and this is the amount of work that's then you can appoint either one or two. So, there's no limitation. It's up to the organization, depending on the scope of work and the amount of work that they need done.

Abgirl Chigume: Thank you so much, Advocate. I'll come back to Professor. Professor, with the rise of AI and machine learning, how should organizations approach data privacy?

Prof. Vusumuzi Maphosa - NUST: Thank you so much, Abigirl. Organizations are supposed to adopt privacy by design when developing their AI algorithms.

As the advocate has said, AI algorithms work on a black box, where they do not provide an explanation on how they arrived at their decision. AI algorithms generally do not provide an explanation on how they arrived at a particular decision.

So, this has to be aligned, I think, with the laws of the country because you need to explain why you reached that decision, especially when it involves profiling individuals. You can't deny someone a loan or a service because you used an AI algorithm. You need to explain so that the person understands.

We also have to secure our AI models. These can be attacked, so we need to secure them. They can be poisoned, which can result in severe data breaches.

We need to also obtain explicit consent from individuals. We have to communicate how their data will be used in AI systems and they have to consent and also provide them an option to opt out. So, data subjects can opt out at any moment of data processing or data collection if they feel so, right?

We also have to monitor for bias and fairness. Many of these AI algorithms have got inbuilt biases primarily because of the data that they were used to train with. So, we need to ensure that there are no biases which can violate human rights and privacy and data privacy rights.

So, again, these AI algorithms and machine learning algorithms are now increasing the threat landscape, right? They are providing threat actors with tools to develop malware, to develop phishing attacks. So, we must be aware as an organization of these threats.

I have a feeling that these free chatbots that we're using are collecting data from us without our consent. So, these are some of the issues that we need to look at and also provide privacy notices so that users are aware what data is being collected and for what purposes.

Again, there's the use of third parties. We need to ensure that the third parties that we're using in our AI ecosystem, the vendors that we're using, they understand organizational privacy standards, right?

Abgirl Chigume: Then the last one, we must always anonymize, pseudonymize, and mask to remove personally identifiable information so that this information is not attributable to particular individuals as we train our AI algorithms. Thank you so much, Abigirl.

Advocate Komborerai Manenji - POTRAZ: Okay. Thank you very much, Professor, for that insight. I'll come back to advocate looking at our time. What do you foresee as the future of data privacy in Zimbabwe and globally?

I mean, it's simple. The future of data protection in Zimbabwe, and globally, is that you tend to end up having more and more regulations around data protection, including the regulation and governance of the use of artificial intelligence in our own countries.

Advocate Komborerai Manenji - POTRAZ: It's an interesting future, if I must put it that way, because if you look at the trends, we are at a time where we're having more DPIAs. We're at a stage where we were without the laws, but the laws, if you look at them, they may not be that sufficient enough.

Sometimes, you end up at a stage where you need to do more to safeguard personal information, and you also get to a point whereby data protection may become sector-specific, so that you may have data protection rules for the health sector, data protection rules for the finance sector. It will become sector-specific depending on the country, and the way it's going.

We're moving towards more and more regulations. But it will be interesting because countries like the U.S. with President Trump and J.D. Vance, who are anti-regulation, are trying to make it loosen up a bit. But it will be interesting to see how that balances out with those countries.

Advocate Komborerai Manenji - POTRAZ: But as you can see, more countries are leaning towards adopting more regulations that protect the future of data protection, because the issue there is that, is the future of innovation safe if there are more regulations around data protection? Because for there to be innovation, people need to work with data sets, and they're unable to do that if there is no personal information.

It's interesting to see that. I believe that we have to have more regulations, but of course, you see that the wave of Donald Trump and J.D. Vance will sweep across the country. That will be my answer.

Abgirl Chigume: Okay. Thank you. Thank you very much, Advocate, for that answer. Now, we can turn to our audience. If you have questions, we'll take a few questions from the chat. Already, I think we have a few questions from people.

Okay. We have someone who's asking, will compliance be affordable for small players? We handle much data since DPO training costs about 1.4K. Aren't we going to have only the big players complying?

Advocate Komborerai Manenji - POTRAZ: Yes, it can be affordable, because the small companies are allowed to come together, and have possibly one DPO who can help

them navigate. They can form an association, or a corporation, or a cooperative of small companies, so as to come up with the issue of doing compliance.

Unfortunately, I understand that the cost may be too high, but if you're a small company, and you're dealing with much data, it means that you are putting a lot of people at risk by being a small company with so much information. Obviously, we need to protect the information of people, because as you can see, data is the new gold.

And then, the other question, they say, can the authority engage academics to collaborate with IT security, global boards, and enable them to drive the situation, make it affordable, even encourage students to undergo such IT, comp science?

Advocate Komborerai Manenji - POTRAZ: I think we are going to have more collaborations, more universities, but it would be an injustice to make this only partnership with IT bodies, because this is not an IT course, as they say. It's a course that cuts across many institutions, so it should be necessary for us just to try and have a neutral programme that's not relegated to a specific body of professionals, because it would then be exclusionary to other boards of professionals.

And then, the first is currently the access levels are different, and many people include those in customer care. How will they be trained as well as they have access to massive information at the times when they're not technical?

Exactly, that's why my point number three, to say that it won't be fair to ask to partner up with one institution, because many people have, but for this course, we are training anyone, those in customer care, those in law, those in IT, anyone who wants to raise a first degree or relevant work experience can apply and get trained, or those in customer care, the associations themselves, they can invite us to do workshops and training, so you can send their professionals under their bodies.

And then, how can I ensure that everything is secured when I'm using it?

I I would refer the question to Prof, to answer this question.

Prof. Vusumuzi Maphosa - NUST: Thank you so much, Advocate. I think when you're using ChatGPT, avoid disclosing or sharing personal information, because as I said earlier, these free platforms are collecting this data without our consent.

Abgirl Chigume: So, obviously, if you share your personal information, ChatGPT is going to record that information and use it for training its model. So, avoid, always anonymize if you are to share any information with these platforms.

Prof. Vusumuzi Maphosa - NUST: Okay, thank you so much, Prof. Prof, I'll come back with another question. What are some of the misconceptions about data privacy that you'd like to debunk?

Thank you so much, Abigirl. Once again, the first one is that data privacy is data security. So, you can achieve data security, but not achieve data privacy. For example, your data may be secure. You've applied organizational and technical measures to protect your data. But if you have not established a lawful basis for collecting that data, you are not practicing purpose limitation and storage limitation already in breach of data privacy.

Prof. Vusumuzi Maphosa - NUST: Okay, number two, another misconception is that if you have got your other professional certifications, you can practice as a data protection officer. So, according to the Act, you are supposed to be certified by POTRAZ for you to practice as a data protection officer.

The other myth, people believe that by deleting their data, their data is gone. Unfortunately, you can delete your data, and people can apply technologies to recover that data. The most secure way of deleting your data is actually shredding your hard drives, all right? I know many companies dispose their computers. After a while, you must be aware that just by deleting data may not go away.

Another misconception is that data privacy is solely the responsibility of the IT department. This is a misconception. Data privacy is a cross-functional responsibility that involves your legal department, marketing department, IT, and other departments within the organization. Everyone has a role in protecting data and ensuring data privacy. These are the few misconceptions I can pick up because of our time.

Abgirl Chigume: Thank you very much, Professor, for this insight.

This has been an incredible, insightful discussion. I want to extend my deepest thanks to our panelists, Advocate, and Professor Maphosa for sharing their expertise and also getting to learn that this is a collective responsibility, whether you're a policymaker, a business owner, or an individual.

And also, I'm sure organizations are going to look into what Advocate has said, that by the 12th of December 2025, all companies should have, either collectively as small companies, they should have a data protection.

Advocate Komborerai Manenji - POTRAZ: Sorry, I think I said the DPO was the 12th of December 2024, and the licensing is the 12th of March 2025.

Abgirl Chigume: Yes, the data protection license is supposed to be there by the 12th of March 2025. And then the office is supposed to be appointed by the 12th of December 2025.

Prof. Vusumuzi Maphosa - NUST: Okay. Thank you very much, Advocate, for that contribution.

Abgirl Chigume: Sorry. I'm a student of the Advocate. If I don't correct that, you won't be happy. Organizations are required to have appointed a DPO by the 12th of March 2025, not December.

Advocate Komborerai Manenji - POTRAZ: Okay. Thank you very much, Professor. Any last words before we close from the Advocate or Professor Maphosa?

Abgirl Chigume: No I have no words except to say that do the needful and be compliant.

Prof. Vusumuzi Maphosa - NUST: Okay, thank you so much. Prof, do you have any last words to say?

I think what I can say is that we're grateful to what POTRAZ has done to ensure that organizations comply with these regulations to ensure that human rights, human dignity is upheld and respected as we collect and process our personal information. And I hope the audience learned something from this conversation.

Abgirl Chigume: Thank you very much, Professor. And to everyone who joined us today, thank you very much for joining us. And let's continue learning and advocating and taking action to protect our privacy. Thank you so much for this webinar.

Prof. Vusumuzi Maphosa - NUST: Thank you, Abigirl.