Regulatory Alert

Data Protection in the Insurance Industry

April 2021

Contact us

Joseph Githaiga
Associate Director
Regulatory Compliance & Advisory
joseph.githaiga@pwc.com

Christopher Ndegwa
Senior Associate
Regulatory Compliance & Advisory
christopher.n.ndegwa@pwc.com

Jehaan Ara Kurji
Senior Associate
Regulatory Compliance & Advisory
jehaan.kassam@pwc.com

Charles Owino
Associate
Regulatory Compliance & Advisory
charles.owino@pwc.com

The Kenyan Data Protection Act 2019 (the "DPA") came into effect on 25th November 2019. It governs the processing of personal data, which is defined as data relating to an identified or identifiable natural person (the "data subject").

The DPA establishes a regulator, the Office of the Data Protection Commissioner ("ODPC") headed by the Data Protection Commissioner ("DPC"), to oversee the implementation and enforcement of the law. The ODPC has recently released draft regulations for public participation, which, once finalized, will supplement the DPA.

The DPA adds to the guidelines and regulations published by the Insurance Regulatory Authority (the "IRA") in relation to data privacy, particularly the Guideline on Market Conduct for Insurers (IRA/PG/18) and the Insurance Market Conduct Guidelines for Insurance Intermediaries.

The processing of personal data is at the heart of insurance underwriting and as such, the insurance sector will be significantly impacted by the DPA and subsidiary regulations. Some of the key considerations for insurance companies arising from this law are set out below.

Key considerations in the Insurance Sector

1. Processing of Personal Data

Personal data is critical to the underwriting process, allowing for more accurate pricing of risk in most categories of insurance. The processing of the data itself, however, is restricted under the DPA to certain lawful bases and the collection limited to only what is necessary for the purpose justifying the collection.

As such, insurance companies will need to assess the personal data they hold and ensure that it is being processed in accordance with the principles set out in the DPA.

2. Special Categories of Personal Data

Sensitive Personal Data such as health data, biometric data, genetic data, property details and family details must be processed under very strict conditions. The processing of health data is particularly prohibited unless the data is being processed by or under the responsibility of a healthcare provider or by a person subject to the obligation of professional secrecy under the law.

Insurance companies will have to carefully consider the processing of children's data which is prohibited unless consent is granted by the child's parent or guardian and the processing is in a manner that advances the rights and best interests of the child.

This Legal Alert has been prepared by the Regulatory Compliance & Advisory team at PwC. The RCA team is composed of qualified advocates with experience in advising on corporate / commercial legal matters gained from Tier 1 institutions and corporate law firms.

3. Automated Decision Making

The insurance industry relies on the profiling of the potential policyholders in making the decision on whether or not to underwrite the client or their business. The use of fully automated decision making such as profiling is restricted where it has legal or other significant effects on the data subject. As such, care must be taken in designing the systems and processes to ensure that the ultimate decision shall always be reviewed by a natural person. Where automated decision making is inevitable, companies are required to notify the data subjects, who retain the right to request for a review of the decision by a natural person.

4. Relationships with Third Parties

The business of insurance ordinarily involves a number of different third parties such as intermediaries, investigators – most of whom will hold personal data relating to the insured. Insurers will need to ensure that there are contracts in place, clearly setting out the relationships between the parties and providing specific processing instructions.

5. Right to Erasure

The DPA gives data subjects the right to have their personal data erased by the insurer where the insurer is no longer authorised to retain the data or where it is irrelevant, excessive or obtained unlawfully. There is, however, an exception provided for data that is needed for evidentiary purposes which insurers need to factor into their system design as such data ought to be retained but access to it restricted.

6. Access to Data

Insured persons, as data subjects, are entitled to access any of their personal data that is held by insurers free of charge. In addition, they are entitled to receive any of their personal data in a commonly used and machine-readable format for transmission to other data controllers.

These requirements shall require insurers (and intermediaries) to design systems that will allow for ease of access and information standards that will allow for data portability.

7. Marketing

Digital and electronic marketing is a tool that has been used to great effect in recent times. One of the keys to the success of digital marketing has been the level of personalisation that can be achieved in a message, due to a mix of data analytics and access to personal information.

The DPA requires that companies have “data protection by default”, which in effect requires that the data subjects opt into marketing material, as opposed to having to opt out of unsolicited messages. This has to be considered when designing marketing campaigns for insurance products. In addition, there is a general prohibition on the use of personal data for commercial purposes such as direct marketing, unless the person has sought and obtained express consent from the data subject or is authorised to do so by law. The data subject must also be informed of such uses when the data is being collected.

8. Transfer of Data Outside Kenya

Insurance companies need to be mindful of any transfer of personal data to other countries as it is generally prohibited unless the data controller or data processor provides proof of appropriate safeguards with regard to security and protection of data.

9. Liability for Misuse of Personal Data

Insurers and brokers will likely be considered to be data controllers under the DPA and thus have an obligation to protect the personal data of subjects. Agents and third-party services such as cloud services will also have an obligation to protect the personal data they handle as data processors.

How Can PwC Help?

The ODPC has recently published discussion drafts of Regulations to the Act. Given the pace at which the ODPC is moving in executing its mandate, organisations should be prioritising gap assessments on their risk exposures. Our RCA’s Data Privacy Team can assist you by undertaking a data protection gap assessment to evaluate your readiness for compliance with the Act and preparing an implementation road map.

Please feel free to reach out to our Data Privacy Team whose contacts are listed herein for further details.

In assessing your data protection preparedness, some key questions for insurance companies arising from the Act are set out below:

Key considerations in the Insurance Sector

1. **Processing of Personal Data**

   Do you have a lawful basis for the processing of the personal data you handle?

   Is your data processing aligned with the principles of data protection?

2. **Special Categories of Personal Data**

   Do you process health data, biometric data, genetic data, property details or family details?

   The consent of a parent or guardian is mandatory prior to processing a child's personal data. Has this been sought?

3. **Profiling**

   Is any decision-making process fully automated (computer-generated)?

   If so, are Clients notified of such automated decision-making processes?

4. **Relationships with Third Parties**

   Do you have contracts with all third parties who handle personal data?

   Has your relationship and information flow been properly defined within the contracts?

   Have you considered any joint or vicarious liability for mishandling of data privacy by third parties?

5. **Right to Erasure**

   Do you have provisions to take requests for erasure of personal data?

   Do you provide written reasons when denying such requests?

6. **Access to Data**

   Do you have mechanisms for allowing Clients access to their personal data?

   Are there categories of personal data you cannot allow access to?

7. **Marketing**

   Do you use personal data in your digital marketing?

   Are your marketing messages unsolicited?

   If your messages are requested for, is there an option to opt out of the marketing messages?

8. **Transfer of Data Outside Kenya**

   Do you transfer data outside Kenya (consider cloud servers too)?

   Do you have the consent of the Client to transfer data outside Kenya?

   Are you assured of the data privacy and information security safeguards in the receiving countries?