Drastic times call for drastic measures

The impact of data privacy legislation on research buyers’ operating environment

Prepared by Kudzai Guvi
Kudzai.Guvi@standardbank.co.za
Today’s agenda

1. What got us here?
2. What are we experiencing?
3. How do we solve this?
4. Where to from here?
Why we have data privacy laws?

Purpose of Protection of Personal Information Act

- Protect people (data subjects) from harm by protecting their personal information
- To stop their money being stolen
- To stop their identity being stolen, and
- Generally to protect their privacy, which is a fundamental human right

Impacted entities

- Any natural or juristic (entities) person who processes personal information, including large corporates and government

Lawful                               Fair
Transparent processing               
Limitation of purpose                
Data subject rights                 Consent
Data transfers                       
                                      safeguard

Source: The Protection of Personal Information Act 2013. Act No.4
What are the privacy legislative challenges that market research clients in the banking industry are facing?

What is the impact of these privacy legislative challenges on market research clients’ ways of working?

To what extent, if at all, are these challenges influencing their operating models, including processes, survey design, timings and other related elements?

How can research agencies better assist or partner with clients in seeking to overcome the identified challenges?
To fulfil the objectives of the study a mixed quali-quant framework was adopted.

- 10 locally controlled banks
- 7 foreign controlled banks
- 3 mutual banks
- 2 co-operative banks
+ numerous representative offices

Focus was placed on the biggest retail banks (*85% of total bank assets)

- 9 fellow market research professionals (senior and middle management who deal with data privacy issues)
+ 2 senior researchers on agency side

*Source: Banking Association of South Africa 2017 Annual Report*
Data privacy legislation has become of paramount importance.

Importance placed on data privacy legislation:
- To a large extent
- To some extent
- Not at all

Impact on the operational environment:
- To a large extent
- To some extent
- Not at all
driven by the need to be fit-for-purpose, compliance and reputation management

Drivers of focus on data privacy legislation

- Ensure department is fit for tomorrow's digital economy
- Comply with increasingly complex local regulations
- Risk of reputational damage in case of privacy incidents
- Opportunity to harness value of your data
- Opportunity to improve data quality
- Comply with increasingly complex global regulations
- The ability of regulators to impose fines
- The opportunity to transform your approach to privacy
- Privacy is not on the agenda
This has led to the implementation of several initiatives internally due to data privacy legislation.

**Initiatives implemented due to data privacy legislation**

**High**
- Changed protocols or procedures around data
- Gained knowledge of the personal data protection environment and trends
- Formulated or been involved in the creation of a data governance framework
- Sought external guidance from industry bodies, consultants, etc.
- Promoted collaboration among Research and IT, Compliance, Legal and similar business areas
- Organised training or briefings for team members
- Privacy-by-design programmes where Privacy Impact Assessments (PIAs), documentation and escalation paths are in place
- Joined various steering committees e.g. Cybersecurity, Risk & Compliance, etc.
- Been assigned or recruited data protection/compliance officers

**Low**
- Appointed a privacy and security lead in your department or business area
While a number of benefits have been derived from this legislation:

- **Adherence to regulations**: Ensuring that customer data is protected and that there are no risks to the bank or the customer.

- **Respect for customers’ desires**: Increased sensitivity to customers’ concerns about how their data is handled.

- **Appropriate use of data**: Ensuring more relevant and tailored communication to targeted audiences.

**SO, IN ESSENCE, THE CUSTOMER DERIVES GREATEST BENEFIT**
there are challenges being faced in adapting to it

CHALLENGES OF DATA PRIVACY LEGISLATION

- Systems and processes
- Lack of role clarity
- Greater hands-on involvement

“Time taken to ensure processes are more rigorous in handling data.”

“There is also lack of ownership and accountability as to who is responsible for ensuring that these processes are fast tracked and fixed.”

“More hands on management of how our suppliers handle data.”

A COMBINATION OF INTERNAL AND EXTERNAL CHALLENGES
with the research elements that have experienced the greatest impact being data handling, sharing and disposal.

**Impact of identified challenges on research elements**

<table>
<thead>
<tr>
<th>Research element</th>
<th>Not at all</th>
<th>To some extent</th>
<th>To a large extent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research supplier selection</td>
<td>2</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Survey design and content</td>
<td>0</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>Usage of creative/innovative methodologies</td>
<td>0</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Data collection</td>
<td>2</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Data handling and storage</td>
<td>0</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Data sharing or transfers</td>
<td>0</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>Data disposal</td>
<td>0</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>Research process timings</td>
<td>5</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Research output quality</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Internal client engagement and relationships</td>
<td>2</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>
While there is positive sentiment towards some research agencies’ adoption of the legislation

**IDENTIFIED PROGRESS**

- Increased awareness and compliance

“Generally, suppliers are increasingly aware of POPI and other data privacy regulation.

“The suppliers we work with are well-informed and comply with all aspects of data privacy (which is guided by a services agreement).”
the major sentiment is that research partners have not yet cracked the code

IDENTIFIED CHALLENGES WITH AGENCIES

Lack of clear understanding of implications of data privacy legislation

"I do not think there is a good enough understanding of the legislation and how it might impact on them and us."

"There is still work that needs to happen as this practice is not across all research suppliers that we make use of. We have had incidences where these conversations had to happen with a supplier after an incident had occurred."

Lack of urgency

"This topic is not always top of mind when engaging with suppliers, which is a concern. I sometimes feel that from a client point of view that this needs to be emphasized and re-emphasized in engagements and in contracts, etc. to ensure that the relevant suppliers adhere to the relevant regulations and requirements of the bank."
which in turn results in difficulties when implementing research solutions

**IDENTIFIED CHALLENGES WITH AGENCIES**

- **Lack of agility & IT platform capabilities**

  “Approvals required from international head offices to implement systems in South Africa, which is time consuming and requires multiple conversations on the requirements.”

  “Lack of IT capabilities to create solutions required.”

- **Lack of full team involvement**

  “Lack of briefing of the full project team involved in managing customer data around the security of information when preparing data, sharing data, making corrections.”

  “Lack of awareness of the full project team on the system and its use.”
Interestingly, agencies claim to be applying data privacy legislation, highlighting some degree of misalignment between both parties.

**AGENCY FEEDBACK**

We are having to be more strict with our clients (we still get clients who email us databases of client data unencrypted despite specifying that it needs to be). We delete any data that is not in line with privacy data.

There is no change in how we interact with the banking or other clients from a research planning perspective but there are changes in the back end data collection process. When before we could share respondent details with a separate team to run back-checking this is not possible any more – only the interviewer knows who the respondent is and all back-checks are done on the basis of anonymity, save the actual responses which are not identifiers.

Actually we have been surprised that most of our clients have not been as concerned as we expected. I think they expect us to be the custodians of the protection.
As a result, the solution lies in closer collaborative efforts

**KNOWLEDGE GENERATION**

"It starts with actually being aware of regulations that are impacting the sectors they conduct research in. Proactively demonstrate that initiatives are being implemented to address regulatory requirements."

**PROACTIVENESS**

"Proactively managing the solution process. Removing internal barriers to drive outcomes. Clients are incurring enormous costs for suppliers to implement solutions under the pretence that it is unique to the client, which indicates there is a lack of interest and devoid from the real world."

**CLOSER WORKING RELATIONSHIPS**

"The key to success is transparency, clear communication and a close and open working relationship between agencies and companies commissioning research."
This implies that new and modified practices are recommended, that if created jointly, will benefit both parties.

3 key aspects are recommended:

1. IT infrastructure & compliance/risk personnel engagement
2. Solutions-oriented innovation
3. Fundamental shift in client-agency partnering
To overcome data privacy legislation challenges, **collaborative engagements** that are open and transparent will enable the development of optimal solutions and offerings.
THANK YOU!