Data Privacy and Protection: Guidance Note to Kenya’s Digital Financial Services

September 2021
The Kenya Financial Sector Deepening (FSD) programme was established by the UK’s Department for International Development (DFID) programme in 2001 to support the development of financial markets in Kenya. In 2005 we were constituted as an independent trust under the supervision of professional trustees, KPMG Kenya, with policy guidance from a Programme Investment Committee (PIC). Our aim today is to help realise a vision of an inclusive financial system to support Kenya’s goals for economic and social transformation. We work closely with government, financial services industry and other partners across key economic and social sectors. The core development partners in FSD Kenya are currently the Bill and Melinda Gates Foundation and the Swedish International Development Agency (SIDA).
# Table of Contents

**TABLE OF CONTENTS**

LIST OF FIGURES AND TABLES  
ABBREVIATIONS AND TERMINOLOGY

01 EXECUTIVE SUMMARY 1

02 FINTECH UNDERSTANDING OF THE DATA PROTECTION ACT IN KENYA 3

2.1 Survey Panel 3

2.2 What Data is Managed 4

2.3 Understanding of Legislation 4

2.4 Implementing DAPA
   2.4.1 Data Protection Officer 5
   2.4.2 Data Sharing 5
   2.4.3 Implementation of the Act 6
   2.4.4 Activities to Support Interaction with Data Subjects 7

2.5 Opportunities Presented by the Act 8

2.6 Challenges Presented by the Act 8

03 DATA PROTECTION IN A FINTECH CONTEXT 9

3.1 Data Collection and Processing Practises 9

3.2 Creating a Program for the Changes
   3.2.1 Establishing a Team 11
   3.2.2 Starting the Assessment with a Data Flow Map 12
   3.2.3 Assessing the Storage and Protection of the Data 14
   3.2.4 Building for Withdrawal of Consent 16
   3.2.5 Creating a Data Protection Impact Assessment (DPIA) 16
   3.2.6 Process for Responding to a Data Subject Access Request (DSAR) 18
   3.2.7 Implementing the Changes 18
   3.2.8 Addressing Unstructured Data 19

3.3 Balancing Consumer Protection with Managing Fraud / AML and CFT 19

3.4 Opportunities for Fintechs 20
# Table of Contents

3.5 **Digital Resources Available** 20  
3.5.1 Tools for a Delivery Program 20  
3.5.2 Data Protection Notice Generator 21  
3.5.3 Security Tools 21  
3.5.4 Open Source Tools 21  
3.5.5 Self-build Guidance for AI 22  
3.5.6 Commercial Tools 22  
3.5.7 Cloud Providers 23  

## IMPLEMENTATION EXAMPLES 25  
4.1 **Capturing Consent** 25  
4.1.1 Examples That Meet the Data Capture Consent Requirements 25  
4.1.2 Examples that Do Not Meet the Capture Consent Requirements 39  
4.2 **Managing Data Subject Requests** 47  
4.2.1 Good practises That Provide Any One of the Four Channels 47  
4.2.2 Bad practises on Managing Data Subject Requirements 55  
4.3 **Managing Complaints** 57  
4.3.1 Good Examples 57  
4.3.2 Bad Examples 57  
4.4 **Cross-border, International and / or Third Party Data Transfers** 57  
4.4.1 Good Examples 57  

## APPENDIX 1 – QUESTIONS ASKED 59
List of figures and tables

**Figures**

<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Size of Company (No. of employees)</td>
<td>3</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Types of Company</td>
<td>3</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Types of personal data processed</td>
<td>4</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Have you implemented a programme to deliver the requirements of the Act?</td>
<td>4</td>
</tr>
<tr>
<td>Figure 5</td>
<td>If yes - how long has it been running?</td>
<td>4</td>
</tr>
<tr>
<td>Figure 6</td>
<td>For those yet to recruit, is there a plan to recruit for the role?</td>
<td>4</td>
</tr>
<tr>
<td>Figure 7</td>
<td>For all – what is the expected seniority of this role or person taking responsibility for the task?</td>
<td>4</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Do you share data with other parties?</td>
<td>5</td>
</tr>
<tr>
<td>Figure 9</td>
<td>What controls do you already have in place?</td>
<td>5</td>
</tr>
<tr>
<td>Figure 10</td>
<td>Have you implemented a programme to deliver the requirements of the Act?</td>
<td>6</td>
</tr>
<tr>
<td>Figure 11</td>
<td>If yes - how long has it been running?</td>
<td>6</td>
</tr>
<tr>
<td>Figure 12</td>
<td>How do you plan to manage Data Subject Access Requests?</td>
<td>7</td>
</tr>
<tr>
<td>Figure 13</td>
<td>How are you managing your unstructured data?</td>
<td>7</td>
</tr>
<tr>
<td>Figure 14</td>
<td>Data Categories</td>
<td>12</td>
</tr>
<tr>
<td>Figure 15</td>
<td>Inventory of where data exists</td>
<td>12</td>
</tr>
<tr>
<td>Figure 16</td>
<td>Data Controls</td>
<td>13</td>
</tr>
<tr>
<td>Figure 17</td>
<td>Example of Reference to Identity data</td>
<td>14</td>
</tr>
<tr>
<td>Figure 18</td>
<td>Interactive Voice Recognition System</td>
<td>15</td>
</tr>
</tbody>
</table>

**Tables**

<table>
<thead>
<tr>
<th>Table</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>Survey Responses</td>
<td>6</td>
</tr>
<tr>
<td>Table 2</td>
<td>Data Map for Retention Analysis</td>
<td>15</td>
</tr>
<tr>
<td>Table 3</td>
<td>Risk Score</td>
<td>17</td>
</tr>
<tr>
<td>Table 4</td>
<td>Residual Risk Score</td>
<td>17</td>
</tr>
</tbody>
</table>
# Abbreviations and Terminology

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>AML</td>
<td>Anti-money Laundering</td>
</tr>
<tr>
<td>AWS</td>
<td>Amazon Web Services</td>
</tr>
<tr>
<td>CBK</td>
<td>The Central Bank of Kenya</td>
</tr>
<tr>
<td>CCPA</td>
<td>California Consumer Protection Act</td>
</tr>
<tr>
<td>CFT</td>
<td>Combating of Financing of Terrorism</td>
</tr>
<tr>
<td>CISO</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>CNIL</td>
<td>Commission Nationale Informatique &amp; Libertés</td>
</tr>
<tr>
<td>COVID-19</td>
<td>Novel coronavirus discovered in late 2019 in Wuhan, China; later renamed SARS-CoV-2</td>
</tr>
<tr>
<td>DAPA</td>
<td>Data Protection Act, 2019</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officer</td>
</tr>
<tr>
<td>FINTECH</td>
<td>Financial Technology</td>
</tr>
<tr>
<td>GDPR</td>
<td>European General Data Protection Regulation</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IVR</td>
<td>Interactive Voice Response</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>MSME</td>
<td>Micro, Small and Medium Enterprises</td>
</tr>
<tr>
<td>NAS</td>
<td>Network-Attached Storage</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OCR</td>
<td>Optical Character Recognition</td>
</tr>
<tr>
<td>PCiR DSS</td>
<td>Payment Card Industry Data Security Standard</td>
</tr>
<tr>
<td>PAIA</td>
<td>Promotion of Access to Information Act of 2000</td>
</tr>
<tr>
<td>PII</td>
<td>Personal Identifiable Information</td>
</tr>
<tr>
<td>POPIA</td>
<td>Protection of Personal Information Act</td>
</tr>
<tr>
<td>QNAP</td>
<td>Quality Network Appliance Provider</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role-Based Access Control</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SPII</td>
<td>Sensitive Personal Identifiable Information</td>
</tr>
<tr>
<td>USSD</td>
<td>Unstructured Supplementary Service Data</td>
</tr>
<tr>
<td>VAPT</td>
<td>Vulnerability Assessment and Penetration Testing</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
Chapter 1

Executive Summary

Globally, consumer services have emerged which have created a mindset of “data is the new oil” – the way to innovate & monetize offerings. Kenya’s Digital Finance Services (DFS) ecosystem is built on this premise of alternative data sources & information sharing to inform decisions, business models and monetisation models.

These enterprise-led innovations have given rise to a range of other digital offers including several mobile app-based models that provide small loans using information stored on an individual’s smart phone. Innovation around data has grown over the years to adjacencies in ride-hailing, gig worker platforms and agri-initiatives, not to mention MSME innovations around data. Such innovations have extended financial inclusion in Kenya; however, it also focuses attention on the need to address potential risks in the provision of such services in the context of data privacy and protection.

With the Data Protection Act (DAPA) in place and draft regulations published by the Data Commissioner, innovators in Kenya’s DFS space now need to think more deeply about compliance with the law that is balanced with innovation around data, just as GDPR created this conversation elsewhere globally. The conversation is already beginning on questions such as “what does good look like?”. There is an opportunity to get ahead of the game versus retroactively asking for change after breaches and enforcement issues arise. To achieve this, the DFS community need to start thinking about the practicalities of complying with the law a practical pragmatic manner while putting the customer first.

This report provides pragmatic guidance to support the practical implementation and compliance with some, not all, requirements of the law. The focus is on context specific guidance for the DFS community using themes from DAPA and the draft regulations as well as drawing from best practice in other markets.

It is likely that this guidance could be the start of a conversation with larger enterprises serving the broader customer base including banks and mobile money providers. For example, there are clauses to compel providers to share data (at the customer’s request) within 30 days. How might a company practically implement that? Are there examples of companies doing this well yet? Or are there global examples that can be used to show the way? How might those who are already exploring the use of Open APIs open the way for others, in a consent-driven manner? This report further seeks to catalyse conversations on the realities of compliance with the consumer in mind.

In developing this report, we have used feedback (through a bespoke survey) from firms working in Kenya to understand their concerns and what they are currently doing to comply with the law. This was intended to inform the areas that the guidance should focus on especially for firms that have started implementing a program to comply with the law. As part of the guidance, we have also highlighted several resources that would be beneficial – both from commercial and open-source providers. We have also showcased examples of good and bad user experiences by firms across markets.
Chapter 2

**Fintechs’ Understanding of the Data Protection Act, 2019**

A bespoke survey targeting fintechs in Kenya was undertaken to gain a clearer understanding of the challenges they were facing in understanding and implementing the Data Protection Act, 2019 (DAPA), and the steps they were taking to comply with the new legislation. The findings are highlighted below, and the survey questions are detailed in Appendix 1.

### 2.1 Survey Panel

Even though the survey distribution was small in terms of the number of respondents (not by design), the actual responses were informative enough to help provide insights and further guidance, because a good mix of firms participated, differentiated by size and commercial business lines. The survey respondents included digital lenders, aggregators, online market providers, insurance firms, mobile network operators and other fintech firms. They were also performing different roles as data controllers and processors.

**Figure 1: Size of Company (No. of employees)**

<table>
<thead>
<tr>
<th>Size of Company</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-10</td>
<td>0%</td>
</tr>
<tr>
<td>11-50</td>
<td>0%</td>
</tr>
<tr>
<td>51-250</td>
<td>30%</td>
</tr>
<tr>
<td>251-1000</td>
<td>20%</td>
</tr>
<tr>
<td>1001-5000</td>
<td>30%</td>
</tr>
</tbody>
</table>
| Greater than 5000 | 10%     

**Figure 2: Types of Company**

- Bank
- Payments Company
- Digital Lending Company
- Insurance Company
- Aggregator
- Online Market Place provider
- Other

---

1 The survey was undertaken prior to the publishing of the draft regulations under the Act.
2.2 What Data is Managed

The companies involved also deal with a broad spread of personal data types, including sensitive data as defined in DAPA. A number of the respondents used data from online sources, such as social networking, to understand the relationship with the data subject. Given the nature of the services the firms provide, capturing data to understand the customer was high on the list of reasons for data collection, followed by analysis of payment data and data subjects’ credit history.

2.3 Understanding and Awareness of the Act

The second area of knowledge we sought to understand from the respondents was their awareness of the data protection legislation generally - both from within Kenya and from those in other jurisdictions. All respondents were aware of the Kenya Data Protection Act, with a 100% positive response rate. When assessing the respondents’ awareness of other international legislation, it is clear that expansion and delivery beyond Kenya is in their current thinking, with 64% being aware of the GDPR and CCPA, and 66% of those affected also being aware that they were impacted by these regulations. This reinforces the need for the Kenyan data protection regulatory framework to be harmonised with other legislation, so that compliance with the Kenyan framework simplifies the process for those wishing to expand their offerings beyond Kenya. Such an approach would be also appealing to international firms that want to establish businesses in Kenya.
2.4 Implementing DAPA

2.4.1 Data Protection Officer

When seeking to understand how firms are ensuring that data protection is key to their digital strategy, it was disappointing to see that so far none of the respondents had appointed a Data Protection Officer (DPO) within their organisation. However, 33% of the respondents did intend to appoint a DPO: not as a dedicated role, but rather by adding the duties and responsibilities of the DPO to an existing role/employee. The expected hierarchical position of the DPO was that of a general employee, with a relatively lower level of seniority than would otherwise be ideal. The lack of seniority for such an important role portends the potential risk of diminishing the strategic focus required to ensure not just compliance but also the overall success of the business.

2.4.2 Data Sharing

Nearly all the responding parties also shared their data with other parties. For over 60% of respondents, the data subjects had been asked permission for this sharing in their contracts – all parties will need to assess that these contracts actually adhere to the new legislation. 45% of the respondents gave data subjects clear reasons for the sharing, and 45% gave general purposes for the sharing. 45% also provided the name of the partner with whom the data was shared. 18% responded without any contract request – this will need to be addressed under the new DAPA. Other reasons provided included sharing with Government agencies as part of their responsibilities, or with a party facilitating delivery of the contract.

Figure 8: Do you share data with other parties?

Figure 9: What controls do you already have in place?
2.4.3 Implementation of the Act

The majority of the respondents have started to implement some incremental changes in their business processes to comply with the requirements of the Act. However, only 33% of the respondents have a specific and dedicated internal project aimed at implementing the provisions of the Act. Some had started their assessment and improvements when the Act was still a Bill.

Most implementation activities have focussed on technical security to safeguard data; improving and enhancing contracts with data subjects; capturing clear consent to own, store and share data; and improving employee awareness of their responsibilities in securing and protecting data. A number of the organisations have also assessed the adequacy of their existing security solutions and are in the process of enhancing them if required. Some have started to separate customer data, to create an anonymous data set to reduce the adverse impact of the data being compromised. Others have started to update the contracts that they have in place, to ensure that partners and other third parties also adhere to the requirements of the Act. Additionally, others have reviewed the customer journeys, terms and conditions, messaging, and digital contracts to ensure they are in line with the Act. Others have started the process of implementing local replication for all data to comply with the need to host in Kenya.

Table 1: Survey Responses

<table>
<thead>
<tr>
<th>ANSWER CHOICES</th>
<th>RESPONSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated Customer</td>
<td>45.45%</td>
</tr>
<tr>
<td>Customers asked for permission to share</td>
<td>36.36%</td>
</tr>
<tr>
<td>Customers asked for permission to share with clear reasons</td>
<td>45.45%</td>
</tr>
<tr>
<td>Customers asked for permission at start of contract</td>
<td>63.64%</td>
</tr>
<tr>
<td>Customers asked for permission to make changes to existing services &amp; new providers required</td>
<td>27.27%</td>
</tr>
<tr>
<td>General purposes of the sharing provided to the customer</td>
<td>45.45%</td>
</tr>
<tr>
<td>Specific name of the partner shared with provided to customer</td>
<td>45.45%</td>
</tr>
<tr>
<td>Customer information securely shared without contract request</td>
<td>18.18%</td>
</tr>
<tr>
<td>Other</td>
<td>36.36%</td>
</tr>
</tbody>
</table>

Figure 10: Have you implemented a programme to deliver the requirements of the Act?

Figure 11: If yes - how long has it been running?
To ensure that access to the subject’s data is minimised, different approaches have been adopted. These range from implementing an Identity Experience Framework to manage the Authentication and Authorisation of access to the data to providing Role Based Access Control. Some of these measures have limited access to the data to a controlled set of people within the firms. Security measures such as implementation of VPNs, enforcing the strength and variety of passwords, and the addition of multi-factor authentication to ensure that a compromised password does not lead to all sources becoming compromised, have also been implemented. Some firms have also implemented and performed Information security controls and Vulnerability Assessment and Penetration Testing (VAPT) of their systems, to ensure that information sent to third parties is also password protected, thus preventing data being reviewed by unintended recipients.

All these measures show that some of the respondents have started to assess their processes and services in light of the Act. However, the controls and mechanisms implemented would need to be examined in detail to assess whether they are robust enough, and that the logs are being actively monitored to identify any compromise.

2.4.5 Activities to Support Interaction with Data Subjects

Given the lack of clarity at the time of the survey on how a Data Subject Access request is expected to happen, it is not surprising that the largest portion of respondents were not sure at this time about how they will manage such requests. 25% of the respondents have a semi-automated process, but none have a fully automated process. This is not necessarily a challenge in smaller organisations, but as these organisations scale, the lack of automated services will increase the burden on them; addressing this early in their lifecycle will allow them to grow quickly without putting data subjects’ rights at risk.

The final area that was explored was the approach to managing unstructured data, for example data that is found in email, PDFs, presentations or images. These documents are covered under DAPA but the tagging and subsequent recovery of these items is possibly the most complex task that will face a data controller or processor. It is likely that firms will employ manual processes to handle unstructured data, possibly with access to a small number of tools, but this is still expected to be a significant compliance burden to both controllers and processors.

---

**Figure 12: How do you plan to manage Data Subject Access Requests?**

**Figure 13: How are you managing your unstructured data?**
2.5 Opportunities Presented by the Act

The general consensus in responses on the positive outcomes the Act will create was that DAPA will help to enhance the level of trust in fintechs. Some respondents see the increased oversight from the Act as a means of weeding out bad practices, and as an honour badge for compliant fintechs. There is an expectation that this will lead to an increased uptake of solutions provided by fintechs. Other respondents see the responsibility to protect sensitive data as an opportunity to enhance their contracts with data processors, now that there is better clarity on where responsibility lies. Others also see the requirement to institute better controls as an opportunity to improve their business processes and structure their data to eliminate ‘noise’ in their current processes. Some respondents also see opportunities for their data subjects with regards to opportunities to leverage their data for better solutions and services, especially through data portability.

2.6 Challenges Presented by the Act

The majority of responses focussed on a lack of guidance, and the risk that individual interpretations can lead to inconsistent application of the law and its enforcement by regulators. Smaller firms in the survey felt that their business processes were disproportionately constrained by the lack of guidance on implementation. There were concerns regarding implementation in the face of unique challenges that are pertinent to Kenya, for example managing consent on channels such as USSD, which has a limited session time. Another area of concern was the need to host within Kenya. This was later clarified in the issuing of the draft regulations, but at the time of the survey, without clarity regarding the criticality of this issue, it presented both an opportunity (for local cloud providers) and a risk (for those hosting outside). The final concern was the risk of unscrupulous data subjects who start baseless disputes to seek financial compensation. The provision that a fee could be charged for excessive requests will help to mitigate this risk, but further guidance is required on the level of acceptable fees.
Chapter 3

Data Protection in a Fintech Context

Consumer services have emerged globally which have created a mindset of “data is the new oil”, i.e. the way to innovate and monetize offerings. Most of Kenya’s fintech solutions are built on this premise of utilising alternative data sources and information sharing to inform decisions, business models and monetisation models.

These enterprise-led innovations gave rise to a range of other mobile offerings, including several app-based models that provide small loans using information stored on an individual’s smart phone. Innovation around data has grown over the years to adjacencies in ride-hailing, gig worker platforms, and agri-initiatives, not to mention MSME innovations around data. Such innovations have extended financial inclusion in Kenya; however, they also focus attention on the need to address potential risks in the provision of such services in the context of data privacy, consent, and data protection.

With the Data Protection Act now in place and draft regulations published, innovators in Kenya need to think more deeply about innovation that is balanced with compliance with the law. While data protection and the safeguarding of privacy is a challenge for an organisation of any kind, financial services firms carry an added responsibility of complying with financial sector regulation. However, the incentives should not only be to comply with the relevant laws but also to develop solutions and business practices that are in the long-term interests of customers.

For data protection, there are conversations around the question of “what does good look like?”, and how innovators and the fintech community can practically comply with the law, while also upholding best practice. For example, while the law compels data processors and controllers to comply with a data subject access request, how can a firm practically implement this? Are there examples of companies that are doing this well that could be emulated? What bad practices should be avoided? How might those who are already exploring Open APIs open the way for others? This section provides practical approaches on the ways in which the innovation and Fintech ecosystem could start to comply with the law in a pragmatic manner, while still keeping the customer in mind. The recommendations and approaches provided in this section are potentially applicable to all organisations, but the use cases explored are primarily focussed on financial services.

This review is not exhaustive as there are many resources, such as the UK’s ICO and free online GDPR material, that provide practical guidance for organisations to quickly accelerate their ability to implement the provisions of GDPR, and that can also be applicable to DAPA while adjusting for minor changes.

3.1 Data Collection and Processing Practices

User experience in data collection is the first thing that should be reviewed. As the requirement is to ask for specific intent, and inform the customer of any third parties involved or who may also receive the data, there is a risk that this request will add another hurdle that might deter customers. As this stipulation is a requirement for all companies, it is also an opportunity to provide an excellent user experience that could differentiate one company from its competitors. A service provider that makes the protection of a data subject’s information a simple interaction is putting their customer’s needs before their own interests.

A very simple test before asking for permission to capture data is to honestly answer this question: answer “Do I really need this information to offer the service?” If the answer is “yes”, then it should be possible to explain to the customer why that data capture is important.

Let us use the example of some bad practices that have already been identified in Kenya – digital lenders

---

2 https://ico.org.uk/for-organisations/
that have captured contact details of their customers’ friends and relatives from their social media sites as part of their on-boarding process. If a customer defaults, the practice is to contact those friends and relatives and coax them into asking the borrower to repay the loan. Under DAPA, these other parties (the friends and relatives) have not provided consent for their details to be captured, hence the act is immediately an offence. If the service was created in such a way that these parties were acting as sponsors or guarantors, the onboarding journey should be extended to include them. This approach would ensure that there is a legitimate reason for having these details, and that the parties have consented to their details being captured as part of the on-boarding process.

It is worth highlighting that even if a contract explicitly states that the capture of information is required for the service, the Data Commissioner has the power to override this requirement if they deem that the data is not needed to perform the service. Take the example of signing up for a web page that monitors share prices or not needed to perform the service. Take the example of signing up for a web page that monitors share prices or the service, the Data Commissioner has the power to override this requirement if they deem that the data is not needed to perform the service. Take the example of signing up for a web page that monitors share prices or exchange rates. The firm can capture an email address so that the user can sign-in and receive a password to access the site. However, if the firm asks for more contact details for marketing purposes, the additional request is not technically essential for the performance of the contract and may be deemed unnecessary. If the service is funded by physically sending marketing material to the customer, the collection of the additional information might be deemed necessary, but the customer needs to be informed that the material will be sent to them in the serving of the contract. The customer can then decide whether this is valuable to them and whether or not to provide their consent. It is important to create the ability to withdraw consent within the product at a later stage to enhance the user experience; for instance, when the customer decides they no longer want to receive marketing material.

We also need to consider the use of USSD for the registration of a service and for capturing and maintaining consent requests. The short session time offered by USSD makes long Terms and Conditions impossible to share easily during a single session, meaning that links to the contracts are more likely to be required. Fortunately, section 4(2) of the Data Protection (General) Regulations 2021 makes provision for the information to be availed through a public notice accessible to a data subject prior to the collection of the personal data. However, there needs to be evidence that the customer was made aware of the Terms and Conditions. The best practice is to keep the Terms and Conditions separate from the capturing of consent. With this in mind, a simple USSD menu could be created for the capturing of consent.

It is also possible that additional data might be required without the data subject being provided with full clarity that this is the case. A good example is the investigation of the data subject to check if they are undertaking any suspicious activity on the dark web. This data capture can also be necessary to check for money laundering or terrorist financing activity, and seeking consent is likely to be counterproductive to this assessment. In this instance, a blanket statement that further information may be captured from publicly available sources to prevent money laundering or terrorist financing may suffice. However, the possible options for these terms will need to be provided by the Data Commissioner’s office.

A data controller will also need to advise a data subject when they may have been subject to an automated decision and failed the assessment. Under DAPA, there is no requirement to notify the data subject if the automated processing is necessary for entering into a contract or is authorised by law. It is worth noting that profiling to perform a credit assessment could be construed as necessary for entering into a contract, or that assessing a customer for money laundering could be authorised by law, although these approaches would require confirmation from the Data Commissioner as part of the firm’s application to register. The data subject rejected from the credit decision may not necessarily need to be notified, but in the provision of good customer experience, they could reasonably expect an explanation. With this explanation the data subject could rectify any information that is incorrect, or adjust their activity, so that a subsequent application is more likely to be successful.

For a data subject suspected of money laundering or other financial crime, the case for explaining the profiling is more complex, and there is a risk of committing an offence under Section 8 of the Proceeds of Crime and Anti-Money Laundering Act 2009. If the data subject is identified as a money launderer, it is possible that the data controller or processor could tip off this party and therefore be at risk of breaching their responsibility to the Financial Reporting Centre. Avoiding tipping off the data subject becomes even more imperative if the transaction is suspected to be part of terrorist financing.

---

In both scenarios, it is far more likely that a decision will not be shared with the data subject but rather require them to provide additional information, such as a clarification of the source of funds, etc. However, until guidance has been formally issued by the Data Commissioner, it might not be possible to make this assumption in the short term, so any fintech actively using profiling is advised to make an early engagement with the Data Commissioner’s Office on this matter to seek clarity.

An additional implication of DAPA is what data should and should not be shared amongst data processors and controllers as part of their working practices. If a fraud investigation is underway and it emerges that information needs to be shared with other parties to support the investigation, it is now likely that sharing that information will be restricted. Imagine a scenario where a payment is made from one financial institution to another to support their customers. Subsequently, the sender suspects the recipient is engaging in fraud, and thus wishes to validate that recipient’s identity. Historically, the sending institution might have contacted the recipient’s financial institution to request identity information. If the recipient has not previously provided consent for the sharing of this information, the recipient sharing any identity information with the investigators would be committing an offence. It is also worth noting that just because consent was not provided, this does not mean that the recipient is a fraudster. It could be possible that the investigation is dealing with someone who simply wishes to protect their identity. We explore modern techniques used to address these instances in section 3.3 on balancing consumer protection with Managing Fraud / AML and CFT.

3.2 Implementing a Data Protection Program

As previously highlighted, there are a number of steps that should be undertaken to understand how data flows through the organisation. The next section highlights best practices in implementing a Data Protection Program within an organisation, and how to identify the best resources to implement the steps highlighted so far.

3.2.1 Establishing a Team

The fines under GDPR and CCPA are set at relatively high levels to compel company boards to give the protection of customer’s data the due attention required. The fines under DAPA are relatively lower. Additionally, there is no requirement under DAPA to have a dedicated Data Protection Officer. Potentially, this role can be shared amongst organisations through Data Protection as a service arrangement. Either way, it is essential to assess how a data protection programme aligns with a company’s core strategy prior to implementation. If the strategy is to put the customer first, then the differentiation of a good experience for data protection and governance could be the element that sets an organisation apart from its competition. The higher the priority the programme takes, the more senior the role that should be appointed to lead the task. Irrespective of a company’s priorities, an agile approach to implementing a data protection programme should be adopted.

It is recommended that a senior manager be appointed to champion, lead, and potentially become the firm’s Data Protection Officer. DAPA provides clear guidance on the requirements of that individual under section 24 (5) of The Data Protection Act. While a legal or technical background is required, a solid understanding of the priorities of the business will also help ensure appropriate controls are applied. Most fintechs are likely to already have a team that is responsible for compliance and risk management, or a CISO or other lead on cyber security. One of these individuals could be well suited to driving the changes needed to deliver a data protection programme, as long as this selection does not cause a conflict of interest as defined in section 24 (2) of DAPA. If the firm has an obligation to comply with GDPR or CCPA, it is highly advisable that this role be given operational autonomy with direct reporting to the board, given the proportionally higher fines that could be applied.

The largest challenge in addressing data protection is understanding all the touch points where an organisation receives customer data, and what happens to the data afterwards. With this in mind, all business units and processes that handle customers’ data should be mapped and captured. This will require that all senior managers that head these business units and processes be aware of the programme and are involved in implementation. Within the team, it will be important to identify people who can act as the voice of the customer and help clarify the questions. “Does the organisation really need to know this information?” and challenge “Who needs access to this information?”
3.2.2 Starting the Assessment With a Data Flow Map

Before starting to build a Data Flow map, the organisation should first create some appropriate categories for the data – including the business reasons for the data capture or the legitimate interest for capture. The categories could include:

- Personal Identifiable Information (PII)
- Sensitive Personal Identifiable Information (SPII)
- Legal requirement (expanded to be descriptive – e.g. fraud management)
- Financial record
- System of record
- Product information
- Strategic plans
- Miscellaneous

Although an organisation might identify multiple categories, the priority in subsequent phases should be on Personal and Sensitive Personal Data even if that data is created by the organisation. The respective definitions from DAPA are outlined in Section 2 of Act. The categorization might help to reveal non-critical or non-essential data for which adding too many controls is likely to be counterproductive.

Once the categories have been identified, the organisation should build a clear inventory of where the data might exist, such as:

- Databases
- Infrastructure
- Remote working locations
- Individual’s machines (separate desktops and laptops)
- Email
- Mobile devices
- Miscellaneous

It is important to consider all the categories of structured, semi-structured and unstructured data. Most firms risk focussing on structured and semi-structured data, when unstructured data is also included in the Act. These different data types should be identified as part of the inventory process.

- Unstructured data is data that is not organised in a predefined manner and is found in images, audio files, presentations, communication channels (such as slack), social media accounts, emails, and documents (including PDFs etc.). This set of data is likely to grow exponentially and therefore become much harder to map: it could equate to 80-90% of a company’s data. Finding an owner for unstructured data can be one of the most complex tasks in the inventory process.

- Semi-structured data is usually data in reports and outputs, but can also include salaries in a spreadsheet.

Structured data is the most commonly understood: it is ordinarily located in databases, and usually the system has a clear owner.

We should now have categories, locations and data types identified. Controls need to be put in place to protect the data – this should include the data transmission as well as the data storage. The following controls should be considered:
In a large organisation where there are many processes and data flows, the registration/sign-up process will be a good starting point for developing the data flow map. This should follow what is commonly referred to as the ‘happy path’ – the path that would be followed if everything went well. Once the end to end of this path has been mapped, the next step is to start at the beginning and capture more paths that diverge from the happy path when things do not go as planned. If an organization deals with third parties, their data flow maps should be developed too, including reviewing their contracts to ensure that they are aligned to the new legislation.

The data flow example below has been created in an interactive whiteboard (Miro⁴) using their free service, but other services and tools could be used. The advantage of such a tool is that it is online, and allows for multiple parties to interact with the board at the same time or asynchronously.

The organization should then map the key roles that should be allowed access to the respective data and whether that access is essential and proportional to the roles. The definition of key roles will be important when applying the relevant security controls. Data access should be guided by a process of least privilege, where everyone starts at a position of zero access. It is at this point where the first perceived conflict is likely to become apparent if high profile users such as the marketing department or CEO are restricted to access data that they could previously access. These stakeholders will need to be managed, as they are the ones likely to object and who have enough authority to create an internal block if they disagree with the interpretation that restricts their data access. However, the reality is that anonymised and aggregated data is often more than sufficient for their needs.

The data flow map should also identify where the organization’s data can leave its systems, including inadvertent output to PDFs, downloads to local machines, screenshots, spreadsheets, and forwarding of emails etc. As such, remote working should ideally be listed in the inventory list as an area that should be monitored. This is because machines that are available for remote working present an additional risk – if an employee can access data and download it to their local machine, it is possible for that data to be subsequently accessed by an unknown actor if the controls in place are inadequate.

---

⁴ [https://miro.com/](https://miro.com/)
When developing the data flow map, the data should be assessed to determine if it is still in its raw form with identifiable individuals or has been aggregated. Aggregated data might be of a lower risk, as an individual is no longer identifiable. However, this is not the case when the data is not from a sufficiently large selection of data where it might be possible to re-identify individuals.

### 3.2.3 Assessing the Storage, Retention Policy and Protection of the Data

Next, the organisation should review its data retention policies for the various data categories and processes mapped in the data flow map, to ensure that the retention policy is appropriate for the data and its use. Take as an example pension documents, where the obligation to store the information could be for seven years after the policy has expired. In real terms, this could be more than a century. As such, the retention policy for this type of data should clearly not apply to all data, but to a small subset where a longer retention period is required. It is possible there might be additional data related to that requiring a longer retention period but that on its own requires a shorter retention period. In the pensions example, knowing which IP address was used to create the initial application serves little purpose in the delivery of pension itself. If the IP address was captured to eliminate fraud, then a retention of more than 12 months is likely to be excessive. However, if the data is needed as part of a suspicious activity report, then it needs to be retained for seven years from the date of the report as required by Section 44 of the Proceeds of Crime and Anti-Money Laundering Act 2009.

The next step is to assess if and how data that identifies an individual is separated from the aggregated data. This assessment will enable the organization to reduce the risk of exposing an individual in the event of a breach. It is worth re-stating that it is possible to reconstruct a person’s identity if there are sufficient data points. For example, a regular visit to a coffee shop, with a payment of a similar amount in a regular time, can quickly lead to an individual being identified based on their habitual pattern or simply by providing a geolocation from their phone’s GPS or IP addresses. In this instance, the data subject is no longer anonymous. As such, it is imperative to anonymise information that can be used to construct or identify a data subject, and to ensure that identifiers such as physical locators are also stored separately.

Let’s revisit our transaction in the coffee shop to understand all the fields that might be captured and how they can be separated. A reference to identify the coffee shop (entity data) can be created and stored separately from the data that can be used to identify the data subject (transaction sensitive data). Using the roles and access controls identified in the data flow map, the organisation can assign access to the respective data as and if needed. For example, only senior compliance managers would be given access to Transaction_Sensitive_Data or Entity_Data in this example, whilst other employees could be given temporary access to the necessary information if needed.

*Figure 18: Example of Reference to Identity Data*

Customer service agents could be allowed to know the name of the account holder when engaging on a call, but would not need access to the address, or other identifiable details. As part of the control review, the organization should assess whether the access granted to customer service agents carries a risk. For instance, it is possible that the customer agent could write sensitive data on a pad that could be easily transferred from the organization’s premises (especially if they are working from home).

The implementation of Role-Based Access Control (RBAC) and an approval process for temporary access can mitigate such risks. If the organisation has an interactive voice recognition (IVR) system, it could be used to capture the required input so that an employee does not need to access sensitive data to authenticate a user. Note that this IVR will also need to have access...
controls implemented to prevent an accidental data breach. If temporary access to data is required, the approval process could also be extended to the mobile app of the data subject, where they could temporarily approve access during their interaction with a customer service agent, rather than just limiting the approval process to an internal supervisor.

Once there is a clear understanding of the individual and aggregated data held by the organization and how each is stored and accessed, the organization can now map each data point to the use cases that relate to the data point. Examples of use cases include the data used for the core system of record, marketing, fraud management etc. The data map should be updated once a new use case has been identified. When considering the retention policy of the data, one should not forget that the data might also be captured to logs, as well as the databases themselves.

Table 2: Data Map for Retention Analysis

<table>
<thead>
<tr>
<th>Table</th>
<th>Field</th>
<th>Data Classification</th>
<th>Storage Case 1</th>
<th>Storage Case 2</th>
<th>Storage Case 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction_Data</td>
<td>Transaction_ID</td>
<td>Financial, System of Record</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction_Data</td>
<td>Date/Time</td>
<td>PII, Financial, System of Record</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Transaction_Data</td>
<td>Payer_ID</td>
<td>PII, Financial, System of Record</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Transaction_Sensitive_Data</td>
<td>IP_Address</td>
<td>PII _Sensitive</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
The data retention requirements for each data point should be dictated by its use case. For example, in the above table, storage case 1 represents data that is held for system of record and thus the retention period could be five years to comply with the Tax Procedures Act 2015 after date of capture. In the example, data that is captured in February 2021 would be retained until the end of February 2026 for compliance purposes. The retention period will vary with each use case and would need to be validated for each use case. For Storage case 2, the retention policy is likely to be within one to three months, and would be subject to consumer consent. For Storage case 3, it is unlikely that the data would be required for more than 13 months to cover annual events. In the above table, an IP Address can be captured and retained for marketing and fraud purposes but the customer can subsequently withdraw their consent for processing their data; in which case, the data can no longer be used for marketing activity. It can be retained for fraud investigation purposes until the fraud retention period expires.

Both technology and businesses will continue to evolve, so a review of the data map and detailed data access controls should also be conducted on a regular basis. The reviews should reassess whether the organisation still needs to retain the data, if there are new data requirements or partners (third parties), or whether processes have changed. In all cases, the appropriate documentation should be updated to reflect the current status, and the revised information should be shared with the impacted data subjects. If a new use-case is no longer compatible with the original consent provided, the organisation will need to seek new consent from the data subject.

It is worth noting that the same approach should be adopted for unstructured data that comes through non-digital channels as with physical correspondence, notes typed up from calls, etc. This is discussed in depth in section 3.2.8.

### 3.2.4 Building for Withdrawal of Consent

One of the new processes that customer-centric organisations will need to implement is a system that tracks user preferences and consent. This system should be used prior to data processing to confirm that there still exists a valid consent to process data. This is especially important if the data is needed for other approved purposes or use cases, as there is a risk of inadvertently processing the data when consent has been withdrawn. The control mechanism to implement the system should be added to the data flow map, and its delivery should be designated as one of the highest priority tasks. Example of tools that may be able to assist are explored in Section 3.5.1: Tools for a Delivery Program.

### 3.2.5 Creating a Data Protection Impact Assessment (DPIA)

Upon completion, the data flow map should provide clarity on the following issues:

- Data that has been captured and the reason for capturing the data
- The consent that has been captured
- Key roles with access to the data
- Data protection and security measures that are in place
- Existing controls to restrict access to the data

The organization should next perform a risk impact assessment before implementing any new data flows and necessary controls. This impact assessment will identify any weaknesses or risks that need to be mitigated. For the impact assessment to be beneficial, the organization should theoretically remove any existing controls that are in place in order to reveal the underlying risks and vulnerabilities to the data, and then determine the effectiveness of the controls. This is especially important when deploying new technologies or processes that might introduce new risks that need to be prioritised.

For the impact assessment, the organisation can adopt a DREAD risk assessment\(^5\) or STRIDE Security model\(^6\) if desired and appropriate. However, a simple approach that uses basic probability and impact scoring can be adopted. In this approach, we assess the probability of risk on a scale of 1 (low) to 5 (high), where the probability of the risk occurring is multiplied by the potential impact of the risk to create a derivative risk rating score. The lowest score we apply to the Probability or the Impact is 1, with the highest being 5. Thus, the lowest derivative risk rating score is 1 (1 x 1) and the highest is 25 (5 x 5). The risk acceptance should be set at a score of 14, so anything scoring 15 or above would require immediate attention.

---

\(^5\) [https://en.wikipedia.org/wiki/DREAD_(risk_assessment_model)]

\(^6\) [https://en.wikipedia.org/wiki/STRIDE_(security)]
Table 3: Risk Score:

<table>
<thead>
<tr>
<th>ID</th>
<th>Risk</th>
<th>Probability</th>
<th>Impact</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sensitive data in table exposed</td>
<td>5</td>
<td>5</td>
<td>25</td>
</tr>
<tr>
<td>2</td>
<td>System of Record data in table exposed</td>
<td>5</td>
<td>3</td>
<td>15</td>
</tr>
</tbody>
</table>

Once the base risk scores have been derived, the probability and impact can be re-assessed as if the mitigation controls had been put in place. The organization can re-scope the risk by multiplying the residual probability and the residual impact to derive the residual risk score. It is worth noting that the impact does not always change but there are scenarios (such as an insurance policy) where it is possible that the impact can be reduced.

Table 4: Residual Risk Score:

<table>
<thead>
<tr>
<th>ID</th>
<th>Mitigation</th>
<th>Residual Probability</th>
<th>Residual Impact</th>
<th>Residual Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Role-based access control, data encryption in transit and at rest</td>
<td>1</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>Role-based access control, data encryption in transit and at rest</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

From the Risk Score table, exposing sensitive data and exposing data in the system of record carry a derivative risk score of 25 and 15 respectively. Once the appropriate risk mitigation measures are applied (role-based access control, data encryption in transit and at rest), the probability of the risk manifesting reduces to 1, and therefore the residual derivative risk scores reduce from 5 to 3 respectively (Residual Risk Score table).

The impact assessment should be performed for all the data identified in the flow map. If the organisation already has existing controls that are deemed sufficient, they should be documented as the mitigation measures for the identified risks. If the controls are deemed as insufficient, the organisation will need to put new ones in place or enhance the existing ones. It is important to note that if sensitive data is at risk, the organisation is required to request the Data Commissioner to review the risk before performing any processing of the data.

The questions below can help an organization to determine whether the risks have been appropriately mitigated:

- Is the cyber threat assessment up to date?
- Is all the data identified in the data flow map controlled by the security of the organisation? If not, what is being done to address it?
- Is the password policy of the right standard with enhanced features such as multi-factor authentication?
- Are the firewall and anti-virus solutions capable of detecting, preventing and eliminating the latest threats faced?
- Are patching and maintenance update procedures in place to reduce 0-day threats?
- Is personal data secure (in storage and when transmitted) and backed up on a routine basis? Where is the backup and how is it also protected?
- Is the Business Continuity Plan up to date and tested, including responses to ransomware?
- Have the risks posed by employees been adequately addressed, including education and training, policies regarding internet and device use, remote working, and employee turnover risks?

If the answers to the questions above lead to a change in the organisation’s security policies, processes or controls, the assessment should be expanded to include these new measures. Some of the tools that can be used to conduct the assessment are highlighted in section Section 3.5.1: Tools for a Delivery Program.
3.2.6 Process for Responding to a Data Subject Access Request (DSAR)

When an organization receives a Data Subject Access Request (DSAR), it will need to have other processes in place to streamline this activity. Unless alternative channels are prescribed in regulations or guidance notes, a data subject access request is likely to be submitted via a telephone call, email or the organization’s web pages. The format of the request itself is provided in Form 3 of the draft Data Protection (General) Regulations 2021.

Once received, the organization should first capture the request in a log to ensure that it is processed in a timely manner. Next, the DSAR needs to be validated to ensure that the person requesting the data is in fact the data subject. If there is no clarity on the identity of the individual making the request, or on what is being requested, appropriate steps should be put in place to get clarity on the same as quickly as possible to avoid delays. From a user experience perspective, the DSAR process should be as straightforward as the original registration process.

Currently, there is no specific guidance on what can be construed as excessive requests or where it is permissible to charge a fee to facilitate the DSAR. However, the request log can point out data subjects that have made multiple requests, for which a reasonable fee might be charged.

The DSAR response to the data subject should have sufficient protection to ensure that it is not compromised during transit. The response should be within a reasonable time that does not exceed 30 days unless the request is complicated. If so, the organization should provide a prompt response to the data subject outlining the complexity of the data and the anticipated delay in complying with the DSAR. Under GDPR, the data controller or processor can extend the response by no more than 60 days (maximum 90 days from when the request was received) and the data subject should be notified of the potential delay within 30 days.

The responder should consider providing the following information:

- The data requested. Any data that is captured as opinion should be clearly marked as an opinion to avoid requests to correct this data
- Categories of the data collected
- Categories of sources of the data collected
- Commercial purpose for the collection of the data
- Categories of third parties that the data has been shared with
- The retention period of the data
- Complaints procedure – including providing details of the Data Commissioner

It is important that data relating to third party data subjects is also protected. This means that some of the information might need to be redacted if consent for disclosing that data cannot be obtained from the third parties. It is worth noting that even in the examples used by the UK’s ICO provision of exemptions there are very few instances where data might be redacted from the information provided to the data subject. Similarly, the Data Commissioner can provide guidance on instances where such exemptions might apply.

3.2.7 Implementing the changes

As the organisation now has a good view of the current and end state of their data infrastructure at both a process and system-wide level, they can start implementing the necessary changes. In an agile approach, this could start as soon as the first key data map has been completed, with the assessment team acting as the product team for the delivery. As mentioned previously, implementation could potentially start with the consent management system, working progressively through the highest priority security improvements (unless of course a critical security change needs prioritising).

It is critical that the organisation seeks to avoid departmental silos, as each silo will take a different approach, risking duplication and a misaligned implementation between the silos. In such circumstances, centralising the data will allow for the architecture and information management flows to be implemented consistently.

The organisation should review their documentation on Policies and Procedures and ensure that these are also updated to reflect the changes needed for DAPA. These include:

- Privacy Notices for Customers
- Data Protection Policy, including how to securely share data with third Parties

Data Privacy and Protection: Guidance Note to Kenya Digital Financial Services

- Data breach policy
- Customer complaint policy
- Business continuity planning
- Data retention policy

Again, the policies and procedures need to cover both Structured and Unstructured Data. The organisation is also likely to require a training program to brief all employees: some will need to be aware of the need to keep information protected, whilst others will require training on the new processes they need to adopt to adhere to DAPA. A well implemented system can be quickly undone by weak employee engagement. As such, organisational changes might be required in larger organisations to ensure a clear separation of responsibility and oversight.

As most fintechs will be dealing with sensitive personal data, if they are licensed under the National Payment Systems Act 2011, they are under requirement to host in Kenya. If new infrastructure or hosting services are required, it will be worth assessing the impact of hosting that infrastructure in Kenya if it is not already hosted there. Although Section 25 of the draft "Data Protection (General) Regulations 2021" provides some guidance on organizations that must process their data in Kenya, there is no definition of equivalency. As was seen with the Schrems II case in Europe where the effectiveness of Standard Contractual Clauses was challenged for hosting data in the United States, the possibility that the US Intelligence Agencies could access the data extinguished the perceived equivalency of security. This made hosting outside the European Union and especially in the United States slightly more complex for organizations based in the United States. Until such a time that the Data Commissioner will issue explicit guidance for all financial institutions on the equivalency of other countries’ ability to host financial services, the working assumption will be that financial services are likely to be expected to host their data in Kenya.

Section 3.5.1: Tools for a Delivery Program explores some of the tools available to support implementation.

3.2.8 Addressing Unstructured Data

As most unstructured data resides in some form of digital storage, it is worth assessing what tools already exist for storing such types of data. One such tool is a basic home Network-attached Storage (NAS) solution offered by firms such as QNAP or Synology, with both having rich full-text search functions (QSirch and Universal Search respectively). QNAP also provides Optical Character Recognition functionality to convert images to a format that is more readable. The same functionality exists for most storage and mail solutions. However, this approach at identifying an individual will be time consuming and will also miss data that has not been entered correctly, or mistyped. In the end, automating processes will be more efficient than the application of storage tools to resolve manual issues. Automation will lead to a more consistent approach, especially as more data is captured. It will also help to address any legacy data until such time that the organisation develops a clear strategy for the data. Any automation needs to address the following:

- PDF data extraction – covered by most search tools
- Intelligent OCR – converting images and structuring the data
- Automatic tagging – to make data more accessible and easier to organise

If the organisation’s in-house skills support it, they can also consider implementing a machine learning tool to help in the capture and categorisation. Unfortunately, most Software as a Service (SaaS) products that deliver this function are not based in Kenya, and organizations risk breaching hosting requirements if they become dependent upon these products.

One such product is provided by MonkeyLearn, who outline their process and guidance on the analytics that they undertake to structure and analyse unstructured data in real time.

3.3 Balancing Consumer Protection with Managing Fraud / AML and CFT

There are instances where financial service regulations might conflict with DAPA. A potential conflict might arise when financial information sharing contravenes data privacy requirements. However, this is not unique to Kenya. In Europe, the Royal United Services Institute (RUSI), the world’s oldest independent think tank on international defence and security, highlighted some of these challenges back in 2017. In 2019, the institute

---

9 The CJEU judgment in the Schrems II case - Think Tank (europa.eu)
10 https://monkeylearn.com/blog/unstructured-data-analysis/
commenced a research project on privacy enhancing technology\textsuperscript{11} with the specific goal of exploring use-cases that are relevant to financial information-sharing, whilst protecting the identity and privacy of individuals. A discussion paper highlighting the case studies was published in January 2021.

This was further evidenced in the first data-driven ‘fintech sandbox’ by the UK’s Financial Conduct Authority, with companies exploring the use of Secure Multi-Party Computation (SMPC): the Dutch TNO (an independent research organisation) trialling their MPC4AML - project\textsuperscript{12}, and Sedicii, an Irish technology company, trialling Prexa\textsuperscript{13}. Both organisations have created a way for financial services organisations to share data in real time – but with no identifiable data even leaving the respective entities. This sandbox was also supported by the Information Commissioner’s Office – as identified in the ICO’s Key areas of focus for the Regulatory Sandbox\textsuperscript{14}.

3.4 Opportunities for Fintechs

The advantages of taking a customer-centric approach to data protection and leveraging the same as a key competitive differentiator have already been highlighted. For agile organisations, the opportunity to set themselves apart and differentiate themselves in their respective market should not be overlooked. For some fintechs, their skills and experience will put them in a strong position to act as a data processor for other organisations. In a similar way, organisations that provide IT services to financial services companies can easily expand their service offerings to include data protection as a service.

Fintechs should also consider developing new services for Privacy Enhancing Technologies such as Symmetric Multi-Party Computation (SMPC), as outlined in section 3.3 on balancing consumer protection with Managing Fraud / AML and CFT. If an organisation is already working closely with other fintechs, then joint exploration of these areas will reduce the development burden, as these solutions have little value in the absence of common processes.

The final area that should be considered is Homomorphic Encryption. Knowledge of these techniques and their specific implementation by cloud providers could be a useful option in overcoming the requirement to host in Kenya. Homomorphic encryption means that data that is encrypted can still be processed in its encrypted format. This may allay some of the fears of the Data Commissioner in relation to hosting sensitive data outside Kenya.

3.5 Tools for a Delivery Program

In delivering a data protection programme, it is important to have access to the right tools. This section highlights some of the general tools that can be utilised by an organization in starting its programme. It is important to clarify that the tools organisation decides to use will depend on its own specific circumstance. Irrespective of the tools deployed, the key element to consider is the use of tools that will help in the both the tactical management of data and for management’s oversight of the data, with the capability to be integrated into the existing infrastructure. It is also important to note that automation will be essential for managing historical data.

3.5.1 Digital Resources Available

Resources provided by the Singapore Personal Data Protection Commission (SPDPC)

As part of their data protection mandate, the Singapore PDPC has provided a number of useful resources that can be used by an organisation to develop data flow maps and undertake a data inventory capture. Each of these tools could provide a good starting point for any organisation.

- Data Protection Impact Assessment\textsuperscript{15}
- Breach Incident Record Log\textsuperscript{16}
- Sample Personal Data Inventory Map Template\textsuperscript{17}
- Data Flow Illustration (pdf)\textsuperscript{18}

\textsuperscript{11} https://www.future-fis.com/the-pet-project.html
\textsuperscript{12} https://app.digitalsandboxpilot.co.uk/projects/5fb-53da7537ab0009d8af8d
\textsuperscript{13} https://app.digitalsandboxpilot.co.uk/projects/5fb-53c47537ab0009d8af837tabs=showcase
\textsuperscript{14} https://ico.org.uk/media/2618112/our-key-areas-of-focus-for-regulatory-sandbox.pdf
\textsuperscript{15} https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guide-to-dpias---011117.pdf?la=en
\textsuperscript{16} https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPMP/Breach-Incident-Record-Log-20170619.xlsx?la=en
\textsuperscript{17} https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPMP/Sample-Personal-Data-Inventory-Map-Template.xlsx?la=en
\textsuperscript{18} https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPMP/Data-Flow-Illustration-PDF-v2.pdf?la=en
• Data Flow Illustration (vsd)
• Sample Consent Registry
• Develop a Process for Dispute Resolution

Tools for Developing a Data Flow Map

The data flow map in section 3.2 of this document has been created by Miro, an online whiteboard and visual collaboration platform. The free version of the platform (at the time of writing) allowed for three working boards with unlimited contributors, enabling simple sharing amongst multiple participants.

Data Protection Impact Assessment

The French Commission Nationale de l’Informatique et des Libertés (CNIL) has made available in their GDPR developers guide, an array of tools including for data protection impact assessment. Strathmore University have also provided Kenya-specific guidance for small organisations to help them understand what is required for a Data Protection Impact Assessment. Strathmore University has also developed a simplified data protection impact assessment toolkit for small organizations such as micro and small enterprises.

3.5.2 Data Protection Notice Generator

Singapore PDPC created a Data Protection Notice Generator for gathering the key information required for sharing with data subjects for create the relevant notices when such data is shared.

3.5.3 Security Tools

For those looking for security guidance, the Open Source Security Foundation provides free courses which can be easily adapted to ensure that systems are not easily accessed by unauthorised personnel, and the required controls are implemented at the design stage rather than as an afterthought.

The U.S. Department of Commerce’s National Institute for Standards and Technology (NIST) has also provided guidance on Protecting Controlled Unclassified Information in Non-federal Systems with a later Supplement to NIST Special Publication 800-171, both of which provide good guidance on the systems and processes that should be implemented to protect data.

3.5.4 Open Source Tools

Awesome Open Source in their article ‘The Top 47 GDPR Open Source Projects’ showcase a wide variety of tools that can be used as a starting point for organisations when implementing a data protection programme. Another article from eComply, Top 10 Free GDPR Tools and Solutions, provides a good baseline for starting an assessment. However, not all the tools showcased are open source. IT Governance also provides a number of tools in their List of free GDPR Resources and Templates and SourceForge’s Best Free GDPR Compliance Software - 2021 Reviews & Comparison provides a large selection of tools. Again, not all are open source. OPENGDPR is an open source initiative, established by mParticle, AppsFlyer, Braze, and Amplitude, that sets a common framework for brands and technology companies to cooperate around the fair and transparent use of consumer data. Their first offering is for those looking for a starting point on Data Subject Access Requests and provides interoperability for Data Controllers and Data Processors. It is available in GitHub - opengdpr/OpenDSR in GitHub - opengdpr/OpenDSR.

Pluribus One have also provided a registry to track progress in the delivery of a data protection programme,
available at GitHub - pluribus-one/gdpr-registry-app. It can also be accessed at the GDPR Registry App with the login details of Username: gdpr and Password: pluribusone.

### 3.5.5 Self-build Guidance For AI

For those looking to deploy their own AI, there is guidance provided by TechGDPR that identifies the strategies for ensuring an organisation's AI is compliant to GDPR (and therefore adaptable to DAPA) - especially on automated decisions and subsequent explainability.

### 3.5.6 Commercial Tools

In Section 3.2.8: Addressing Unstructured Data, MonkeyLearn was used as an example to identify customer data in unstructured data. However, before commissioning the use of a specific tool, it is worth considering the organization’s own specific needs and then narrowing down and selecting a tool that can meet those needs. Various firms have developed commercial tools and solutions in response to the need to comply with the GDPR requirements, including:

- **ManageEngine DataSecurity Plus** with sensitive data discovery tools and file server auditing
- **Dathena** - an automated tool
- **MinerEye Data Tracker**
- **SourceForge also provides alternatives to MonkeyLearn** for handling unstructured data. Not all these tools are comparable to MonkeyLearn’s GDPR capabilities, but the following are a closer match:
  - **Keatext**
  - **Semantria**
  - **Luminoso**

A number of organisations have also provided an overview of tools that can be used:

36 [https://github.com/pluribus-one/gdpr-registry-app](https://github.com/pluribus-one/gdpr-registry-app)
41 [https://www.minereye.com/](https://www.minereye.com/)
42 [https://sourceforge.net/software/product/MonkeyLearn/alternatives](https://sourceforge.net/software/product/MonkeyLearn/alternatives)
43 [https://sourceforge.net/software/product/Keatext/](https://sourceforge.net/software/product/Keatext/)
44 [https://sourceforge.net/software/product/Semantria/](https://sourceforge.net/software/product/Semantria/)
45 [https://sourceforge.net/software/product/Luminoso/](https://sourceforge.net/software/product/Luminoso/)
3.5.7 Cloud Providers

Most cloud providers have started to also offer tools for the management of data. However, such services might be unavailable to some organisations given the restrictions on hosting data outside Kenya.

**AWS**

Amazon Web Services (AWS) has provided a dedicated section on their website on [compliance with GDPR when using AWS services](https://aws.amazon.com/compliance/gdpr-center/) with a number of articles on how they can help an organisation to comply with the GDPR requirements. In this section, Amazon directs their customers to [providers](https://aws.amazon.com/blogs/apn/how-aws-supports-customers-and-apn-partners-on-the-journey-to-gdpr-compliance/) that develop tools that can be used to ensure compliance.

**Azure**

Azure, the cloud computing service offered by Microsoft, outline some of the [new capabilities to enable robust GDPR compliance](https://azure.microsoft.com/en-gb/blog/new-capabilities-to-enable-robust-gdpr-compliance/) on their webpage. In the publication, the Azure team highlights some of the tools they offer their customers to accelerate the implementation of a data protection programme that is GDPR compliant. This is further complemented with guidance from Microsoft on the tools provided by Azure and other Microsoft Products and partners to [support compliance with GDPR](https://www.microsoft.com/security/blog/2017/12/19/how-microsoft-tools-and-partners-support-gdpr-compliance/).

**Google Cloud**

Google has provided a [GDPR Resource Center](https://cloud.google.com/security/gdpr/resource-center) including information on how they support the delivery of General Data Protection Regulation (GDPR).
Chapter 4
Implementation Examples

This section highlights examples and case studies of how enterprises, including fintechs in several markets, go about their compliance with what is regarded as best practice in data privacy and protection. In addition, it also showcases examples that do not uphold best practice and where improvements can be made. The objective is to showcase what good practice ‘looks like’, pulling out different examples on capturing consent, managing a data subject access request, complaints handling, and providing notices for transferring data to other jurisdictions.

4.1 Capturing Consent

Capturing consent for web-based interactions goes beyond capturing consent for the application of cookies to include consent for any other data created or collected when the consumer interacts directly with the organisation. Most organisations have taken consent management for cookies as sufficient to address data compliance, yet cookie data might not be all that is captured. Consequently, consent management should be expanded to capture consent for all types of data. For example, if an algorithm determines a customer’s gender based on their activity, the resultant output data relating to the customer is determined as ‘Sensitive Personal information’ and the organization should seek the customer’s consent to capture this data. Many organisations use the privacy policy on their website to cover such a stipulation, but this does not fully meet the requirement to separate the consent and contractual terms.

Technical data that is usually captured in cookies include:

- Internet Protocol (IP) address
- Login information (where applicable)
- Browser type and version
- Time zone setting and location
- Browser plug-in types and versions
- Operating system and platform
- Other technology information that may be available from the devices used to access the site

With the above in mind, it is imperative to provide the customer with sufficient information on the types of data collected as part of cookies to enable the customer to make an informed choice about whether to accept or reject the cookies. This assessment of the examples of good and bad practices tries to identify those that are customer-centric and provide a good user experience. In addition to the examples of capturing data consent, additional designs that create a good user experience are explored, including:

- Whether the cookie policy pops up when the user is on the home page.
- If there is no pop-up, whether there is a link to the cookie policy on the home page that a customer can refer to.
- If the policy gives the user the option to ‘accept’, ‘decline’, or ‘defer’ the decision for later.
- If there is a cookie policy, whether there are different preferences displayed that a customer can select, or whether it is a binary ‘accept’ or ‘reject’ option.

4.1.1 Examples that Meet the Data Capture Consent Requirements

Bluewave Insurance Agency

Bluewave Insurance Agency is a Kenya-based fintech that offers a range of micro-insurance products aimed at low-income users. This is a good, customer-centric example.

When the consumer lands on the home page, the cookie policy is displayed. Whilst there is no accept/decline or selection of preferences options, the ‘Learn more’ link takes the consumer to a different website with an educational video on what cookies are and how the company uses them.

---

55 https://www.bluewaveinsurance.co/
56 https://www.cookiesandyou.com/
The privacy policy clearly states what information is being collected, including sensitive data such as gender, but the policy does not differentiate sensitive data from other types of data.

**What personal information do we collect?**

We capture and store the following personal information: Name, Gender, Date of Birth, Physical Address, National Identity Card number, Passport number, Family details including names of children and spouse, Email address, Phone number and KRA PIN number.

Safaricom who provide mobile phone-based money transfer (MPESA) and INTERSWITCH who provide integrated digital payments are our 3rd party service providers and they will capture your personal information via our web applications and Mobile applications.

Interswitch collects payment details including credit card details such as credit card holder name, credit card number, credit card expiry date and the card security code.

MPESA collects payment details such as ID number, phone number and name.

We also collect health data in instances where we need to process a health related claim or for the provision of similar services.

**DLA Piper Africa**

DLA Piper Africa is part of a multinational law firm, with offices in several countries, whose website has a client-centric experience.

The home page immediately makes the cookies disclaimer visible, providing three options:

1. See our Cookie policy
2. Cookie settings
3. Accept cookies

---

57 https://bluewaveinsurance.co/privacy-policy/
When selecting the cookie settings, the below Privacy Preference Centre is displayed. Each of the preferences provides a layman’s definition of what is being collected and for what purpose.

The website allows the customer to select their location and language. Once a different location is selected, a pop-up is displayed where one has the option to make the new location their default location, and the notification that “Selecting a default location will set a cookie.”
The privacy policy gives the most recent update date as October 2020 and has a very clear structure to navigate, making it easy to access the information one is seeking, for example on the Information that is collected.

We may collect information directly, as well as from third parties or automatically related to the use of our Sites and Services.

Information we collect

We may collect personal information about you—such as your name, address, telephone number, fax number, e-mail address, etc.—directly from you. For example, personal information may be collected when you fill out a 'Contact Us' form, sign up for our mailing lists, register for events we host or sponsor, submit information as part of certain online services (eg, our Privacy Scorebox), post comments on our blogs, or otherwise provide us personal information through the Sites and Services. Generally, the information we collect includes your:

- Name, company name and title/position.
- Email address, phone number, mailing address and contact details.
- Contact preferences and interests.
- Business affiliations.
- For events, it may include dietary restrictions, requested accommodations and other event-related preferences.
- If you register for, attend or participate in CLEs that we make available, we may collect your Bar number and other information necessary for CLE credit and reporting purposes.
- Information provided in conjunction with our Client Services.
- Other information related to your request or inquiry, or that you provide when you communicate, engage or otherwise interact with us or the Services.

Last updated October 2020

Your privacy is important to us. This DLA Piper LLP (US) Privacy Policy (the "Privacy Policy") applies to the personal information that DLA Piper LLP US ("DLA Piper," "we" or "us") collects and explains our information practices and your related choices with regard to such information. We also collect health data in instances where we need to process a health related claim or for the provision of similar services.

1. Scope
2. Information we collect
3. Use of personal information
4. Disclosure of personal information
5. Cookies and similar devices
6. Direct marketing
7. International transfers
8. Access and correction
9. Third party websites and links
10. Co-sponsored events
11. Our commitment to security
12. How to contact us
13. Revisions to our Privacy Policy
14. Additional Privacy Information for California Residents

https://www.dlapiper.com/en/colombia/privacy-policy/#Information%20we%20collect
Automatically-collected information

We use cookies, log files, pixel tags, local storage objects and other tracking technologies to automatically collect information when users access or use the services or visit our Site, such as an IP address, general location information, domain name, page views, a date/time stamp, browser type, device type, device ID, Internet service provider ("ISP"), referring/exit URLs, operating system, language, clickstream data, and other information about the links clicked, features used, size of files uploaded, streamed or deleted, and similar device and usage information. For more information, see the Cookies and similar devices section below.

Information received from third parties

We may collect or receive information about individuals from service providers, and other third parties, such as our clients, representatives and professional advisers, content providers, government authorities and public sources and records.

Etsy

Etsy is a US e-commerce retailer with a global e-commerce platform. Not only does this retailer meet all the basic consent requirements, they also educate their customers, including those that are not registered. A cookie pop-up is immediately displayed to the consumer with an ‘accept’ or ‘update settings’ option, with the latter providing additional preferences if selected. The customer can also navigate backwards to change the preferences selected.

On the static footer of the website there is a ‘Privacy settings’ option under the ‘Help’ category. When a consumer selects this option, it displays a further option that allows the customer to personalise their advertising.

62 https://www.etsy.com/
63 https://www.britannica.com/topic/Etsy
Etsy’s cookie policy informs its customers that the data collected as part of the cookies is for ‘beyond just advertising’. A previous version of the policy is also available to the consumer, which can be referenced if a dispute was logged prior to the current policy coming into effect.

The contents breakdown has been well structured, with the information in layman’s terms and therefore easy to understand and follow. Additional information, together with links to the various advertising service providers, i.e. TrustArc’s preference manager, are provided, enabling the customer to manage all of their advertising choices, not just those on Etsy’s site.

Etsy does not distinguish between sensitive and non-sensitive data. However, in the privacy policy paragraph 2 “Information Collected and Received”, they clearly state the type of personal data that is collected.

https://www.etsy.com/legal/cookies
https://preferences-mgr.truste.com/
https://www.etsy.com/legal/privacy
JUMO

JUMO is a South African fintech that provides a mobile financial services platform.

When a consumer lands on the home page there is no cookie pop-up. However, the Privacy Policy, Cookie Policy, Responsible Disclosure, Terms of Use etc. are located on a static banner on the footer of the page. The banner is available on every page that one navigates to. There is no need to scroll down to find the quick link each time the user wants to reference back. While this is a very customer-centric approach, it does little to help a consumer who wishes to block the cookies.

On the plus side, one of the commendable ‘tech stack features’ is their ‘Data privacy & responsible banking’ message.

Even though a cookie policy pop-up is not presented, a customer can reference their browser cookie settings to create cookies that align with the policy.

When a consumer selects the cookie policy link there is a section titled ‘Change your cookies settings’ where generic information is provided, and a link to ‘All about Cookies’ that takes the user to a page that gives more information on what cookies do.

In their privacy policy, JUMO advises their customers when the page was last updated, goes on to outline what data is collected, and distinguishes between sensitive and non-sensitive personal data. JUMO then goes further by informing its customers how their personal information is collected, in paragraph 5 of the privacy policy.

5. How is your personal information collected?

We use different methods to collect information from and about you:

1. Direct interactions. You may give us your personal information when registering on or submitting information through any JUMO website or by corresponding with us by post, phone, email or otherwise. This includes Personal Data you provide when you:
   • create an account on any of our platforms
   • subscribe to our service or publications
   • as part of our contractual agreement through accepting our product terms and conditions
   • request marketing to be sent to you;
   • apply for an employment vacancy
   • enter a competition, promotion or survey
   • give us feedback or contact us directly; or
   • provide feedback or contact any of our partners

2. Automated technologies or interactions. As you interact with our website, we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies and other similar technologies. We may also receive Technical Data about you if you visit other websites employing our cookies.

We also collect, use and share Aggregated Data such as statistical or demographic information for any purpose. Aggregated Data could be derived from your personal information but it will not directly or indirectly reveal your identity.

67 https://www.jumo.world/
68 https://www.jumo.world/cookie-policy/
69 https://www.allaboutcookies.org/manage-cookies/
70 https://www.jumo.world/privacy-policy/
**Luno**

*Luno* is a South African fintech cryptocurrency platform. A cookie pop-up is not presented when the home page is opened. When the consumer selects the privacy policy and the link to "How we use cookies"\(^ {72} \), details on what data is collected and how a consumer can delete cookies is provided.

For information on how to delete or reject cookies, you can consult the "help" function within your browser, or visit [www.allaboutcookies.org](https://www.allaboutcookies.org), where you will also find more information data about cookies generally.

Luno provides a privacy policy\(^ {73} \) which shows the last update occurring at March 2021.

If specific customers need to be aware of items that are unique to them, Luno provides ‘special notes’ that make this information very visible. These are found in the privacy paragraph ‘How we share personal data’. Luno clearly states what information will be shared, and the purpose for sharing, so a consumer can judge for themselves what data is being provided.

---

**OLX**

*OLX*\(^ {74} \) is an Egyptian e-commerce retailer that connects local people (on global sites) to buy, sell or exchange used goods and services, and provides a good example.

When a consumer lands on the home page, there is no cookie pop-up. When a consumer navigates to the bottom of the home page the Privacy policy\(^ {75} \) is displayed with a link.

Despite the lack of a cookie pop-up, this is still a good example, because there is an ‘Articles in this section’ menu option, where the ‘Policy on Cookies and Similar Technologies’\(^ {76} \) is available.

---

\(^ {71} \) [https://www.luno.com/](https://www.luno.com/)


\(^ {74} \) [https://www.olx.com.eg/en/](https://www.olx.com.eg/en/)


Within the cookie policy, the, what, why, what kind and with who (third party) are explained. The consumer is also educated on how to go about managing the cookies.

The privacy provides a clear explanation and detailed view of what personal data will be collected, and includes a section specifically aimed at children. What the policy does not do is distinguish between sensitive (i.e. gender) and non-sensitive data.

**Pepper.pl (Google translate used)**

Pepper.pl is a Polish fintech e-commerce retailer. On the home page, cookie pop-up and cookie settings are displayed that a consumer can select from. Until a consumer makes a choice about the use of cookies, they cannot continue.
Pepper.pl has taken the cookie policy and provided the consumer with the data fields they collect, and a definition in layman’s terms. From a consumer perspective, unless you are a developer or business analyst, this is possibly far too granular – but provides clarity on what specific files are used for.

Pepper.pl has a unique way of displaying how personal data is processed, and what the data is used for, in a simple table format found in the privacy policy.

4. What types of data do we process?

We process various types of personal data:

<table>
<thead>
<tr>
<th>Personal data you must provide: Depending on how you use our services, you will need to provide certain categories of personal data.</th>
<th>Account information (email address, username, password)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Information You May Provide: When you use our services, you will need to provide certain categories of personal information.</td>
<td>Additional information (name, surname, alias, your description)</td>
</tr>
<tr>
<td>Your activity (your: occasions, discussions, comments, saved threads, likes, keyword alerts, filters, searches, private messages)</td>
<td>Results of our surveys (e-mail address and behavioral data)</td>
</tr>
</tbody>
</table>

6. Why and for what do we use your data?

We need to process your personal data for several reasons that are legally justified. Processing is lawful when:

- it is necessary to perform the contract or take action before its conclusion,
- it is necessary to fulfill a legal obligation,
- it is necessary for the purposes of legitimate interests, or
- the data subject has consented to it.

Y OU HAVE THE RIGHT TO WITHDRAW YOUR CONSENT AND OBJECT TO THE PROCESSING BASED ON YOUR LEGALLY REASONABLE INTEREST FOR THE PROCESSING OF THE DATA MENTIONED ABOVE, AT ANY TIME, OR CONTACT US.

We collect, process and use the following personal data for the following purposes:

<table>
<thead>
<tr>
<th>OBJECTIVE</th>
<th>LEGAL BASIS</th>
<th>TYPE OF PERSONAL DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration and login</td>
<td>Agreement</td>
<td>Account information</td>
</tr>
<tr>
<td>Provision of services</td>
<td>Agreement</td>
<td>Account information, additional information, your activity and trends</td>
</tr>
</tbody>
</table>

Polskie ePlatności (Google translate used)

Polskie ePlatności is a Polish e-commerce fintech which is customer centric in a variety of ways. When the home page is opened, the message ‘How can we help you?’ is displayed, with the ‘cookie policy’, whereby the following options are available: Not now / I’ll decide later / Done.

If the ‘done’ option is not selected, the cookie policy will pop up again every time a new page is visited, and to the same Not now / I’ll decide later / Done options are presented. This is potentially frustrating from a customer-centricity perspective.

78 https://www.pepper.pl/cook ies-policy
79 https://www.pepper.pl/privacy-policy
80 https://www.pep.pl/
II. WHO PROCESSES YOUR DATA

In addition, the Policy also determines the method we apply to protect your data, the rights you enjoy and how you may exercise these rights. There have been also indicated the tools to manage your consents and authorisations.

Content of the document

The data we collect include specific objects for which they are used. PeP as well as the methods of their usage, and making them available, as well as the users' use of the Websites of Centrum Rozlicze Elektronicznych Polskie eP (hereinafter referred to as the "Policy"). The Policy provides for the specified types of data collected through the Website and the rules of collecting, storing and accessing to the information on the user's devices, among other things, using the cookie files, in relation to the Privacy Policy.

Privacy Policy

I. PRELIMINARY INFORMATION

Clear options are provided that a consumer can select from, but there is no option to select or deselect essential cookies.

2. Cookie files and pixel markers

When you use our Website, the information, which often constitute personal data, is downloaded from your search engine and then saved. The collected data include, for example, the data in the form of cookie files and pixel markers. These files allow to identify the software you use and adjust individual preferences. Cookie files usually include the name of domain from which they originate, time of their storage on the device and assigned value; they also contain the data concerning the activity in the Website.

Cookie files and pixel markers are used to gather the information related to your use of the Website. The cookie files specifically allow to:

a) maintain your session (after log-in) and you do not need to enter a log-in and password on any subpage;

b) adjust the content of websites to your preferences and optimize the usage of websites; and, specifically, these files allow to recognize your device and, respectively, display the website that is tailored to your needs;

c) verify the method of your using the website and creating statistics which help grasp how other users use

The opening page of the privacy policy is customer centric because of the visual display of what information will be covered in the policy, instead of it being left as a text-heavy legal document.

The type of data collected is described in broad statements, and does not go into the detail seen in other examples; because the site does not require sensitive data, this has not been provided as a data type.

81: https://www.pep.pl/polityka-prywatnosci
STATSports

STATSports is a Northern Ireland retailer, specialising in sports equipment, that collects vast quantities of data from the consumer, who is presented with the cookie pop-up at the bottom of the screen with the option to either close or read the policy.

There is a privacy policy that covers the STATSports general process. This clearly identifies what information is collected, but includes when they might need to share this information to others, for example Klarna to facilitate a Buy Now Pay Later transaction. A link is then provided to Klarna’s privacy policy. General parties who might receive the consumer’s data are described in the “How information is shared” section.

HOW INFORMATION IS SHARED

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. The following third-party service providers process personal information about you for the following purposes: AWS (Amazon Web Services) and Shopify.

As their product lines delineate different approaches to the sharing of data (the ‘Pro’ data is not shared), there are privacy policies for each of these product lines, e.g. APEX athlete series, Coach series, Pro series, and Team series.

82 https://statsports.com/
83 https://statsports.com/privacy
Below are two separate screenshots for the APEX team series and APEX Pro Series. STATSports collects different data and have different procedures from their devices, and have taken the approach of ensuring customers are aware what data is collected and how it will be used.

**APEX TEAM SERIES PRIVACY POLICY**

**STATSPORTS PRIVACY NOTICE**

_Last updated: May 2018_

At STATSports we are committed to protecting the privacy and security of your personal information. We have developed this privacy notice to describe how we collect, use, share and store your personal information when you use the STATSports website, mobile app and/or STATSports wearable devices (our “Services”).

Within this Privacy Notice we will cover the following topics, to go to a specific section, please just click the relevant link below:

- **About us and this notice**
- The information we collect and how we collect it
- How we use the information we have collected
- How information is shared
- Storage and security
- Notice in respect of children
- Retention of your personal data
- How to access or delete your data

**APEX PRO SERIES PRIVACY POLICY**

**STATSPORTS PRIVACY NOTICE**

_Last updated: May 2018_

At STATSports we are committed to protecting the privacy and security of your personal information. We have developed this privacy notice to describe how we collect, use, share and store your personal information when you use the STATSports website, mobile app and/or STATSports wearable devices (our “Services”).

Within this Privacy Notice we will cover the following topics, to go to a specific section, please just click the relevant link below:

- **About us and this notice**
- The information we collect and how we collect it
- How we use the information we have collected
- How information is shared
- Storage and security
- Notice in respect of children
- Retention of your personal data
- How to access or delete your data

---


Vodacom

Vodacom is an international mobile communications company. The South African site was accessed as an example due to POPIA. On the home page, there is a cookie policy where the user can activate different consent preferences. Unless a consumer accepts or manages the cookies, they cannot continue to navigate the site.

A variety of consent preferences are presented, each with a noticeably clear and concise definition in layman’s terms.

On the privacy policy page, the consumer is presented with a visual display of the different data privacy categories to select from. Vodacom does not distinguish between sensitive and non-sensitive data.

It is worth noting that although a consumer may consider this data sensitive, the calculation of all fees and bills requires the capture of phone numbers that a consumer calls or sends messages to, along with all associated data. This excerpt can be found in the privacy policy in the ‘Personal Information we collect about you’ section, under the heading: “We can get your personal data when you:”

We will also get information on how you use our products and services, such as:
- The phone numbers that you call or send messages to (or the phone numbers that you receive calls and messages from),
- The date, time and length of the calls and messages you send or receive through our network, and your approximate location at the time these communications take place.

This makes it clear that the information is captured, including a customer’s approximate location – all of which is needed to establish communication and charge for services.

---

86 https://www.vodacom.co.za/
87 https://www.vodacombusiness.co.za/vodacom/privacy-policy/terms
4.1.2 Examples that Do Not Meet the Capture Consent Requirements

**A. MWEBESA & Company Advocates**

A. MWEBESA is a Uganda-based law firm. When the home page opens, there is no cookie pop-up. Under the Quick Links heading at the bottom of the home page a link is provided to the Privacy Policy. When the user selects the hyperlink, they are diverted back to the top of the page, irrespective of what page they are currently on.

The remainder of the Quick Links functionality was further tested, and again performed poorly:

1. Sitemap: request for URL was not found on this server
2. Privacy policy: not available and navigates back to the Contact Us page
3. Terms of Use: same as the privacy policy’s functionality
4. Contact Us: email, contact number and office location are displayed
5. Request Consultation: System generated Request Consultation form
6. Webmail: diverted to the below where the user is requested to enter their address and password, which they are not registered for.

**Assihub**

Assihub is an e-commerce retailer in Togo. There is no cookie pop-up on the home page. At the bottom of the home page are messages on Confidentiality and Terms and Conditions, with ‘click here’ links for more information.

---

88 [https://amwebesa.com/](https://amwebesa.com/)
90 [https://amwebesa.com/sitemap.xml](https://amwebesa.com/sitemap.xml)
91 [https://amwebesa.com/index.html#consult](https://amwebesa.com/index.html#consult)
92 [https://amwebesa.com:2096/](https://amwebesa.com:2096/)
93 [https://assihub.com/](https://assihub.com/)
The ‘Confidentiality’ link is the Privacy policy and provides a basic outline of privacy policy, use, and persons concerned. No reference is made to data protection legislation. The policy does not state what data is captured.

Your privacy is very important to us.

It is ASSIHUB’s policy to respect your privacy regarding any information we may collect while operating our website. Accordingly, we have developed this privacy policy so that you understand how we collect, use, communicate, disclose and use personal information. We have described our privacy policy below.

We collect personal information by lawful and fair means and, where applicable, with the knowledge or consent of the person concerned.

Before or when collecting personal information, we will identify the purposes for which information is being collected.

We collect and use personal information only to fulfill the purposes specified by us and for other ancillary purposes, unless we obtain the consent of the individual concerned or as required by law.

Personal data must be relevant to the purposes for which it is to be used and, to the extent necessary for those purposes, must be accurate, complete and up to date.

We will protect personal information using reasonable security safeguards against loss or theft, as well as unauthorized access, copying, use or modification.

We will make available to customers information about our policies and practices relating to the management of personal information.

The cookie policy is a reference in the privacy policy and covers sections 6 and 7, which do not outline which personal data is collected whilst navigating the site.

SECTION 6 - AGE OF CONSENT

By using this site, you represent that you are at least the age of majority in your state or province of residence or that you are the age of majority in your state or province of residence and that you have given us your consent to allow Your minor dependents to use this site.

SECTION 7 - CHANGES TO THIS PRIVACY POLICY

We reserve the right to modify this privacy policy at any time, so review it frequently. Changes and clarifications will come into effect immediately after their publication on the site. If we make any material changes to this policy, we will notify you here that it has been updated so that you are aware of what information we collect, how we use it and under what circumstances, if any, we use and / or disclose it.
Jacquie Creations

Jacquie Creations is a Togolese e-commerce platform. The ‘cookies’ pop-up is presented at the bottom of the home screen, but no preferences are available for selection. The site does not have any legal policies available. While navigating the site without accepting cookies, the page loads are faster; once cookies are accepted, the speed at which the pages render slows significantly.

The cookie functionality seems to have been created to conform to the most basic data protection legislation.

MiFinity

MiFinity is a Northern Ireland fintech. In addition to noting all the policies, MiFinity aims to instil a sense of security with ‘DigiCert Trusted and PCi DSS certified’ certifications.

A cookie pop-up is presented at the bottom of the screen:

Due to the structure of the licensed entities, MiFinity provides two distinct privacy policies for UK and non-UK residents.

1. UK: Northern Ireland Entity
2. Non-UK: Maltese Entity

Both policies are identical, but for the Company and Contact Information. Unfortunately, MiFinity creates uncertainty is in the Your Rights section, where the user is advised they can withdraw consent, but that this may end the service with MiFinity. This approach creates an unnecessary obstacle.

https://jacquiecreations.com/
https://www.mifinity.com
Makro.co.za

Makro is an e-commerce retailer. As Makro has physical stores in South Africa, many South Africans used the online store to purchase essential goods in bulk during stage 5 of the COVID pandemic. More registered users means more data, so protecting personal information is now more important than ever.

As the home page opens, there is no cookie policy pop-up, but 14 cookies are created. The privacy policy is at the very bottom of the page, along with the terms and conditions.

The privacy policy is a basic one, and personal information is captured when the user creates an online profile. Makro confirms in the ‘Use of your information’ section that the user can manage communication preferences ‘here’ – without providing a link or clarification of where ‘here’ is.
Makro confirms it will personalise the site based on the user’s activity, but also advertises to that user based on the fact of their visit to the website. Thus the user is tracked when they visit other stores, an issue Makro does need appear concerned about managing.

Oel Marketplace (Google translate used)

Oel Marketplace 99 is a Togolese e-commerce retailer. There is no cookie pop-up, and a legal link at the bottom of the home page. This link opens substantially more slowly than any other page, and is also full of adverts.

The first time that a privacy policy is made available is on the Registration page 100. The policy makes no reference to data protection legislation and there is no reference to what and how the data will be used, only that a seller may not “collect in any way information about users, including e-mail addresses, without their consent”.

How this is applied in reality is uncertain, as the user must first register as a ‘salesman’.

99 https://oel.tg/
100 https://oel.tg/politique-de-confidentialite/
Shopee

Shopee is a Singaporean-owned company, but the example selected was for Indonesian users. There is no cookie pop-up; in the privacy policy the cookie policy in paragraph 5 elaborates what data is collected and how it is used. However, there is no distinction made between sensitive and non-sensitive data. The clause 3.1 states that the personal data Shopee collects includes but is not limited to the data described in the policy.

SOUQ

SOUQ is an Egyptian (Saudi Arabian) e-commerce platform that sells retail goods; it is a poor example of best practice despite being a subsidiary of Amazon.

The privacy policy and terms and conditions link is available, after a long scroll, at the bottom of the home page. The last update to the privacy policy was 20/9/2018.

3. WHAT PERSONAL DATA WILL SHOPEE COLLECT?

3.1 Personal data that Shopee may collect includes but is not limited to:

- name;
- e-mail address;
- date of birth;
- billing address;
- bank account and payment information;
- telephone number;
- gender;
- information sent by or connected to the device(s) used to access our Services or Platforms;
- information about your network and the people and accounts you interact with;
- photos, including photographs taken for the purpose of submitting proof of delivery electronically, or audio or video recordings that you share with us;
- government-issued identification or other information necessary for our due diligence, getting to know your customers, identity verification, or fraud prevention purposes;
- any other information about the User when the User registers to use our Service or Platform, and when the User uses the Service or Platform, as well as information relating to how the User uses our Service or Platform; and
- all data about the content used by the User.

101 https://shopee.co.id/
102 https://shopee.co.id/docs/3612
103 https://deals.souq.com/eg-en
104 https://egypt.souq.com/eg-en/privacy-policy/c
Takealot.com

Takealot.com is a South African e-commerce retail store whose ethos is “Our customers come first.” Service delivery is the foundation on which this company has been built.

A cookie pop-up is not displayed on the home page, but the cookie policy can be found in the Terms and Conditions via a link at the bottom of the home page, where a customer would not necessarily think to look.

Paragraph 15 addresses data consent, and what personal data is collected; no mention is made regarding the use of sensitive data, even though gender is captured. In clause 15.5 that will not be done without express consent is stated, but in clause 15.15, the following statement is made: “If you do not disable ‘cookies’ you are deemed to consent to our use of any personal information collected.”

TymeBank

TymeBank is a digital-only bank in South Africa. When the home page opens there is a cookie pop-up which states the user can change their cookie settings at any time, without confirming how; a link to the cookie policy is given, which provides all the details of what data is being collected, and includes information about targeted advertising.

105 https://www.takealot.com
106 https://www.takealot.com/help/terms-and-conditions
107 https://www.tymebank.co.za/
In the privacy policy\textsuperscript{109} TymeBank makes it clear that the policy is governed by PAIA (Promotion of Access to Information).

When a consumer references the privacy policy (PAIA compliance aside), there is ambiguity around exactly what TymeBank is accountable for (see graphic on next page). The customer is required to read all documents carefully. This shifts ‘accountability’ to the consumer and is not customer centric.

The data collected below is more specifically related to a credit application.

Two potential problems were identified:

1. Biometric information, referring to data such as fingerprints. POPIA makes allowances for this, but the term is open to interpretation. Please refer to Werksmans discussion points on Biometrics and POPIA\textsuperscript{110}

2. There is a lack of further explanation of terminology; for example not every customer would understand the term ‘IP address’.

\textsuperscript{109} https://www.tymebank.co.za/legal/privacy-policy/

\textsuperscript{110} https://www.dataguidance.com/opinion/south-africa-use-biometric-information
4.2 Managing Data Subject Requests

Every consumer has the right to ask the responsible party to access, update or delete personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully. We, identified four channels that can facilitate this customer-centric functionality:

- Online application request form
- Email
- Formal letter
- Telephone

4.2.1 Good Practises on Managing Data Subject Requests

Bluewave Insurance Company

The privacy policy confirms the consumer’s rights when it comes to the access, update, and deletion of their personal data. Other than a generic “How to Contact us” link, the consumer is not provided with the channel by which they can log a request, but in the absence of guidance from the Data Commissioner’s office, they may have erred on the side of caution.

Rights regarding your personal information

- You have the following rights in respect of any personal data we hold
- Right to be informed of the use to which their personal data is to be put
- Right to object to the processing of all or part of your personal data
- Right to request confirmation of what personal data we hold for you
- Right to request that we correct any errors, omissions, out-dated, inaccurate, incomplete or misleading data, and request third parties processing your data of the same, this will however not apply to personal data required for the purposes of evidence and we shall instead of erasing or rectifying, restrict processing and inform you within a reasonable time.
- Right to request that we no longer use the information to contact you
- Right to request removal from any contact / mailing list we have the data on
- Right to request that we restrict our use of your data
- Right to request that we delete personal data that is authorised to retain, irrelevant, excessive or obtained unlawfully, and request third parties processing your data of the same, this will however not apply to personal data required for the purposes of evidence and we shall instead of erasing or rectifying, restrict processing and inform you within a reasonable time.
- Right to request that we transfer your data to another organisation
- It is our intention that we will resolve any issue you may have with regard to data privacy

https://bluewaveinsurance.co/privacy-policy/
A data subject access request online took one minute from start to finish. This might take longer for customers with more history, but nonetheless the process mitigates the 'negative' aspects of data management and highlights the fact that the customer can be part of the company’s thinking.

From within this page, the user can clear recently viewed listings, request data and request deletion of data.

Within 30 seconds a confirmation is sent – the first validation they are dealing with the same customer. There is a link in the mail to a validation page.
Hi [First name of data Subject],

We have received your data access request to download your personal information. For security and verification purposes, please confirm this request by clicking the button below.

Confirm my Etsy personal data download

Once you confirm your request, you will be able to download a ZIP file of your data in both CSV and JSON formats for two weeks. You can make additional requests to download your data after the two-week period has elapsed. The downloaded data contains personal information. Please keep the link private and download the file to a safe location. If you didn’t request access to download this information, please report the issue to Etsy Support.

The link 'Confirm my Etsy personal data download' takes the user to another page, which then allows a return to the account’s Privacy Settings:

Here, the user is informed, “You can now download your data.”

At this point the user is asked to authenticate with their password - again to ensure only the customer has the required access. A zip file can now be downloaded containing all of the user’s data.
JUMO

A **right to access** is documented under “Your rights as a data subject” on the privacy policy portion of the site. The user is provided with email access or the option to write a formal request, via a link that takes them directly to the **contact us page** to obtain the address. The toggle functionality gives the country and contact details.

Luno

The user’s **right to access, update, or remove personal data** would appear to need further explanation and refinement on the Luno website. The process and procedures are not well defined. Whilst there is the functionality to submit a **support ticket**, the link does not take the user to a page where the request can be submitted, but to a page that asks, “What’s your message about?” From a customer centricity perspective, this is not ideal.
While the privacy policy provides the consumer with their rights in terms of access, correction and right to object, the consumer is not provided with any communication channel in this specific paragraph to request any of said rights:

The consumer does have the ability to edit/delete their data on their personal profile. The ‘how to’ can be accessed via the ‘Help Centre’, and by selecting ‘Accounts and My Ads’.
How can I edit/delete my ads?

To edit or delete your ad follow the below steps:

- Login to your account. Register if you don’t have an account.
- Click on your name on the top right.
- Click on “Ads.”
- You will see a list of your ads and the option to edit or deactivate an ad.

Once you deactivate an ad it will be moved to “My archived ads.” From this tab you can choose to delete your ad permanently or you can activate it again by clicking on “Activate ad.”
Pepper.pl

The Pepper website is a good example of a customer-centric experience when a customer wants to access, change, delete or update their personal information. Below is the ‘how to’ found in Pepper’s privacy policy. Data can be downloaded directly from the website, and the process, procedure and functionality gives the customer full ownership and control without forcing them to submit a formal request.

<table>
<thead>
<tr>
<th>The right to rectify data</th>
<th>You can do this by going to your account settings where you can update your data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The right to be forgotten</td>
<td>You can exercise this right by going to your account settings. In the &quot;Profile!&quot; section you will find the &quot;Delete Account&quot; button. We'll keep your account and data for 30 days and then be permanently deleted. If you change your mind, you can reactivate your account by signing in again (within 30 days). In the event that your account is suspended or permanently blocked, you can access it in restricted mode, which will allow you to delete your account. Please note that some of your personal data may be stored in accordance with the seventh section of this privacy policy.</td>
</tr>
<tr>
<td>Right to access / transfer data</td>
<td>You can exercise this right by going to your account settings. In the &quot;Profile!&quot; section you will find the &quot;Download Data&quot; button. You will receive an email notification when they are ready to download. You can generate data every two weeks. In the event that your account is suspended or permanently blocked, you can access it in restricted mode, which will allow you to download your data.</td>
</tr>
</tbody>
</table>

Poradnik Pracownika (Google translate used)

Email or formal letter options are provided.

119  https://www.pepper.pl/privacy-policy#rights
120  https://poradnikpracownika.pl/polityka-prywatnosci
**Shopee**

The method for the requesting of access to and correction of personal data is customer centric and described in the privacy policy clause 13.2.1 below:

13.2 Requesting Access to or Correction of Personal Data

13.2.1 If you have an account with us, you can access and/or correct your own personal data that we currently have or control through the Account Settings page on the Platform. If you do not have an account with us, you can request to access and/or correct your personal data that we currently have or control by sending a written request to us. We will need enough information from you to confirm your identity and the nature of your request so that we can handle your request. Therefore, please submit your request in writing by sending an email to our Personal Data Protection Officer at the email address dpo.ico@shopee.com.

**SOUQ**

This site offers the ability for consumers to access, correct, and delete their data in writing via an email option found on the “Customer Support” link, but no email address could be found there. The following information is provided in the privacy policy:

Accessing, reviewing and amending your personal information

1. You can access and review your personal information in the My Account section of the Site. If your personal information changes in any way or is incorrectly presented on the Site you should immediately update or correct your personal information (as applicable) by accessing the My Account section on the Site or, alternatively, by contacting our customer support team. The “Customer Support” link on the top of each Site webpage contains our customer support email and phone details.

2. Please note that we shall retain your personal information during and following the end of your use of the Site as required to comply with law, for technical troubleshooting requirements, to prevent fraud, to assist in any legal investigations and to take any other actions otherwise permitted by law.

**STATSports**

On the legal page the consumer is informed of all the rights extended by GDPR, including requesting access to the data and its removal. The consumer can send an email or select the ‘request now’ option, where an online request form opens for the consumer to complete with the necessary details.
For the APEX Pro Series and APEX Team Series, the process is via email and can be found in the privacy policy in the ‘How to Access or Delete Your data’ section.

10. We’re here to help

If you want to update your personal information, have a concern about privacy, need more information or want to update your preferences, were just a phonecall away.

If you have a query, need to access your personal information, make a correction or lodge a complaint, please call 0860 999 119.

TymeBank

Requests are permitted via telephone. Unless the call is recorded, there is no evidence a customer has called to complain about, change, delete or even update their information.

4.2.2 Bad Practises on Managing Data Subject Requests

DLA Piper Attorneys

The process for contacting DLA Piper to gain access to personal data is not provided.

Although there is a “Contact Us” online form, the “type*” dropdown list did not have data access as an option.

13. How to access your information and your other rights

You have the following rights in relation to the personal information we hold about you:

- **Your right of access**
  If you ask us, we’ll confirm whether we’re processing your personal information and, if necessary, provide you with a copy of that personal information (along with certain other details). If you require additional copies, we may need to charge a reasonable fee.

- **Your right to rectification**
  If the personal information we hold about you is inaccurate or incomplete, you are entitled to request to have it rectified. If you are entitled to rectification and if we’ve shared your personal information with others, we’ll let them know about the rectification where possible. If you ask us, where possible and lawful to do so, we’ll also tell you who we’ve shared your personal information with so that you can contact them directly.

- **Your right to erasure**
  You can ask us to delete or remove your personal information in some circumstances such as where we no longer need it, or if you withdraw your consent (where applicable). If you are entitled to erasure and if we’ve shared your personal information with others, we’ll let them know about the erasure where possible. If you ask us, where it is possible and lawful for us to do so, we’ll also tell you who we’ve shared your personal information with so that you can contact them directly.

---

126 [https://statsports.com/apex-team-series-privacy-policy/#_HOW_TO_ACCESS](https://statsports.com/apex-team-series-privacy-policy/#_HOW_TO_ACCESS)
Werksmans Attorneys

Whilst the privacy policy states the client’s legal rights, information about how to access, update, change or delete data is not provided. Only contact details for the Data Protection Officer are provided at the end of the policy.

12 YOUR LEGAL RIGHTS

You may have rights under the South African and other laws to have access to your Personal Information and to ask us to rectify, erase and restrict use of, your Personal Information. You may also have rights to object to your Personal Information being used, to ask for the transfer of Personal Information you have made available to us and to withdraw consent to the use of your Personal Information.

The below list of companies did not include any reference to a privacy policy on their websites:

- MWEBBESA & company advocates
- Assihub
- Jacquie Creations
- Lidao

4.3 Managing Complaints

For every instance there should be a DPO role that a consumer can contact if they have a complaint. The contact details for the DPO, i.e. email address and physical address, need to be made available. Again, only examples where this role has been clearly defined, and a process and procedure (whether by email or via an online request) is made available to the consumer, have been included below.

4.3.1 Good Examples

- Bluewave insurance company (however, they do not identify their DPO)
- Etsy
- MiFinity
- Pepper.pl
- Shopee
- SimilarWeb
- STATSport

4.3.4 Bad Examples

- OLX

4.4 Cross-border, International and / or Third Party Data Transfers

The transfer of specific personal data is sometimes required, depending on different categories as per the list below. This section examines whether the privacy policy has a specific clause/s that provides for any data transfers. Every example that has been provided must at least make reference to third party data transfers.

- When a third party is requesting the data, e.g. for legal/regulatory reasons.
- If the business facilitates cross-border or international transfers for either transactional or financial purposes, and then indicates whether the information is available to the consumer.

Only a list of good examples has been provided, as links to the privacy policies have been made available in the “Capturing Consent” examples, and the specific information in relation to whether the clause/s are available are included in those privacy policies.

4.4.1 Good Examples

- Bluewave insurance company
- DLA Piper Africa
- Etsy
- JUMO
- Luno
- Makro
- MiFinity
- OLX
- Pepper.pl
- Polskie ePłatności
- Poradnik Pracownika
- Shopee
- SimilarWeb
- SOUQ
- STATSport
- takealot.com
- Vodacom
- Werksmans Attorneys
Appendix 1

Survey Questions Asked

<table>
<thead>
<tr>
<th>General Questions</th>
<th>1-10 / 11-50 / 51-250 / 251-1,000 / 1,001-5,000 / Greater than 5,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size of Company in Employees</td>
<td></td>
</tr>
<tr>
<td>Type of Company</td>
<td>Bank / Payments Company / Digital Lending Company / Insurance Company / Aggregator / Online Market Place provider / Other (please specify)</td>
</tr>
<tr>
<td>Type of Personal Data Processed</td>
<td>KYC / Background Checks / Payments Data / Credit History / Social Network Mapping / Other (please specify)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Protection Awareness</th>
<th>Yes / No / Unsure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are you aware of the Kenyan Data Protection Act 2019?</td>
<td></td>
</tr>
<tr>
<td>Do you know who the Kenyan Data Commissioner is?</td>
<td></td>
</tr>
<tr>
<td>Are you aware of the European General Data Protection Regulations (GDPR) or California Consumer Privacy Act (CCPA)?</td>
<td>Yes / No / Unsure</td>
</tr>
<tr>
<td>Do the European and Californian regulations also apply to you?</td>
<td>Yes / No / Unsure</td>
</tr>
<tr>
<td>Do you have a Data Protection Officer?</td>
<td>Yes / No / Unsure</td>
</tr>
<tr>
<td>If ‘No’, do you plan to recruit one?</td>
<td>Yes / No / Unsure</td>
</tr>
<tr>
<td>What is the seniority of the role in the organisation?</td>
<td>General Employee / Director reporting to board / Board Member / Other</td>
</tr>
<tr>
<td>Do you share data with other parties?</td>
<td>Yes / No</td>
</tr>
</tbody>
</table>

- If yes, what controls do you have in place to manage the sharing of that information?

  Updated Customer Contracts / Customers asked for permission to share / Customers asked for permission to share with clear reasons / Customers asked for permission at start of contract / Customers asked for permission as they make changes to existing services and new providers required / General purposes of the sharing provided to the customer / Specific name of the partner shared with provided to customer / Customer information securely shared without contract request / Other (please specify)
### Controls in Place to Protect Customer Data

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What policies and procedures have you implemented or improved in light of the Act?</td>
<td></td>
</tr>
<tr>
<td>Have you implemented a programme to deliver the requirements of the Act?</td>
<td>Yes / No</td>
</tr>
<tr>
<td>• If yes - how long has it been running?</td>
<td>A few weeks / 1-3 Months / 4-6 Months / 7 Months to a year / Modified existing long-term project</td>
</tr>
<tr>
<td>• What solutions have you implemented to support you in delivering the requirements?</td>
<td></td>
</tr>
<tr>
<td>How are you controlling data access within your organisation?</td>
<td></td>
</tr>
<tr>
<td>How do you plan to manage Data Subject Access Requests?</td>
<td>Not sure at this time / Manual process / Manual process with some tools / Semi-automated process / Fully automated process / Other (please specify)</td>
</tr>
<tr>
<td>How are you managing your unstructured data?</td>
<td>Not sure at this time / Manual process / Manual process with some tools / Semi-automated process / Fully automated process / Other (please specify)</td>
</tr>
</tbody>
</table>

### Looking beyond Implementation

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What are the opportunities you see from the Act?</td>
<td></td>
</tr>
<tr>
<td>What are the challenges the Act presents (not addressed above)?</td>
<td></td>
</tr>
</tbody>
</table>
The advantages of taking a customer-centric approach to data protection and leveraging the same as a key competitive differentiator have already been highlighted. For agile organisations, the opportunity to set themselves apart and differentiate themselves in their respective market should not be overlooked. For some fintechs, their skills and experience will put them in a strong position to act as a data processor for other organisations. In a similar way, organisations that provide IT services to financial services companies can easily expand their service offerings to include data protection as a service.