Data Privacy and Protection in Kenya: A Regulatory Review

January 2022

fsd Kenya

Creating value through
inclusive finance

MFX
MOBILE | FINANCE | DIGITAL

Data privacy and protection in Kenya: A Regulatory Review

Authored by:
Rob Reeve
Francis Gwer
Muriuki Muriungi
and Paul Makin

MFX
MOBILE | FINANCE | DIGITAL

fsd Kenya

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).

UKaid from the British people

Sida
SWEDISH INTERNATIONAL DEVELOPMENT COOPERATION AGENCY

BILL & MELINDA GATES foundation

Table of Contents

Table of Contents

List of tables

Abbreviations and Terminology

AI	Artificial Intelligence
AML	Anti-money Laundering
AWS	Amazon Web Services
CBK	The Central Bank of Kenya
CCPA	California Consumer Protection Act
CDD	Continuous Due Diligence
CEIP	Carnegie Endowment for International Peace
CFT	Combating of Financing of Terrorism
CISO	Chief Information Security Officer
CNIL	Commission Nationale Informatique & Libertés
COVID-19	Novel coronavirus discovered in late 2019 in Wuhan, China; later renamed SARS-CoV-2
DAPA	Data Protection Act, 2019
DDPA	Dutch Data Protection Authority
DPO	Data Protection Officer
€	Euro
EEA	European Economic Area
EU	European Union
FAQ	Frequently Asked Questions
FCA	Financial Conduct Authority
FINTECH	Financial Technology
GDPR	European General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
ICO	Information Commissioner's Office
IP	Internet Protocol
IVR	Interactive Voice Response
KES	Kenya Shilling

Abbreviations and Terminology

KYC	Know Your Customer
MSME	Mirco, Small and Medium Enterprises
NAS	Network-Attached Storage
NIST	National Institute of Standards and Technology
OCR	Optical Character Recognition
PCiR DSS	Payment Card Industry Data Security Standard
PAIA	Promotion of Access to Information Act of 2000
PDPC	Singapore's Personal Data Protection Commission
PII	Personal Identifiable Information
POCAMLA	Proceeds of Crime and Anti-Money Laundering Act 2009
POPIA	Protection of Personal Information Act
QNAP	Quality Network Appliance Provider
RBAC	Role-Based Access Control
ROPA	Record of Processing Activities
SaaS	Software as a Service
SPII	Sensitive Personal Identifiable Information
USSD	Unstructured Supplementary Service Data
UCLOUVAIN	Université Catholique de Louvain
VAPT	Vulnerability Assessment and Penetration Testing
VPN	Virtual Private Natework

Chapter 1

Executive Summary

This document has been developed to provide a review of the regulatory framework for data protection in Kenya. The report takes a broad view of what constitutes the regulatory framework, going beyond the Data Protection Act, 2019 (DAPA) to include the European General Data Protection Regulation (GDPR) and the California Consumer Protection Act (CCPA). The inclusion of GDPR and CCPA in the analysis stems from their coverage and applicability. GDPR applies to the processing of personal data of individuals who are residents of the European Economic Area (EEA) regardless of their location. Likewise, the CCPA applies to California's residents (natural persons) even if they are temporarily outside of the state. Consequently, GDPR and CCPA will apply to firms based in Kenya that process the personal data of EEA and California residents respectively.

As such, the objective of this review is to provide guidance to firms on the impact of DAPA and the extent to which both GDPR and CCPA apply to their businesses and operations. The document provides a detailed regulatory assessment of DAPA against the various articles and recitals in both the GDPR and the CCPA. This comparison identifies some of the challenges that fintechs and other firms might face during implementation. However, it is not just about identifying the potential challenges. The document goes further to provide policy recommendations to strengthen the regulatory framework and enhance market function. In the analysis of DAPA and its comparison with the GDPR and the CCPA, there are a few issues that either remain open to interpretation or are in need of further clarification. Such areas are highlighted in the document and additional insights on how other jurisdictions have addressed them are provided.

Whilst this document was being developed, the Office of the Data Protection Commissioner issued various regulatory instruments including guidance notes such as the Guidance Note on Access to Personal Data during Covid-19 Pandemic[1], Guidance Note on Consent[2], Guidance Note on Data Protection Impact

1 *https://ict.go.ke/wp-content/uploads/2021/01/Draft-Data-Request-Review-Framework-Jan-2021.pdf*

2 *https://www.odpc.go.ke/download/odpc-consent/?wpdmdl=7626*

Assessment[3], a Complaints management Manual[4] and draft regulations including the Data Protection General Regulations. There have also been court cases – including the retroactive application to the government's rollout of the National Integrated Identity Management System (NIIMS)[5] popularly known as *Huduma Namba* which had begun in November 2020 which the Attorney General has vowed to appeal.This document has been updated to reflect the policy provisions in the regulatory releases including those that are still in draft form, as well as the implications of the court case (if the appeal is not successful). It is expected that some of the draft policy provisions might change and as such, this document might undergo further revisions to reflect the new positions. All the same, the regulatory framework is still evolving and the policy recommendations herein can provide further guidance on enhancing and strengthening the regulatory framework to be able to deliver better outcomes in the long run.

The first major area that still needs clarification is the process for a Data Subject Access Request. Although a Data Subject might challenge and seek correction or deletion of data under DAPA, there is no clarity on the process or timelines to request access to the data in the first instance. Under the GDPR, there is a clear process for managing a request without creating a data breach when sharing this data and set deadlines for basic and complex requests. There are also protections for data controllers or processors to apply fees for excessive or repetitive requests, to cover their cost of processing the requests. When analysing the provisions on the registration of Data Controllers or Processors, the process and timeline for registration has not yet been confirmed, and it is unclear if companies domiciled outside Kenya need to register when processing data of Kenyan citizens. In the United Kingdom (UK), there is a small charge for registration to cover administrative costs, and it is uncertain if such an approach will also be adopted in Kenya.

With the absence of timelines for registration, there also remains uncertainty on the timelines for enforcement, even though the Act is now in force with cases now being brought to the court. In the *judgement against the National Integrated Identity Management System (NIIMS)*[6] popularly known as *Huduma Namba* which had begun in November 2020, and the failure to conduct a Data Protection Impact Assessment has led to the rollout of being found illegal. The expectation is that enforcement will be pursued in cases where a breach is detected and post-registration for those organisations which are considered to have insufficient controls or consent for managing existing data. However, further guidance from the Data Protection Commissioner can ensure that data controllers and data processors are aware of the implications of placing the data that they hold at risk. This can also help the data processors and data controllers to make informed decisions on the controls and solutions required and hence forestalling the implementation of solutions in areas where full clarity on the expected process is yet to be provided.

The enforcement also needs to be evaluated against the fines that will be levied on organisations that are found to have committed an offence. Although the fines in DAPA

3 *https://www.odpc.go.ke/download/odpc-protection/?wpdmdl=7628*
4 *https://www.odpc.go.ke/download/odpc-complaints/?wpdmdl=7624*
5 *http://kenyalaw.org/caselaw/cases/view/220495/*
6 *http://kenyalaw.org/caselaw/cases/view/220495/*

are large in relative terms to other frameworks in Kenya, the actual use of the terms "lower of 1% of turnover or 5 million KES" compared to 'the higher of €10 Million (1,330 million KES) or 2% of global turnover' under GDPR mean that offenders may risk the fine if repeat payments are lower than the cost of implementation. It is worth highlighting that Singapore's Personal Data Protection Commission (PDPC) is reviewing increasing the fine applicable from a maximum of US$1 million (approximately 108 million KES) to the higher of 10% of a company's revenue or US$10 million (approximately 1,080 million KES). The key understanding needed from the Data Protection Commissioner is whether the fine will be applied per data subject, or per incident of breach. If applied per data subject, the penalties from DAPA will be significantly greater.

In the Act when we assessed the process for gaining consent, it was not clear if consent must be specifically obtained, or if it can be captured as part of general terms and conditions – leaving the data capture open to potential abuse. In their guidance for consent, the Office of the Data Protection Commissioner clarified that consent must be "separate from other terms and conditions", and does not include data that is not necessary for the performance of that contract.

We also reviewed the implications of unstructured data – data that is not ordinarily in a database but instead in file storage and email services, and therefore likely to be in services not necessarily hosted in Kenya. The clarity on the need to host in Kenya is addressed later in this document. However, if it is a firm requirement for all parties to host in Kenya, the impact on organisations could be much higher than anticipated. A separate companion document[7] published alongside this one provides guidance on some approaches and tools to handle unstructured data.

Throughout this document, we identify some of the learnings that both the GDPR and the CCPA have presented in an aim to accelerate a higher standard of data protection for data subjects in Kenya e.g., examples of possible weaknesses from solely anonymising data. We believe that this analysis will provide sufficient guidance for data controllers and processors, and with the companion document allow them to implement appropriate controls and governance that ensures the data they manage is well protected and appropriate to their actual needs. We have also included an assessment of the UK, Dutch, South African and Singaporean Data Commissioners websites – to garner an understanding of how other countries are ensuring the clarity of their respective legislation.

7 Financial Sector Deepening Kenya (FSD Kenya). 2021. Data privacy and protection: Guidance Note to Kenya's Digital Financial Services

Credit/ Pexels -Sora-Shimazaki

> Data can be collected indirectly if it is publicly available and was made public in either public records, or the subject deliberately made it public. This approach should protect a consumer where their data is leaked, but potentially still allows data controllers or processors to capture information from dark web searches.

Chapter 2

Understanding the Data Protection Act

The intention of this section is to provide to the reader a comparison of the Kenyan Data Protection Act, (DAPA) with the General Data Protection Regulation (GDPR) and the California Consumer Protection Act (CCPA). We explore the similarities and differences between all three – using the foundational principles of the GDPR (most similarity for DAPA) as a reference point. It is worth noting that supporting regulations of DAPA are yet to be promulgated, although sets of regulations have recently been issued for public participation. Whereas there are still areas where regulation is expected to clarify gaps in DAPA, the GDPR has enshrined in law many of the points that will be addressed by Kenyan regulations, making the comparison complex.

The foundational principles are:

- Lawfulness / Fairness / Transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality / Security
- Accountability

This document is neither intended to provide legal advice nor should it be relied upon as a source of legal advice. The information is meant to be general and informative in nature, and the materials and references provided in the document may not be applicable in all (or any) situations and should not be acted upon without specific legal advice based on one's circumstances. The analysis is based on the version of the CCPA and UK Data Protection Act available in December 2020. It is worth highlighting that all global companies have already implemented the necessary changes to comply with both the GDPR and the CCPA. Given the prominence of technology companies and venture capital companies based in California, awareness of the need for tech companies to address the protection of consumers' data has never been more critical.

The GDPR which came into effect on came into effect on 25th May 2018 provides the most comprehensive data protection laws in the world to date. Given how long it was in discussion and the time it has now been active legislation, there is a large volume of work that can be used to support any government looking to implement a data protection strategy for her citizens. The groundwork for the GDPR dates back to 1995, with implementation work starting in 2011. A more detailed timeline of GDPR is available via '*The History of the General Data Protection Regulation*'[8].

The CCPA came into effect on 1st January 2020 as a first of its kind for the USA, and currently there are no other plans for a federal privacy law in the U.S. Given the State of California alone is equivalent to the fifth largest global economy, its effectiveness will be a key point of impact and interest for the remainder of the world. The full timeline of the CCPA is also available in the '*CCPA Regulations from the Office of the Attorney General in the State of California*'[9]. The CCPA introduces rights to access and delete personal information, and the introduction of additional protection for minors (under the age of 16).

Although it is the key legislation aimed at protecting the rights of individuals, there are several key differences

8 *https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en*

9 *https://oag.ca.gov/privacy/ccpa/regs*

between DAPA and the GDPR. These differences are explored in further detail in this section of the document. A more detailed legislative comparison is also provided. The first major distinction for the CCPA is that both DAPA and the GDPR are built upon a fundamental principle that personal data is collected with a clear legal basis (the capture is against a known use) – which is not the case for CCPA.

The next area is how the company is expected to safeguard data. DAPA and the GDPR have a much wider scope, providing clearer guidance on the limitations of collection, as well as the rules for accountability within an organisation. DAPA and the GDPR also ensure the appointment of Data Protection Officers (DPOs), maintenance of a register of the information processed and Data Protection Impact Assessments. The CCPA is not as explicit, but it does require companies to train their staff that deal with data requests.

The CCPA has also excluded certain categories – that are covered by other legal frameworks, such as medical data and credit reporting agencies. It restricts the selling of data, allowing consumers to opt-out and manage data acquired during a merger or acquisition.

The full text of the GDPR can be found on the *'EU Legal Publications Site'*[10] while the full text of the CCPA can be found in the *'California Legislative Information'*[11]. The CCPA also provides a mechanism for additions or changes to some provisions by the California Attorney General. The latest updates can be found on *'CCPA Regulations from the Office of the Attorney General in the State of California'*[12].

2.1 Lawfulness / Fairness / Transparency

2.1.1 Who is protected by the legislation?

DAPA defines a "data subject" as an identified or identifiable natural person who is the subject of personal data. It also clarifies that all companies based in Kenya, and all companies processing data in Kenya are subject to the legislation. There are, however, a few issues that will need to be clarified to ensure that Kenyan residents are not excluded, and that Kenyan companies are not disadvantaged on the global stage. Given the input of the proposed *"Data Protection (General) Regulations 2021"*[13], the impact on non-Kenyan companies is substantially reduced. Under the original Act (DAPA), any organisation offering a global service, but still providing adequate protection might have decided to deliver to Kenya later as the costs for following the Act could have reduced the priority of delivery of services in Kenya.

Data can be collected indirectly if it is publicly available and was made public in either public records, or the subject deliberately made it public. This approach should protect a consumer where their data is leaked, but potentially still allows data controllers or processors to capture information from dark web searches. Any organisation adopting such approaches will need to ensure that the data captured can be remedied by the user, and that their processes clearly identify this capture mechanism and the approval of any data subject. In a fintech context, the research of subjects to adhere to Know Your Customer (KYC) and Continuous Due Diligence (CDD) processes can lead to such a situation – a few services are now being introduced that use information found in the dark web to identify and combat financial crime and fight terrorism.

We discuss the specific requirements for consent in Section 2.1.5.1 Right to be informed.

The GDPR defines "data subjects," as those who are living natural persons and does not specify residency or citizenship requirements. Residency validation will be triggered for entities without an EU establishment – meaning any service operating outside the EU that captures the data of EU citizens will need to adhere to the legislation (including employees), but if no EU citizen data is processed, then the regulation does not apply. The fundamental question for any organisation is – "What if an EU citizen uses the service offered?"

The CCPA primarily protects consumers who are residents of California. Although there is no specific reference to how the legislation affects companies outside California, it is clear that "volume of business" with Californian residents is a key metric. This changes the question for any organisation to – "How many Californian residents are using my service?"

10 *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679*
11 *https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=*
12 *https://oag.ca.gov/privacy/ccpa/regs*
13 *https://www.odpc.go.ke/wp-content/uploads/2021/04/Data-Protection-General-regulations.pdf*

POLICY RECOMMENDATION 1

As a data processor or controller bears the burden of proof for any consent – the Data Protection Commissioner should ensure that there are clear examples of what is and is not acceptable to show consent has been provided. This simple act will ensure that any user experience factors the complexity of low literacy levels among data subjects as well as reduce the possibility for abuse.

POLICY RECOMMENDATION 2

Further guidance is needed from the Data Protection Commissioner for organisations collecting publicly available data and their need to ensure that the data captured can be remedied by the user. The collector's processes need to clearly identify this capture mechanism and the approval of any data subject to do so. In a fintech context, services are now being introduced that use information found in the dark web to identify and combat financial crime and fight terrorism for adherence to KYC and (CDD). The notification process is not expected to present a challenge, but notification that the information has been captured and allowing a party to rectify it may lead to a violation of Financial Crime legislation – especially in the case of an ongoing investigation into Terrorism Financing.

DAPA

2, 18 (1) 21(3), 28 (1, 2), 32 (1, 4)

"Data subject" is defined as an **identified** or **identifiable natural person** who is the subject of personal data, and "personal data" means **any information** relating to an identified or identifiable natural person;

"Identifiable natural person" is defined as a person who can be identified directly or indirectly, by reference to an **identifier** such as a name, an **identification number**, **location data**, an online identifier or to one or more factors specific to the **physical**, **physiological**, **genetic**, **mental**, **economic**, **cultural** or **social** or **social identity**;

"Sensitive personal data" means data revealing the natural person's **race**, **health status**, **ethnic social origin**, **conscience**, **belief**, **genetic data**, **biometric data**, **property details**, **marital status**, **family details** including names of the person's children, parents, spouse or spouses, **sex** or the **sexual orientation** of the data subject;

A company cannot act as a **Data controller** or **data processor** unless **registered** with the Data Commissioner. The **register** will be a **public document** available for inspection by any person.

The data subject's data can be collected **indirectly** when it is already a **public record**, or the data subject has **deliberately** made the data public. A data subject **should consent** to collection from another source, but they should **not** be **prejudiced** by its **collection**. The collection from third parties is allowed to **prevent**, **detect**, **investigate**, **prosecute** or **punish** for **a crime**; or to **enforce** a **law** imposing a pecuniary penalty; or to **protect** the interests of the **data subject** or **another person**.

A data controller or data processor shall bear the **burden of proof** for establishing a data subject's **consent** to the processing of their personal data for a specified purpose.

In determining whether **consent was** freely **given**, account shall be taken of whether, among others, the performance of a contract, including the provision of a service, is **conditional on** consent to the **processing of** personal **data** that is not **necessary** for the performance of that contract.

GDPR	CCPA
Article 1(1, 2), 6(1)	125 (b), 140 (g)
"Data subjects," who are living natural persons and does not specify residency or citizenship requirements. Residency validation will be triggered for entities without an EU establishment. Employee data is also fully protected. Data controllers can only process personal data when there are legal grounds for it. The legal grounds are: consent, or when processing is necessary: ▪ for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; ▪ for compliance with a legal obligation to which the controller is subject; ▪ in order to protect the vital interests of the data subject or of another natural person; ▪ or the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; ▪ for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Further permissible uses are provided for the processing of special categories of personal data under Article 9(2). As a general rule, the processing of special categories of personal data is restricted unless an exemption applies.	"Consumers" who are natural persons and who must be California residents. Does not cover legal persons. There is no list of grounds that clarify how businesses can collect and sell personal information. It does confirm that consent must be obtained from the consumer when they enter into a service that provides financial incentive because of the personal information that is given.

POLICY RECOMMENDATION 3

"A data controller must be registered" – but registration will not be mandatory for all organisations as defined in the act provides a contradiction as the processing of an invoice or a card transaction with personal details, will mean all entities will be expected to register. They will be caught by the means and purposes as defined in the registration regulation. Further guidance from the Commissioner's Office on scenarios where registration is not mandatory will assist organisations who were expected to be registered. In the UK, registration at the ICO is chargeable for all organisations that process personal data – however, the self-assessment process allows parties to identify if they do, indeed, need to register.

POLICY RECOMMENDATION 4

"A data controller must be registered" – but registration will not be mandatory for all organisations as defined in the act provides a contradiction as the processing of an invoice or a card transaction with personal details, will mean all entities will be expected to register. They will be caught by the means and purposes as defined in the registration regulation. Further guidance from the Commissioner's Office on scenarios where registration is not mandatory will assist organisations who were expected to be registered. In the UK, registration at the ICO is chargeable for all organisations that process personal data – however, the self-assessment process allows parties to identify if they do, indeed, need to register.

POLICY RECOMMENDATION 5

All efforts should be made to automate the registration process to reduce the burden on the Office of the Data Protection Commissioner.

The guidance on **Registration self-assessment**[14] on the UK Information Commissioner's Office (ICO) website allows a data processor or controller to identify if they need to register by asking a series of questions. Such a service takes the burden away from the Data Protection Commissioner's office.

The **Data protection public register**[15] is also available from the UK ICO and allows a data subject to confirm if a company is registered.

POLICY RECOMMENDATION 6

This registration guidance can also be used to clarify the scope for non-Kenyan entities processing sufficient volumes of Kenyan Data Subjects' data or deriving sufficient value from it.

- When and how should these foreign entities register with the Data Protection Commissioner?
- How do they address the specific need to host in Kenya, if applicable, without ?

2.1.2 Who must adhere to the legislation?

DAPA has defined that entities (data controllers or processors) that are established in Kenya, or those processing data of data subjects located in Kenya, must adhere to the legislation and by virtue of the regulations on registration "that person determines the purpose and means for processing personal data" all entities processing personal data are expected to register. This means that organisations in Kenya need to adhere to the legislation and that people in Kenya are protected but currently, guidance for entities outside of Kenya would benefit from further clarification.

It is worth noting that the definitions for businesses apply to these entities – irrespective of jurisdiction. The residency of the protected party is the measure defined above. The CCPA is also subject to interpretation on this point, as it applies to those entities "doing business in California" – which is defined as making profit or pecuniary gain under the California Franchise Tax board.

14 *https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/*

15 *https://ico.org.uk/ESDWebPages/search/*

DAPA
4(b) 18 (2)
A data controller or data processor is defined as **established** or ordinarily resident in **Kenya** and processes personal data while in Kenya; or not established or ordinarily resident in Kenya but **processing personal data** of data subjects located in Kenya. There are no thresholds to determine who is covered in either size or volume – including foreign companies. The Data Commissioner shall prescribe thresholds required for mandatory registration of data controllers and data processors, and in making such determination, the Data Commissioner shall consider; the **nature** of industry; the **volumes** of data processed; and whether **sensitive personal data** is being processed. "Data controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the **purpose and means** of processing of personal data;

GDPR	CCPA
Article 4(7, 8), 28(3), 30	**105 (d) , 140 (c, d, v)**
Primarily applied to data controllers. A data controller is a natural or legal person, public authority, agency or other body that determines the purposes and means of the processing of personal data, alone or jointly with others. This definition includes not-for-profit organisations. The business must define the "means and purposes of the processing".	A business or for-profit entities ("businesses") are covered under the CCPA. With thresholds to determine the businesses covered. (revenue over US$25 million, managing the data of more than 50,000 consumers, households or devices, derives more than 50% of revenue from selling the information). The business must determine the "purpose and means of the processing".
A data processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Their activities must be governed by a binding contract or other legal act with regard to the controller. The contract should set out the subject matter, duration, nature and purpose of the processing, the types of personal data processed, the security measures, and the obligations and rights of the controller. Processors can only process personal data on instructions from the controller. Upon termination of the agreement with the controller, processors must return or destroy personal data at the choice of the controller. In addition, if the processor wants to engage another processor (sub-processor) it has to have the written authorisation of the data controller.	A service provider is a legal entity organised for profit that processes personal information on behalf of a CCPA-covered business. The consumer's personal information is disclosed for a business purpose, pursuant to a written contract that prohibits the legal entity from retaining, using, or disclosing the personal information for any purpose (including a commercial purpose) other than performing the services specified in the contract. Businesses must also: Provide proper notice to consumers about personal information sharing practices; Obligate the service provider from further collecting, selling or using the personal information except as necessary to perform the business purpose.
There are no thresholds to determine who is covered in either size or volume – including foreign companies. Processors (service providers acting on behalf of controllers) also must maintain a record of processing according to article 30.	Service providers are not covered, but they must follow the instruction of the data controller.
Law enforcement and national security areas are excluded (although it may apply to businesses providing services to these agencies).	Law enforcement and national security areas are excluded (although it may apply to businesses providing services to these agencies).

2.1.3 What data capture tasks are covered?

All legislation, including DAPA, consistently apply to both automated and non-automated capture of data. However, many organisations fail to understand that in addition to the stated "basic filing system" this means that the coverage of the legislation includes their unstructured data. For example, any photos, emails, or scanned documents are covered, and therefore should there be need for correction or deletion, this data must also be addressed. This effectively extends the scope of activities a data controller or processor needs to manage beyond the traditional database management system to include all forms of storage, including File Systems and email.

The inclusion of unstructured data, sent in an email, and hosted on an email service run outside of Kenya could also put an organisation at risk of breaching the legislation. This is especially so if the mail service were to include workflow functionality (further extending the "processing").

As part of the registration process, a data controller or processor needs to provide: a Description of the data, Purpose, Category of Subjects, Risks, Safeguards and Security measures and Mechanisms to protect the data. This will ensure companies work through their data process and are clear on the tasks they are performing and the processes of protecting them.

The CCPA goes further on the protection of data by defining collecting and selling as well as processing and ensures that any merger or acquisition forces the acquirer to ensure that they are still using the data for the same purposes, and if not, give the data subject the option to opt out.

DAPA does clarify in section 72 that the sharing of data that is incompatible with the purpose for which it was collected (shared without clear consent and to the original purpose) is an offence. Similarly, if that data is subsequently sold – both parties (seller and buyer) are committing an offence. As part of the guidance note of consent, the Commissioner's Office clarified that the recipient of possible transfers should be part of the consent process, any transfer outside of this scope is at risk of being deemed an offence. Consent must also be a separate and clear act, simply notifying a customer in lengthy contract terms that the data might be sold to a third party is not acceptable. A customer is therefore unlikely to find themselves at the end of sales calls or unsolicited text messages that they never expected. Under sections 16 and 17 of the recently released *"Data Protection (General) Regulations 2021"*[16], the subsequent opting out mechanism will also reduce the persistent interruption of these calls as customers will be able to opt out.

POLICY RECOMMENDATION 7

As the Data Protection Commissioner considers the enforcement and improvement of definitions, the area of unstructured data, and the hosting of this data outside of Kenya should be explored and direction provided as part of the available guidance.

POLICY RECOMMENDATION 8

The provision of guidance such as **"Does an organisation need my consent?"**[17] from the UK ICO website to highlight how the consent would be validated for a consumer would be useful. Or guidance such as "Keep your consent requests separate from other terms and conditions" as provided in their **Consent**[18] guidance to organisations or the example in section 12.12 of Singapore's PDPC document **"Advisory Guidelines on Key Concepts in the Personal Data Protection Act"**[19]**.** Using a consistent approach for data subjects and those collecting and managing the data will ensure that the protection of individuals is clear and maintained. By making the consent of sharing more explicit, it will hopefully address some of the existing abuses in Kenya.

16 *https://www.odpc.go.ke/wp-content/uploads/2021/04/Data-Protection-General-regulations.pdf*
17 *https://ico.org.uk/your-data-matters/does-an-organisation-need-my-consent/*
18 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/*
19 *https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en*

DAPA
4 (a) 19 (2) 28 (3), 51 (2), 72 (1, 5, 6)
Covers **automated** and **non-automated** delivery (including a basic filing system). An application to register as a data controller or processor shall provide the following particulars: a **description of** the **personal data** to be processed; **a description** of the **purpose** for which the personal data is to be processed; the **category of data subjects**, to which the personal data relates; a general description of the **risks**, **safeguards**, **security measures** and **mechanisms to** ensure the protection of personal data; any measures to indemnify the data subject from unlawful use of data by the data processor or data controller; data controller or data processor shall collect, store or use personal data for a purpose which is lawful, specific and explicitly defined. There are exemptions if: it relates to processing of personal data by an individual in the course of a purely personal or household activity; if it is necessary for national security or public interest; or disclosure is required by or under any written law or by an order of the court. A data controller who **discloses** personal data **incompatible** with the **purpose for which the data has been collected** commits an offence. A **person** who offers to **sell personal data** where such personal data has been **obtained in this way** commits an offence. **An advertisement** indicating that personal data is or may be for sale constitutes an offer to sell the personal data.

GDPR	CCPA
Article 4(2), 23(1)	**110 (a), 140 (e, q, t)**
Covers **automated** and **non-automated** delivery (including a basic filing system). The definition of "processing" covers "any operation" performed on personal data "such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."	"Processing" is "any operation or set of operations that are performed on personal data" by either automated or not automated means. **"Collecting",** "**Selling"** or **"Sharing"** of Personal information. There are different obligations for each of these: ▪ "Collecting" under the CCPA is **"buying, renting, gathering, obtaining, receiving**, or **accessing** any personal information pertaining to a consumer by any means." ▪ "Selling" includes **"renting, disclosing, releasing, disseminating, making available, transferring,** or otherwise communicating personal information for **monetary or other valuable consideration."** ▪ Data sold in a merger, acquisition of bankruptcy is exempted, unless the thirds party alters the approved purpose - upon **acquisition** or **merger**, the acquiring company must review how the company uses the data when **compared** to the **contractual commitment**. Re-opening the option to "opt out".

2.1.4 What data is excluded?

All legislation ensures that an individual capturing data in the course of a purely personal or household activity – for example entering contact details into an address book – is not inadvertently brought within the scope of the Data Protection Act 2019 (DAPA). Public research may be conducted and the output exempt if the capture and processing adhere to the Act and the output does not lead to identification of data subjects. The use of anonymisation is promoted, but care should be taken even with anonymisation. DAPA has provided the Data Protection Commissioner the discretion to exempt certain provisions for other clear instances beyond Journalism, Literature and Art and Research, History and Statistics in the future. Guidance on these exemptions is expected to come from the Data Protection Commissioner.

There are also clauses to ensure that data captured for national security or public interest purposes are also exempted. In the fintech space, all deposit taking entities or payment entities must ensure that they work to combat the financing of terrorism (CFT) or the assessment of politically exposed persons (PEPs). So for fintechs which have the responsibility for capturing data to perform their Know Your Customer (KYC) and Continuous Due Diligence (CDD) duties, they now enter a potential grey area – where consent is taken but alternative data capture is required to validate what the customer has shared – and informing the customer they intend to do this could be considered as "tipping off" and thus against the provisions of anti-money laundering law.

For a fintech that needs to report suspicious activity it is important to note that Section 17 (1) of the Proceeds of Crime and Anti-Money Laundering Act 2009 (POCAMLA) clearly states that: "The provisions of this Act shall override any obligation as to secrecy or other restriction on disclosure of information imposed by any other law or otherwise." This provision does not give the Fintech entity freedom to process any data it chooses, but does allow for processing of personal data to allow for identification of the proceeds of crime and anti-money laundering.

It is also worth highlighting sections 8 and 13 of POCAMLA – where the data processing is expected to lead to subsequent reporting, the disclosure of this reporting to the data subject is potentially an offence. Therefore, caution should be observed by a data controller or processor to ensure that they fully understand the implications of these regulations and balance the rights of a data subject and the identification of financial crime. For example, the evidence of a potential financial crime needs to be kept for seven years which means that information needs to be kept for seven years from the reporting.

Additionally, in their interactions fintech companies may need to discuss personal information with other financial institutions to validate that transactions are in fact legitimate. The introduction of the GDPR has brought focus on how these activities can be supported whilst adhering to Data Protection Regulation. The Royal United Services Institute (RUSI) has created a programme to research the role of Public-Private Financial Information Sharing Partnerships – "The *Future of Financial Intelligence Sharing*".[20]

POLICY RECOMMENDATION 9

As DAPA does not define the protection of a household, it is worth noting that a similar omission in the GDPR has led to the definition of households being reviewed. It is possible that a household could be identified through the output of public research, even though a given individual might not be identified. Guidance on how to protect households will aid those conducting research whilst protecting households. It is also worth noting that identification of an individual has been possible from what has been considered "anonymised" data. This has been addressed further in section 2.3.1.7 on **"Historical or scientific research".**

POLICY RECOMMENDATION 10

As the Data Protection Commissioner creates their code of practice, clarification on anonymous, aggregate and de-identified data (noted in the GDPR and the CCPA) would ensure that researchers and other data controllers take sufficient safeguards in the collection and creation of datasets. Guidance such as Singapore's PDPC's **"Guide to Basic Data Anonymisation Techniques"**[21] will also aid those actively engaged in anonymisation techniques**.**

20 *https://www.future-fis.com/*

21 *https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf?la=en*

POLICY RECOMMENDATION 11

Given the perceived conflict of data processing and using additional information to help identify potential terrorist activity or financial crime, guidance was given from the Data Protection Commissioners Office and the Financial Report Centre, such as this **joint statement**[22] from the UK's Financial Conduct Authority (FCA) and ICO where they jointly confirmed that the new requirements of the GDPR and requirements on Financial Services organisations were generally compatible – but ongoing discussions would be maintained. This has been very evident in the FCA's latest Digital Sandbox pilot where the ICO were active participants in the use of large volumes of synthetic data to support research on Fraud and Lending following Covid-19.

The ICO also provides **specific guidance**[23] for small financial providers. This covers Anti-Money Laundering, the need for consent, deletion of data and the appointment of a Data Protection Officer.

POLICY RECOMMENDATION 12

It is recommended that both the Financial Reporting Centre and the Data Protection Commissioner's Office consider how to actively promote sharing amongst fintechs, whilst protecting data subjects. With the use of Privacy Enhancing Technologies, we explore this in further detail in Section 2.3 on Balancing consumer protection with Managing Fraud / AML and CFT in [Implementation Guidance]

DAPA
51 (1, 2), 52 (3), 54

The processing of personal data is **exempt** if: it relates to processing of personal data by an **individual** in the course of a **purely personal** or **household activity**; if it is **necessary** for **national security** or **public interest**; or disclosure is **required** by or **under** any **written law** or by an **order of the court**.

Personal data which is processed **only for research purposes** is exempt if: data is **processed** in **compliance** with the **relevant conditions**; and **results** of the research or resulting **statistics** are **not** made available in a form which **identifies** the **data** subject or any of them. The Data Commissioner will prepare a code of practice containing practical guidance in relation to the processing of personal data for purposes of Research, History and Statistics.

The Data Commissioner **may prescribe other instances** where compliance with certain provisions of this Act may be exempted.

GDPR	CCPA
Article 11, 2(1), 30(5)	**Article 11, 2(1), 30(5)**
Anonymous data is information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. Several demonstrations have highlighted that too many data points can lead to the data identifying an individual, leading to the data no longer being anonymous.	▪ "Aggregate consumer information" and "de-identified data" ▪ **"Aggregate consumer information,"** is defined as information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. ▪ **"De-identified"** information, which is information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses de-identified information puts in place some technical and organisational measures to prevent re-identification.

22 *https://www.fca.org.uk/news/statements/fca-and-ico-publish-joint-update-gdpr*
23 *https://ico.org.uk/for-organisations/in-your-sector/finance/general-data-protection-regulation-gdpr-faqs-for-small-financial-service-providers/*

GDPR	CCPA
Article 11, 2(1), 30(5)	**Article 11, 2(1), 30(5)**
Individuals for purely personal or household activity – to avoid personal address books being brought in to scope.	▪ Individuals and businesses not using the data for "commercial" activity
	▪ **Publicly available information** – from Federal, State or local government records.
	▪ Medical information because it is covered specifically by the Confidentiality of Medical Information Act. ▪ Protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, established pursuant to the Health Insurance Portability and Accountability Act (HIPPA). ▪ It excludes information collected for clinical trials purposes subject to the Federal Policy for the Protection of Human Subjects, which would also include data related to health.
Law enforcement and national security areas are excluded (although it may apply to businesses providing services to these agencies)	▪ Law enforcement and national security areas are excluded (although it may apply to businesses providing services to these agencies)

2.1.5 What rights does the consumer have?

2.1.5.1 Right to be informed

There are several key definitions within DAPA that ensure a data subject is informed:

- Data must be processed in a transparent manner, with the subject informed of the use to which their personal data is to be put; collected for explicit and specified purposes;

- The data controller or processor – before collecting – inform the data subject of their rights; that personal data is being collected; for what purpose it is being collected; who the data is being transferred to and the safeguards taken to protect the data when transferred; the contact details of the controller or processor; who else might receive the data; a description of the technical and organisational security measures taken to protect the data; whether collection is required under any given law and if this is voluntary or mandatory; the implications if not all data is provided.

An implementer should familiarise themselves with the Office of the Data Protection Commissioner's *guidance note on Consent* [24], the Commissioner's Office clarified how consent is obtained, and how to ensure that a data subject is able to clearly exercise their rights. Failure to adhere to this guidance is likely to lead a data controller or processor into difficulty. The key points have been extracted and provided below, as how a customer is informed is intrinsically linked to how consent is captured. The data subject must be offered control and offered a genuine choice and declining the consent should be without detriment. It is important to note that consent can also be deemed invalid by the Data Protection Commissioners Office, rendering the processing activity unlawful, if the controls become illusory.

Citing section 25 of the act, it is essential that a data controller or processor is clear on the data they capture and how they intend to use it. Any data that is not necessary in relation to a specified purpose of processing and is fundamentally unfair will be deemed as unlawfully obtained as the consent will be deemed to NOT have been given.

24 *https://www.odpc.go.ke/download/odpc-consent/?wpdmdl=7626*

Consent must meet the following minimum criteria:

1. Any manifestation of express, unequivocal, free, specific.
2. Informed indication of the data subject's wishes; and
3. By a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject

"Free" implies real choice and control. If there is no real choice and control, and the data subject feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid. If a data subject is unable to refuse or withdraw their consent without detriment. A data subject should also be free of inappropriate pressure or influence.

In order to be "informed" a data subject must have a clear understanding of the processing activities, and the implications on their rights. Data controllers and processors should ensure they:

- Give a data subject sufficient information so they can understand the processing and the implications on their rights
- Clarify the nature of the data to be processed
- Their rights
- Consequences of not consenting.
- Provide this information clearly and simply – in plain language and a manner that is understood by the data subjects
- Provide a prominent and concise request for consent – separate from other terms and conditions

Failure in any of these points is likely to make the consent invalid.

The controller must identify itself **AND name any third party** who will be relying on the consent. They must provide the purposes for processing, with a separate consent for each granular purpose (unless they are clearly interdependent). They should provide the option to withdraw consent at any time, and details on how this right is exercised

All of these requirements are likely to affect any product registration process, as such a product manager is advised to look to optimise their data processes and minimise the number of requirements for capturing personal data, or look to only request approval for processing at different times in the customer journey, to reduce the points of friction in a customer's journey. The Office of the Data Protection Commissioner also clarifies the process to actually ensure how consent is captured. With either a statement or a clear affirmative act – through an active motion or declaration. With either a written or recorded oral statement that can include electronic means.

A data controller or processor should also be able show that there is a link between the consent and the processing.

As long as the data is processed (or stored), there must be a demonstrable evidence of the required consent. This includes evidencing how consent was captured and what information was provided at the time of obtaining consent. For Pensions or Insurance agencies, this can mean that the archival and storage process of data must also hold the original consent and the documentation provided to the customer at the time. When consent is withdrawn, all processing should stop immediately. Data can be retained, but only as long as required for compliance with a legal obligation or for a legal claim. If data is retained, it is important that any data controller or processor has adequate controls in their data usage to prevent stored data being inadvertently used. The guidance also confirms that consent should be clear and given before processing commences – in line with the act itself.

If the reason for processing changes or a new purpose is introduced, after consent is obtained, new and specific consent is required. As such, a controller or processor needs to continuously monitor and ensure that the consent received, is still in line with the original consent as the idea of evolving consent is not a valid concept – either new consent or a lawful basis for the new purpose is required. Once a lawful basis has been established, there is a requirement for consistent application of that basis and another cannot be introduced just because it is deemed convenient for the processing. The relevant lawful basis needs to have been decided in advance of the processing.

If the statutory requirement has a defined set of data, then consent should be sought for data beyond that point with the data subject being advised of the statutory requirement and its limitations with respect to the processing. This is important to note for any person relying upon POCAMLA 2009.DAPA also states that data that is processed and used to create an automated

decision requires further notification to the data subject, as they have a right not to be subject to a decision based solely on automated processing, including profiling. There are exceptions – such as needing to process the data in order to enter into a contract, but if the data subject is affected the data controller or processor must notify the data subject in writing that a decision has been taken based solely on automated processing and the data subject may request the processor to reconsider the decision or take a new decision that is not based solely on automated processing. Once the processor has been notified, they will need to comply with the request and then advise the data subject regarding what steps they took, and the outcome.

The requirement for fintechs automatically processing data to identify fraud or suspicious activity in their management of financial crime should be managed by ensuring that if an automated decision is taken, then a compliance officer should review the information – potentially negating the need to advise an individual that they have been subjected to automated processing – as identified in Section 2.1.4 What data is excluded? Organisations should understand the implications of these regulations and balance the rights of a data subject and the identification of Financial Crime.

POLICY RECOMMENDATION 13

When the Data Protection Commissioner extends their guidance, they can provide examples for different industries to highlight how the law should be interpreted. For financial services, they could use the example of a credit decision that is based on the processed data and declines a loan, as this will be seen to significantly affect a data subject but is also required to enter into a contract. Exploring the various elements in such a use case i.e. use of additional data, the right to correct etc., will provide data controllers, processors and data subjects with clarity on how to interpret the law. A possible scenario relevant to Kenya – a customer applies for a loan which uses social media data as part of the algorithm, the loan application is rejected – what should the data controller do, and what can a customer do? Or when the data subject defaults on the loan – the data subjects' social media contacts were captured as part of the processing. What, if anything, can the data controller do with this extra information – even if it were captured in a contract? Would contacting these parties be acceptable?

POLICY RECOMMENDATION 14

As mentioned earlier, the ICO and PDPC guidance separates terms and conditions from the consent process, to make it a very active decision. Extending this guidance on consent to cover and explaining the following elements would also help data controllers, processors and data subjects:

- the legitimate interest of the data controller or the third party;
- data retention period or criteria to determine that period;
- the right to withdraw consent at any time;
- the right to lodge a complaint with a supervisory authority;
- when data is necessary for the performance of a contract, the possible consequences of not doing so; and
- the existence of automated decision-making, including profiling, including the logic involved, and the consequences of such processing.

To assist in this guidance, examples provided in Singapore's PDPC document, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act"[25], provide a good reference point.

- Section 12.63 provides good examples for legitimate interest and profiling;
- Section 18.4 provide good examples of retention periods that might be longer than a customer expects but still valid;
- Sections 12.44, 12.45 12.47, 12.48 and 12.54 provide different examples on withdrawing consent – that may still have residual consent for the data subject;
- Section 12.44 also deals with the impact on a contract of withdrawing consent – in this example a customer ending with early termination fees.

25 *https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en*

POLICY RECOMMENDATION 15

Further guidance is requested for the notification of a data subject in writing if they have been subject to automated processing. "In writing" is generally reserved for physical correspondence and does not allow the use of electronic forms of communication. In Section 2.5 on **"Users right to be forgotten"**, we explore that communication other than "in writing" is considered acceptable – and situations where "in writing" is used as the communication method if the alternatives are not sufficient. The starting point being to use the same method that a user applied for the service.

DAPA

25 (b, c, d) 26 (a), 29 (35), 44, 47

Data must be processed **lawfully**, **fairly** and in a **transparent manner** in relation to any data subject; collected for **explicit**, **specified** and **legitimate** purposes and **not further processed** in a **manner incompatible** with those purposes;

Data collection should be **adequate**, **relevant**, **limited** to what is necessary in relation to the purposes for which it is processed; Collected only where a **valid explanation** is provided whenever information **relating to family** or **private affairs** is required; Data subject is to be **informed of the use** to which their personal data is to be put; A data controller or data processor shall, before collecting personal data, in so far as practicable, inform the data subject of: the **rights** of the data subject; the fact that personal data is **being collected**;) the **purpose** for which the personal data is being collected; the **third parties** whose personal data has been or will be transferred to, including **details of safeguards** adopted; the **contacts** of the data controller or data processor **and** on **whether any other entity** may receive the collected personal data; a description of the **technical** and **organisational security measures** taken to ensure the integrity and confidentiality of the data; the data being collected **pursuant to any law** and whether such collection is **voluntary** or **mandatory**; the **consequences** if any, where the data subject **fails to provide** all or any part of the **requested data**.

Every data subject has a **right not to be subject** to a decision **based solely on automated processing**, including profiling, which produces legal effects concerning or significantly affecting the data subject. This **shall not apply where** the decision is; **necessary for** entering into, or performing, **a contract** between the data subject and a data controller; **authorised by a law** to which the data controller is subject and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or **based** on the **data subject's** consent.

Where a data controller or data processor takes a **decision**, which produces legal effects or significantly affects the data subject **based solely on automated processing**; the data controller or data processor must, as soon as reasonably practicable, **notify the data subject in writing** that a decision has been taken based solely on automated processing; and the **data subject may**, after a reasonable period of receipt of the notification, request the data controller or data processor to: reconsider the decision; or take a new decision that is not based solely on automated processing.

A data controller or data processor, upon receipt of a request, shall within a reasonable period of time; **consider the request**, including any information provided by the data subject that is relevant to it; **comply with the request**; and by notice in writing **inform the data subject** of the **steps** taken to comply with the request and the outcome of complying with the request.

GDPR

Article 13 , 14

Information must be provided to data subjects by controllers at the time when **personal data are obtained, when the personal data is collected directly from data subjects.**

- the **identity** and the **contact details** of the controller;
- the **contact details** of the data protection officer;
- the **purposes** and **legal basis** of processing; and
- **categories** of personal data processed;
- any other **recipients** or **categories** of recipients of the data.

CCPA

100 (a, b), 110 (a, c), 115 (d), 130 (a), 135 (a)

The CCPA states that information on the following must be provided to individuals:

- the **categories** of personal information to be collected;
- the **purposes** for which collected personal information is used; and
- if a business sells personal information about the consumer to third parties, the rights of the consumers and the methods to exercise such rights must be given to consumers. This includes a link to the '**Do Not Sell My Personal Information**' page where consumers can exercise their right to opt-out.

GDPR	CCPA
Article 13 , 14	**100 (a, b), 110 (a, c), 115 (d), 130 (a), 135 (a)**
The GDPR also states that information on the following must be provided to individuals: ▪ the legitimate interest of the data controller or the third party; ▪ data retention period or criteria to determine that period; ▪ the right to withdraw consent at any time; ▪ the right to lodge a complaint with a supervisory authority. ▪ when data is necessary for the performance of a contract, the possible consequences of not doing so; and ▪ the existence of automated decision-making including profiling, including the logic involved and consequences of such processing. Data controllers cannot collect and process personal data for purposes other than the ones about which the consumers were informed, unless they provide them with further information and the right to object. The GDPR provides specific information that must be given to the data subject when their data is collected by a third party, which include the sources from which data was collected. Notice must be given within a reasonable period after obtaining the data, but at the latest within one month; or at the time of the first communication with the data subject; or at the latest when personal data are first disclosed to a recipient.	Customers must be informed **before or at the point of collection.** Businesses **cannot** collect additional personal information without advising the consumers the information that is to be collected and the purpose. The following must be provided to individuals: ▪ the categories of personal information collected / sold / disclosed for business purposes in the previous 12 months; and ▪ alternatively, if no personal information was sold, that should be written in the privacy policy. There is a specific requirement that consumers receive **"explicit notice"** when a third party intends to sell personal information about that consumer that has been sold to the third party by a business. The businesses **privacy policy must be updated every 12 months.**

2.1.5.2 Right to object

A Data Subject has a right to object to the processing of all or part of their data, including the right to withdraw consent at any time. Any withdrawal of consent does not affect the lawfulness based on prior consent before its withdrawal. Accordingly, if a data controller or processor have obtained lawful permission, they do not need to remove data from previously processed activity – but they do need to prevent its use in the future.

In financial services, personal data will have been captured for KYC purposes establishing a compelling legitimate interest. As long as the data is not used for other purposes, the data controller or processor will still be able to utilise this information.

The CCPA has also ensured that the selling of the personal information passes a further burden of responsibility to the party collecting to provide a "Do Not Sell My Personal Information" page available from their home page. There are minor exceptions to this – for example vehicle warranty information, which will be required if a vehicle needs to be recalled for safety purposes – but these exceptions do not allow the collector to share or sell the data for any other reason.

With DAPA coming into effect on 24th November 2019, organisations should have already requested consent for continued processing of historic data. **If there is no evidence of consent** having been given historically, they have not obtained consent and therefore **they are technically committing an offence**. The lack of "grandfather" rights under DAPA, as with the GDPR, meant that when the GDPR came into effect on 25th May 2018, data controllers and processors had to either delete or anonymise the data to make it untraceable to an individual. For the GDPR, it is worth noting that the law was announced and a two-year window period given for organisations to ensure that they are compliant with it before it was enforced. Given the current timing from the Data Protection Commissioner, it is expected a similar path will be followed.

POLICY RECOMMENDATION 16

When preparing its Guidance, the Data Protection Commissioner should consider the GDPR approach in ensuring that opting out is as easy as opting in – for example a simple check box to opt in means a simple check box to opt out. The following guidance[26] from the ICO provides a good guideline for data controllers and to data subjects on what may be expected.

POLICY RECOMMENDATION 17

As DAPA is already law, guidance from the Data Protection Commissioner on the enforcement time frames – expected to be broadly in line with the registration deadlines yet to be introduced – will give organisations sufficient time to confirm consent, or transform their historic data as already prescribed within the Act.

DAPA
26 (c), 32 (2, 3) 36, 37 (3)
A data subject has the **right to object** to the processing of **all** or **part** of their personal data. A data subject shall have the right to withdraw consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on prior consent before its withdrawal. A data subject has a right to object to the processing of their personal data, **unless** the data controller or data processor **demonstrates compelling legitimate interest** for the processing which overrides the data subject's interests, or for the establishment, exercise or defence of a legal claim. The Cabinet Secretary, in consultation with the Data Commissioner, **may prescribe practice guidelines** for commercial use of personal data in accordance with this Act.

GDPR	CCPA
Article 7(3), 13(2), 14 (2), 17, 21 (1, 2)	**115 (a, b) 135 (a), 145 (f, g)**
Data subjects have several ways to opt-out of processing of their personal data: ▪ they can **withdraw consent**; ▪ they can exercise the general right to object to processing that is based on legitimate interests or on a task carried out in the public interest; or ▪ they can object to processing of their data for direct marketing purposes. Information about this right and on how to exercise it must be included in the **privacy notice**. In particular, in the context of direct marketing, opting-out must be as easy as opting-in.	Consumers have the right to **opt-out from selling of their personal information**. They also have the right to opt-out from the subsequent selling of their personal information by a third party that received personal information after an initial "selling." The third party shall not sell the personal information unless the consumer has received **"explicit notice"** and is provided an opportunity to opt-out. If a business sells consumers' personal information, information about this right must be given to consumers in the notice. Moreover, a link to the page **'Do Not Sell My Personal Information'** must be included in the homepage of the business. The CCPA allows businesses to create a California-specific description of consumers' privacy rights. The CCPA provides consumers with a right to opt-out from the selling and/or disclosing for business purposes of their personal information. The opt-out can therefore only stop the selling of personal information, and it does not impact other uses of their information.

26 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-privacy-information-should-we-provide/*

GDPR	CCPA
Article 7(3), 13(2), 14 (2), 17, 21 (1, 2)	**115 (a, b) 135 (a), 145 (f, g)**
The GDPR provides data subjects with the **right to object** to the processing of their personal data when the processing is based on the legitimate interest of the controller or a third party. The data controller would have to cease processing personal data unless it demonstrates that there are compelling legitimate grounds to continue the processing. Moreover, the data subject has the right to object to processing for direct marketing as well as to withdraw consent at any time. The GDPR does not prescribe the specific language to be used.	However, the right to opt-out of the sale is absolute, in the sense that businesses cannot reject an opt-out request on the basis of their compelling legitimate grounds. Businesses must adhere to the language provided in the CCPA, namely the homepage of their website must have a link titled '**Do Not Sell My Personal Information**.' The right to opt out does not apply to vehicle information or vehicle ownership information retained or shared between a new motor vehicle dealer and the vehicle's manufacturer if the vehicle or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose.
Consumers have the right to opt-out from selling of their personal information. They also have the right to opt-out from the subsequent selling of their personal information by a third party that received personal information after an initial "selling." The third party shall not sell the	Customers must be informed **before or at the point of collection.** Businesses **cannot** collect additional personal information without advising the consumers the information that is to be collected and the purpose. The following must be provided to individuals: ▪ the categories of personal information collected / sold / disclosed for business purposes in the previous 12 months; ▪ alternatively, if no personal information was sold, that should be written in the privacy policy. There is a specific requirement that consumers receive **"explicit notice"** when a third party intends to sell personal information about that consumer that has been sold to the third party by a business. The businesses **privacy policy must be updated every 12 months.**

2.1.5.3 Right of access

A data subject has a right to access their personal data. However, DAPA does not define the process through which such a request can and should be processed. The only element that provides some insight is the data subjects' right to receive personal data in a structured, commonly used and machine-readable format – defined as part of data portability. Data portability conditions give the processor 30 days to provide the data. We have provided an approach based on best practice in our companion document [Implementation Guidance] Section 2.2.6 Process for responding to a Data Subject Access Request (DSAR).

In Section 8 of the recently released *"Data Protection (General) Regulations 2021"*[27], the Data Protection Commissioner has provided further insight and a form to manage a data access request. The form does clarify certain costs apply, (copying, USB or translation). However, it still does not address the mechanism for the request or time frame. Most worryingly – although the new Form 2, 4 and 5 (which allows for data to be ported, modified or erased) has a clear identification step, warning that misrepresentation may lead to prosecution, this does not exist in the access request. In section 22 of the *"Data Protection (General) Regulations 2021"*[28], the Data Protection Commissioner leaves the access process to be part of an organisation's data policy.

27 https://www.odpc.go.ke/wp-content/uploads/2021/04/Data-Protection-General-regulations.pdf
28 https://www.odpc.go.ke/wp-content/uploads/2021/04/Data-Protection-General-regulations.pdf

POLICY RECOMMENDATION 18

The process for an access request is defined to ensure a data subject can identify the data held about them, and then be able to request a deletion or correction. However, this is impossible if data subjects do not have visibility of the data held. Some of the key questions to answer are:

- How is a request made?
  - Orally- if by phone should this be toll-free phone number?
  - In writing?
  - On a webpage?
- Is the controller or processor responsible for validating that the request is from a valid individual (to prevent this process being abused by unscrupulous parties)?
  - This must be balanced with creating an unnecessary burden – that is greater than the process to add the data.
- Should the request be responded to free of charge (there will be a cost for the controller or processor to manage it)?
  - If the request is free – how are controllers and processors protected from excessive requests?
  - If the request is not free – is it proportionate to the service?
- Should the response be via the same medium as the request or are there discrete approaches mandated?
- In addition to the raw data, should further information be provided? For instance:
  - Categories of information collected;
  - Categories of Sources;
  - Commercial purpose for its collection;
  - Categories of third parties the information has been shared with;
  - The retention period of the data;
  - Complaint's procedure.
- What if data is part of a larger document
  - What if it identifies other parties? Should the other data be redacted or replaced?
  - What if timing is a critical portion of the right to correct? Should time be visible?
- How long should the response take? Data portability requests should be completed in 30 days.

Once a Data Subject access request process has been created, the guidance from Singapore's PDPC guide-to-handling-access-requests[29] or the UK's ICO for a business[30] and guidance for the data subject[31] are good reference materials for the types of information that will be useful to all parties.

DAPA	
26 (b), 38 (1)	
A data subject has the right to access their personal data in the custody of a data controller or data processor; A data subject has the right to receive personal data concerning them in a structured, commonly used and machine-readable format.	
GDPR	**CCPA**
Article 12 (1, 3, 5), 13 (1), 14 (1, 2), 15 (1, 3)	**100 (d), 110 (a), 130 (a), 145 (g), 185 (a)**
The GDPR states that, when responding to an access request, a data controller must indicate the purposes of the processing; the categories of personal data concerned; the recipients or categories of recipients to whom personal data have been disclosed to; and any sources from which data was collected. The GDPR specifies that individuals also have the right to receive a copy of the personal data processed about them. Data subjects must have a variety of means through which they can make their request, including through electronic means and orally. When the request is made through electronic means, the data controller should submit the response through the same means.	A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

29 *https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guide-to-handling-access-requests-v1-0-(090616).pdf?la=en*
30 *https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/frequently-asked-questions/right-of-accesssubject-access-requests-and-other-rights/*
31 *https://ico.org.uk/your-data-matters/your-right-to-get-copies-of-your-data/*

GDPR	CCPA
Article 12 (1, 3, 5), 13 (1), 14 (1, 2), 15 (1, 3)	**100 (d), 110 (a), 130 (a), 145 (g), 185 (a)**
The GDPR specifies that data controllers must have in place mechanisms to ensure that the request is made by the data subject whose personal data is requested access to. The GDPR states that data subjects can exercise this right free of charge. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character. The right applies to all the personal data collected and processed about the data subject making the request. Under the GDPR, the data controller must include further information in the response to a request of access, notably, the retention period, the right to lodge a complaint with the supervisory authority, the existence of automated decision making, and existence of data transfers. Data controllers can refuse to act on a request when it is manifestly unfounded, excessive or has a repetitive character. Data subjects' requests must be complied without "undue delay and in any event within one month from the receipt of the request." The deadline can be extended an additional two months taking into account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request. The GDPR has a distinct right to data portability, which applies under its own specific conditions (see below).	A customer can ask for: the categories of personal information collected/sold; the categories of sources from which the personal information is collected; the business or commercial purpose for collecting or selling personal information; and the categories of third parties with whom the business shares personal information. The CCPA specifies that individuals also have the right to be given access to the pieces of personal information collected about them. Consumers must be given at least two methods to make their request to access their personal information, notably via a toll-free phone or a webpage. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information. The CCPA specifies that businesses must have in place mechanisms to ensure that the request is made by the consumer whose personal information is requested access to. Disclosure and delivery of personal information as required by the right of access must be free of charge. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character. The right applies only to personal information collected in the 12 months prior to the request. The deadline to respond to such a right is 45 days of receipt of the consumer's request. It could be extended for an additional 45 days, but notice should be given to the consumer within the first 45 days. However, there seems to be an inconsistency in the current text of the law that allows an extension to 90 days, under a different provision. When data is provided electronically to the consumer this data should be sent in a portable and readily usable format that allows for the transmission of this data to third parties.

2.1.5.4 No discrimination due to exercising rights

DAPA, like the GDPR, does not include an explicit provision stating that a data subject must not be discriminated against on the basis of their choices on how to exercise their data protection rights. But it does state that data should be processed fairly; the subject has a right not to be subjected to solely automated decision making; and that consent is not freely given if consent requires the provision of consent for data that is not necessary for the performance of the contract. A service provider who requests the name and address from a user but only needs the name to process the request – is forcing the user to provide the address details, meaning consent for the address is not freely given.

In their *guidance note on consent*,[32] the Office of the Data Protection Commissioner confirms that the exercise of the right to withdraw consent or not even giving it in the first instance should not lead to any detriment. We provide a detailed review of the guidance in Section 2.1.5.1 Right to be informed. Any discrimination because

32 *https://www.odpc.go.ke/download/odpc-consent/?wpdmdl=7626*

of exercising this right, is likely to be one of the key measures on whether or not consent is deemed lawful – the guidance applies section 25 of DAPA and the fair and transparent manner to assess and measure "Free choice". If the Data Protection Commissioner's Office can evidence coercion or discrimination in the accepting of the processing then the consent will be deemed unlawful with the data controller or processor likely to find themselves at risk of a fine.

The CCPA goes further to define that the denial of goods or services, the charging of different prices, differing quality and suggesting this will be deemed to be discrimination. Schemes can be set up that provide financial incentive, but they must be explicitly opted into – allowing the consumer to make an informed choice that these incentives add sufficient value.

POLICY RECOMMENDATION 19

Expanding the scope to explicitly address any potential discrimination will ensure that consumers and providers understand what is expected of them.

DAPA
25, 32 (4), 35 (4)
Every data subject has a right not to be subject to a decision based solely on automated processing. (4) In determining whether consent was freely given, account shall be taken of whether, among others, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

GDPR	CCPA
Article 5, 13, 22	**125 (a)**
The GDPR does not include an explicit provision stating that a data subject must not be discriminated on the basis of their choices on how to exercise their data protection rights. However, it is implicit from the principles of the GDPR that individuals must be protected from discriminatory consequences derived from the processing of their personal data. For example, Article 5 states that personal data must be processed 'fairly'; Article 13 states that data subjects must be informed of the consequences derived from automated decision-making; and Article 22 specifies that individuals have the right not to be subject to solely automated decision making that has a legal or significant effect upon them. Additionally, the GDPR emphasises that when processing is based on consent, in order for consent to be valid, it must be freely given. Consent is not considered freely given if the data subject has no genuine or free choice or is unable to refuse or "withdraw consent without detriment."	The CCPA states that consumers must not be discriminated because of the exercise of their rights under the CCPA. The CCPA defines the scope of this right by stating that consumers must not be discriminated against because of the exercise of their rights under the CCPA, which means they must not be: ▪ denying goods or services; ▪ charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties; ▪ differing level or quality of goods or services; and ▪ suggesting they will receive a different price or rate for goods or services. It has to be noted that businesses can set up schemes for providing financial incentives, but consumers must opt-in to become part of them.

2.1.5.5 *Right to Data Portability*

DAPA provides the right for a consumer to have their data moved from one controller or processor to another. This movement should be as simple as possible. If the company states that it is unable to comply with such a request, the Data Protection Commissioner may determine if the company is technically capable of such movement. The data portability request should be complied with within 30 days, but where the portability request is complex, or there is a lot of data to process, the data controller can agree to a more realistic time frame in consultation with the Data Protection Commissioner.

The GDPR and CCPA, similar to Data Subject Access Requests, ensure that the mechanism for a request is clear, and that there is more than one option for making the transfer request. They also ensure that mechanisms are in place to prevent anyone other than the data subject from making these requests.

The GDPR states that only the information provided by the consumer needs to be transferred. In the financial services sector, organisations may seek input from external reference agencies as part of their duties - KYC and CDD, for example looking at sanctions lists or adverse media. Under DAPA, this collected data is also subject to data portability. This data is part of an organisation's proprietary decision-making process and may also have associated costs. Providing this information to a receiving third party should be considered carefully, and a fee might be levied, to cover the original cost of obtaining this data and the processing. This interpretation should also be reviewed to ensure that proprietary information created by the data controller, such as Credit scores, are not ported or freely handed to a competitor.

In Section 10 of the "*Data Protection (General) Regulations 2021*"[33], a data subject can request the porting of their data, and the data controller (when paid a reasonable fee) must port the data within 30 days. A standard form has been provided by the Data Protection Commissioner in the First Schedule of Form 2. The Data Protection Commissioner does provide the option for a data controller or data processor to decline this request, but the data subject should be notified within seven days of the request being received if this is the case. As we identified earlier, although not currently confirmed by the Data Protection Commissioner, a reasonable denial of data porting could be used for the restriction to only include the data supplied or created by the data subject.

POLICY RECOMMENDATION 20

Before any data is allowed to be ported, the Data Protection Commissioner should ensure that there is a "fair" validation process of the data subject and confirm they have approved the porting of data, to prevent unscrupulous providers porting customers' data they do not have the right to port.

A "fair" validation process was discussed in Section 1.1.4.3 of this document on 2.5 Users right to be forgotten.

POLICY RECOMMENDATION 21

As part of their guidance, the Data Protection Commissioner should also review the timeline for any given extension in the processing of the request, setting a maximum time expected to cover complex or numerous requests from a data subject. The current process risks the Data Protection Commissioner's office becoming buried under extension requests, some of which may in fact be delaying tactics. In the Sub Section "Can we extend the time for a response"[34] the UK ICO provides guidelines for this, and immediately provides examples on how to assess a complex request. The data subject is also aware of these timelines in the subsection "How long should an organisation take"[35] – both of these reducing the burden on the Data Protection Commissioner thereby allowing more focus to be on enforcement.

POLICY RECOMMENDATION 22

Another area to address is what data should be ported i.e. under the GDPR, businesses do not have to port more data than is necessary. The UK ICO provides the data subject with clear guidance in the section "What kind of data this right relates to"[36] that the data is that provided by the data subject (which in the example includes data from smart meters or wearables). Extending this guidance to fintechs to consider the background data that has been collected or created, and whether this should be included, will assist all parties in understanding their obligations.

33 *https://www.odpc.go.ke/wp-content/uploads/2021/04/Data-Protection-General-regulations.pdf*
34 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/what-should-we-consider-when-responding-to-a-request/*
35 *https://ico.org.uk/your-data-matters/your-right-to-data-portability/*
36 *https://ico.org.uk/your-data-matters/your-right-to-data-portability/*

DAPA
38
A data subject has the right to: **receive** personal data concerning them in a **structured, commonly used** and **machine-readable** format; to **transmit** the data obtained **to another** data controller or data processor **without** any **hindrance.** Where possible, the data transmitted directly from one data controller or processor to another; Where data **controller** or data processor **declines** to comply with a request the **Data Commissioner** may make a **determination** on the **technical capacity** of the data controller or data processor. This right shall not apply in circumstances where; processing may be necessary for the performance of a task carried out in the public interest or in the exercise of an official authority; or it may adversely affect the rights and freedoms of others. A data controller or data processor shall comply with data portability requests, at reasonable cost and within a period of 30 days. Where the portability request is complex or numerous, the period may be extended for a further period as may be determined in consultation with the Data Commissioner.

GDPR	CCPA
Article 13 (2), 14 (2), 20	**100 (d), 130 (a)**
Data subjects have the **right to receive their data processed on the basis of contract or consent in a "structured, commonly used, and machine-readable** format" and to transmit that data to another controller without hindrance. The GDPR states that consumers can exercise this right **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character. Data subjects must have a variety of means through which they can make their request, including through **electronic means and orally**. When the request is made through electronic means, the data controller should submit the response through the same means. The GDPR specifies that data controllers must have in place **mechanisms** to ensure that the request is made by the data subject whose personal data is requested access to. The GDPR provides that this must be done only when **technically feasible**. The right to data portability **only** applies to the **personal data** that has been **provided by the data subject** themselves and that is processed on the basis of **consent** or **contract** and the processing is carried out by **automated means**. Data controllers must respond without **undue delay** and in any event **within one month** of receipt of the request. It could be extended an **additional two months**, but notice should be given to the data subject within the first month. In addition to having data subjects receive personal data under the right to data portability, the GDPR **extends this right to having the personal data transmitted directly from one controller to another.**	When businesses provide data electronically to the consumer following an access request this data should be sent in **a portable and readily usable format that allows for the transmission of this data to another entity** without hindrance. Consumers can exercise this right **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character. Consumers must be given at least two methods to make their request to access their personal information, notably via a **toll-free phone or a webpage**. The business may send the response via mail or electronic means. The CCPA specifies that businesses must have in place **mechanisms** to ensure that the request is made by the consumer whose personal information is requested access to. The CCPA provides that this must be done only when **technically feasible**. The right to data portability is an **extension of the right** to access, and therefore it is subject to the same limitation (e.g. it only applies to data collected in the previous 12 months). Businesses must respond within **45 days** from receipt of the request. It could be extended an a**dditional 45 days**, but notice should be given to the consumer within the first 45 days. The CCPA's right is limited to allowing consumers receive their personal information, and it does **not** extend to having a business transfer the information to another business.

2.2 Purpose limitation

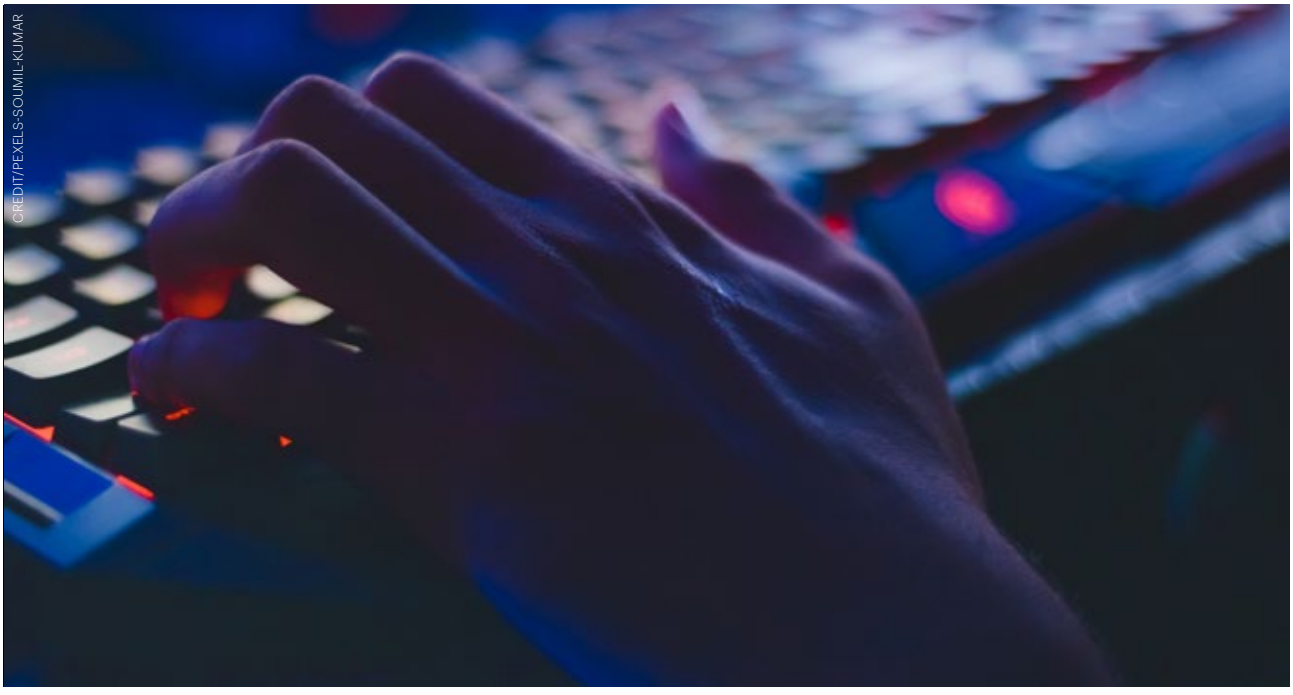
2.2.1 How to ensure that the data is only used for the expected purposes?

DAPA specifically ensures that the data is limited to what is necessary in relation to the purposes for which it is processed, kept in a form which identifies the data subjects for no longer than is necessary, as well as ensures that the data use is explicitly defined. It goes on to further ensure that the data is only processed for the purposes agreed or that the processing is necessary or required by key exceptions (both from a public interest and legal perspective) or for the purposes of historical, statistical, or scientific research.

Data should be accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay. If further processing is required, it should be under the same conditions as those agreed to by the data subject. Contravention of this will lead to the data controller or data processor committing an offence. Following the example set in the GDPR with the use of a Records of Processing Activities (ROPA), data controllers and processors can ensure that all the key information is captured in one place, and therefore a company will have clarity on the data being processed, and the controls around it.

POLICY RECOMMENDATION 23

As part of its guidance, the Data Protection Commissioner can provide a view of how something like a Records of Processing Activities provides a structured approach to the requirements of a Data Controller or Processor and can standardise the information provided to the Data Protection Commissioner's Office. The UK ICO has provided more information in their guide "Records of Processing and Lawful Basis"[37]. In the document "Advisory Guidelines on Key Concepts in the Personal Data Protection Act"[38], Singapore's PDPC provides examples of purposes – without providing all reasons in Section 8, exploring deemed consent in Sections 12.8 to 12.24 and how to ensure data remains accurate in Section 16.6.



CREDIT/PEXELS-SOUMIL-KUMAR

37 *https://ico.org.uk/for-organisations/accountability-framework/records-of-processing-and-lawful-basis/*

38 *https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en*

DAPA
25 (d, f, g) 28, 30
Data is adequate, relevant, **limited** to what is **necessary** in relation to the purposes for which it is processed; should be **accurate** and, where necessary, **kept up to date**, with every reasonable step being taken to **ensure** that any **inaccurate** personal **data** is **erased** or **rectified** without delay; kept in a form which identifies the data subjects for **no longer than is necessary** for the purposes which it was collected; data controller or data processor shall collect, store or use personal data for a purpose which is lawful, specific and **explicitly defined**. A data controller or data processor shall not process personal data, unless: ▪ The data subject **consents** to the processing for one or more **specified purposes**; or ▪ The processing is necessary: for the **performance of a contract** to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract; for **compliance** with any legal obligation to which the controller is subject; in order to **protect** the vital interests of the **data subject or another natural person**; for the performance of a **task** carried out **in** the **public interest** or in the **exercise** of **official authority** vested in the controller: the performance of **any task** carried out by a **public authority**; for the **exercise**, by any person in the **public interest**, of any other functions of a public nature; for the **legitimate interests** pursued by the data controller or data processor by a third party to whom the data is disclosed, **except** if the processing is **unwarranted** in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or for the purpose of **historical**, **statistical**, journalistic, literature and art or **scientific research**. ▪ **Further processing** of personal data shall be in **accordance** with the **purpose of collection**. ▪ A data controller who **contravenes** the provisions **commits an offence**.

GDPR	CCPA
Article 13 (2), 14 (2)	**115 (a, b, c)**
The GDPR provides data subjects with a right to withdraw consent at any time as well as a right to object if their personal data is processed on the basis of legitimate interest or performing of a task in the public interest.	The CCPA does not have a list of "positive" legal grounds required for collecting, selling or disclosing personal information. However, consumers may ask businesses not to sell their personal data. In case a consumer opts-out, the business will only be able to sell and/or disclose personal information if the consumer gives their explicit permission. For a business to not be considered as "selling" personal information when it shares it with a service provider for a business purpose, the service provider must not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

2.3 What are the key data definitions?

2.3.1 Personal Information

DAPA defines a person as identifiable if they can be directly or indirectly identified by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. It also provides further clarity on sensitive personal data. Sensitive personal data would reveal a natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject.

Further insight is also provided in the definition of "profiling" meaning any form of automated processing of personal data to evaluate certain personal aspects relating to a natural person, in particular race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth, personal preferences, interests, behaviour, location or movements. Fintechs will be dealing with both personal, and sensitive personal data as well as profiling – therefore the expectation is that they will bear a high duty of responsibility.

POLICY RECOMMENDATION 24

As mentioned previously in section 2.1.4 "What data is excluded?" Households are not defined, but a household could be easily identified, and therefore individual members of a household also identified if the household is observed.

POLICY RECOMMENDATION 25

As part of the guidance on Profiling, the Data Protection Commissioner's Office can consider the following page from Singapore's PDPC on "Singapore's approach to AI governance"[39] or the UK's ICO on "Automated decision making and profiling"[40]. Expanding the examples to cover scenarios in financial services, where profiling will be used in insurance and fraud monitoring services to assist organisations in managing their activity appropriately.

DAPA

2, 25 (a, b), 39 (2), 45

"Identifiable natural person" means a **person** who can be **identified directly or indirectly**, by reference to an **identifier** such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity;

Processed in accordance with the right to privacy of the data subject:

"**Sensitive personal data**" means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject;

"**Profiling**" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth; personal preferences, interests, behaviour, location or movements;

A data controller or data processor shall delete, erase, anonymise or pseudonymise personal data not necessary to be retained under sub-section (1) in a manner as may be specified at the expiry of the retention period.

39 *https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework*

40 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/*

DAPA
2, 25 (a, b), 39 (2), 45
No category of sensitive personal data shall be processed unless section 25 applies to that processing. Without prejudice to section 44, sensitive personal data of a data subject may be processed where; ▪ The processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that: the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes; and the personal data is not disclosed outside that body without the consent of the data subject. ▪ The processing relates to personal data which is manifestly made public by the data subject; or ▪ Processing is necessary for: (i) the establishment, exercise or defence of a legal claim; (ii) the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject; or (iii) protecting the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.

GDPR	CCPA
Article 4 (1), 9	
"Personal data" comprises "any information that directly or indirectly relates to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an **identifier** such as a **name**, an **identification number**, **location data, an online identifier** or **to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person**." Online identifiers may be considered as personal data, such as **IP [internet protocol] addresses, cookie identifiers, and radio frequency identification tags.** In Article 9, the GDPR also specifies the personal data that falls under special categories of personal data – including elements of biometric data with further exemptions applied to it. Special categories are defined as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	"Personal information" comprises "information" that directly or indirectly relates to, is reasonably capable of being associated with, or could reasonably be linked to a particular consumer or household. The act defines "personal information," as: ▪ **Identifiers** such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers. ▪ **Commercial information**, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies. ▪ **Biometric information**. ▪ **Internet or other electronic network activity information**, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement. ▪ **Geolocation data.** ▪ **Audio, electronic, visual, thermal, olfactory**, or similar information. ▪ **Professional or employment-related information.** ▪ **Education information**, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99). **Inferences** drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behaviour, attitudes, intelligence, abilities, and aptitudes.

2.3.2 Public Data

DAPA states that personal data can be collected indirectly when the data is contained in a public record. Personal data can be collected if the data subject has deliberately made the data public, and sensitive personal data when the data subject has manifestly made it public. This means that data not clearly released by the data subject should not be considered "Public" – however, data in officially released documentation such as marriage licence records or the outcome of a court case should be considered "Public" as their purpose is to make this information readily available to all.

The GDPR requires that publicly available source data is subject to the same notifications – i.e. the processor must notify the data subject that they are processing this data. The term "manifestly made public" is also used – meaning a subject has purposefully made the data public, rather than failing to secure their social media accounts. The CCPA conversely does not consider data as "Personal Information" if it is data from a publicly available source.

DAPA
28 (2), 45 (1)
Data can be **collected indirectly** when the data is contained in **a public record;** the data subject has deliberately made the data public; Sensitive data is **allowed** to be processed if the processing relates to personal data which is **manifestly** made **public** by the data subject.

GDPR	CCPA
Article 14 (2)	
If a controller collects personal data from **a publicly available source**, the controller will be subject to the requirements laid down in the GDPR.	As mentioned previously - "Personal information" does not cover data from a publicly available source.

POLICY RECOMMENDATION 26

When preparing their guidance, the Data Protection Commissioner should create a set of examples of what a data subject should reasonably expect of treatment of their public data. It may for example, provide a comparison of a person has provided access to their social media account or forgotten to restrict access to their account. In the first example, the personal data is being made available to the controller or processor, whereas in the latter the data is available – but the user may not consider this is being captured and used.

In their guidance on "Personal Information Online"[41] on page 18 in the section "Collecting information about people from the internet" the ICO of the UK provides similar guidance on the things that should be considered.

2.3.3 Biometric / Genetic Data

DAPA provides a clear definition on biometric data, similar to those of the GDPR and CCPA, and then classifies it as sensitive personal data – which requires special treatment. It does not provide a definition of genetic data, but it does include it in the category of sensitive personal data.

DAPA defines "biometric data" as personal data resulting from specific technical processing based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition. In GDPR "genetic data" is defined as "personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question."

In addition to the additional security considerations of sensitive personal data, the duration for keeping this data also needs to be reviewed. A body wears over time, and the technology advances, so a one-off capture is

41 *https://ico.org.uk/media/for-organisations/documents/1591/personal_information_online_cop.pdf*

not sufficient to maintain for the lifetime of a given product. Continuous Due Diligence requires a re-check of the data, to ensure that one is still dealing with the same entity, and therefore data that is refreshed should lead to the historic information being archived or deleted.

DAPA
2
"**Biometric data**" means personal data resulting from specific technical processing based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition;

GDPR	CCPA
Article 4 (13, 14)	
"Biometric data" is defined as "personal data resulting from specific technical processes related to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data." **"Genetic data"** is defined as "personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question."	**"Biometric data"** is defined as "an individual's physiological, biological or behavioural characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information." Although there is a definition, there is no special provision for this data type, solely ensuring that this data is clearly personal information.

POLICY RECOMMENDATION 27

To ensure that genetic data is also properly safeguarded, the Data Protection Commissioner could consider providing a definition for "Genetic data".

The Data Protection Commissioner could also create a guidance page similar to the UK ICO's "What is Special Category Data"[42] where they provide further context on all of the categories.

42 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/*

2.3.4 Health and Medical Data

DAPA provides a clear definition on Health data, similar to that those of the GDPR and the CCPA, and then classifies it as sensitive personal data – which requires special treatment. The legislation goes on to define who should be processing Health Data. Under CCPA, the health data is protected under the Health Insurance Portability and Accountability Act (HIPAA).

DAPA
2, 46
"**Health data**" means data related to the state of physical or mental health of the data subject and includes records regarding the past, present or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates the data subject to the provision of specific health services; Personal data relating to the health of a data subject may only be processed: by or under the responsibility of a health care provider; or by a person subject to the obligation of professional secrecy under any law. The condition is met if the processing: is necessary for reasons of public interest in the area of public health; or is carried out by another person who in the circumstances owes a duty of confidentiality under any law.

GDPR	CCPA
Article 4 (15), 9 (1)	
Personal data related to health is held to a higher standard, since it is one of the special categories of data.	Medical data is excluded as outlined earlier.

POLICY RECOMMENDATION 28

As Health data is likely to be required in insurance services, when the Data Protection Commissioner prepares their guidance, clarification on these specific circumstances where a duty of confidentiality is required would assist in removing any confusion on whether these entities may or may not process this data. The UK ICO's webpage titled "What Is Special Category Data" also covers the treatment of Health and Medical data.

2.3.5 Households

Under DAPA, Households are mentioned as part of the exemptions of "household activity.". Households are also protected in so far as they covered as part of sensitive personal data i.e. data on property, family including names of the person's children, parents, spouse or spouses. Unlike the CCPA, but like the GDPR, the specific protection of households is not included. Enforcement action has extended the scope of the GDPR to potentially include Households.

DAPA
2, 51 (2)
The processing of personal data is exempt from the provisions of this Act if it relates to processing of personal data by an individual in the course of a purely personal or household activity; "Sensitive personal data" means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, **property** details, marital status, family details including names of the person's **children, parents**, **spouse or spouses**, sex or the sexual orientation of the data subject.

GDPR	CCPA
It does not specifically mention households, but there has been discussion and enforcement action that has extended the scope to potentially include households.	The definition of personal information refers to information relating to households in addition to information related to individuals.

POLICY RECOMMENDATION 29

As part of the guidance, the Data Protection Commissioner should review the approach to households, especially as large households are more likely to be statistically identifiable – as not creating this further classification potentially negates some of the benefits of the legislation afforded to a data subject because the subject may be more readily identifiable.

2.3.6 Children/Minors

As a Financial service is likely to capture the age of an individual as part of their KYC processes, they will need to consider the impact, if any, of Children or Minors using their services.

The DAPA does not specifically define the age of a child, or minor as this is defined under Article 260 of *the Constitution of Kenya 2010*[43]. It defines an adult as "an individual who has attained the age of 18 years and a child as "an individual who has not attained the age of 18 years." It is also defined in section 2 of "*The Children's Act 2001*"[44] which defines a child as "any human being under the age of 18 years" and a child of tender years as "a child under the age of ten years." It allows the rights given to the data subject to be exercised by a person who has parental authority or by a guardian.

The data processing for a child is not allowed, unless the parent or guardian provides consent, or if the processing advances the rights of the child. To ensure that the data subject is not a child, a data controller or processor must incorporate appropriate mechanisms. Mechanisms shall be based on available technology, the volume of data processed likely to be that of a child and the possibility of harm arising out of processing of personal data of a minor. The Data Protection Commissioner can specify further in the future to clarify this process. Where a data controller or processor exclusively provides counselling or child protection services to a child, they may not be required to obtain parental consent.

Credit/ Pexels-Katerina-Holmes

The GDPR does not define a "child," though it recognises children as "vulnerable natural persons" that merit specific protection. Specific protection should apply when children's personal data is used for marketing or collected for services offered directly to a child. Consent of a parent or guardian is required for providing services to a child below the age of 16. However, parental consent is not required in the context of preventative or counselling services offered directly to a child. When any information is addressed specifically to a child, data controllers must take appropriate measures to provide information relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language that the child can easily understand.

Under the CCPA, businesses must have opt-in consent to sell personal information of consumers under the age of 16 if businesses have "actual knowledge" that a consumer is under 16. For consumers under the age of 13, the child's parent or guardian has to affirmatively authorise the sale of the consumer's personal information. A business is deemed to have had actual knowledge of a child's age if it "wilfully disregards" a consumer's age.

POLICY RECOMMENDATION 30

As part of the guidance, the Data Protection Commissioner should provide examples of what controls are acceptable to validate parental approval. For example, a parent or guardian would also need to log into the service and then confirm they approve; or a confirmation link that is sent to a parent's email account and what mechanisms exist to validate that the account belongs to a parent rather than a friend. For financial services, this could be achieved by the KYC process extending to parents if a child can apply for the service.

POLICY RECOMMENDATION 31

The Data Protection Commissioner could also provide guidance on whether the protection of children should be covered by a risk-based approach as proposed in the "Risk-Based Age Checks and Parental or Guardian Consent"[45] of the UK's ICO.

43 *http://extwprlegs1.fao.org/docs/pdf/ken127322.pdf*
44 *http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ChildrenAct_No8of2001.pdf*
45 *https://ico.org.uk/for-organisations/accountability-framework/records-of-processing-and-lawful-basis/risk-based-age-checks-and-parental-or-guardian-consent/*

DAPA
27 (a), 33
A **right** conferred on a data subject may be **exercised** where the data subject is a minor, by a **person** who has **parental authority** or by a **guardian**; Every data controller or data processor shall **not process** personal data relating to a child **unless**: **consent** is given by the child's **parent or guardian**; the processing is in such a manner that **protects and advances** the **rights** and **best interests** of the child. A data controller or data processor shall incorporate **appropriate mechanisms** for age verification and consent in order to process personal data of a child. Mechanisms contemplated shall be determined on the basis of: **available technology**; **volume** of personal data processed; **proportion** of such personal data **likely** to be that of a child; possibility of **harm** to a child arising out of processing of personal data; and such other factors as may be specified by the Data Commissioner. A data controller or data processor that exclusively provides counselling or child protection services to a child may not be required to obtain parental consent as set out.

GDPR	CCPA
Article 8 (1)	**120 (c)**
The GDPR does not define "child," although it recognises children as "vulnerable natural persons" that merit specific protection with regard to their personal data. Specific protection should apply when children's personal data is used for marketing or collected for services offered directly to a child. Where the processing is based on consent, consent of a parent or guardian is required for providing information society services to a child below the age of 16. EU Member States can decide to lower the age, which may be no lower than 13. Controllers are required to make reasonable efforts to verify that consent is given or authorised by a parent or guardian. However, the consent of the holder of parental responsibility should not be necessary in the context of preventative or counselling services offered directly to a child. The GDPR does not provide for any exception for a controller that is not aware that it provides services to a child. It is not clear whether the consent requirement will apply if the child's personal data is unintentionally collected online. When any information is addressed specifically to a child, controllers must take appropriate measures to provide information relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, that the child can easily understand.	The CCPA does not define "child." The CCPA, however, ensures opt-in rights for minors under the age of 16. Businesses must have opt-in consent to sell personal information of consumers under the age of 16 if they have "actual knowledge" that a consumer is under 16. For consumers under the age of 13, the child's parent or guardian has affirmatively authorised the sale of the consumer's personal information. A business is deemed to have had actual knowledge of a child's age if it "wilfully disregards" a consumer's age.

2.3.7 Historical or scientific research

DAPA allows for processing of data for historical, statistical, journalistic, literature and art or scientific research, and the normal principles do not apply. The Data Protection Commissioner will prepare a specific code of practice on personal data for the purposes of journalism, literature and art, and a specific code of practice on the use of data for research, history and statistics. The legislation also provides specific sections on these uses. Processing for journalism and art still needs to be in line with the original purpose, and the data subject should not be identifiable, with appropriate measures taken to safeguard the data from being used for other purposes.

As fintechs are using more and more data to identify better ways to lend or to detect suspicious actors, the data they are using will potentially fall into the category of research even though this is commercial research. This is potentially further compounded if that data is then used to create synthetic data which is then processed by other parties. The DAPA section on processing for research, history and statistics states – "The further processing of personal data shall be compatible with the purpose of collection if the data is used for historical, statistical or research purposes" – implying that a specific definition might not be necessary. However, to ensure that customers are clear, it is advisable that the purposes of research, history and statistics be updated. Given the increased use of Machine Learning (ML) and Artificial Intelligence (AI), which leverage on research and historical data, such updating will help avoid any confusion between the definitions of research and its application in automated processing.

Data controllers and processors will need to demonstrate that their research is either scientific or historical in nature, and in the public interest. This applies to both public-sector and private-sector research. It can include, for example, technological development and demonstration, fundamental research, applied research and privately funded research. Commercial scientific research may therefore be covered, but there is need to demonstrate that it uses rigorous scientific methods and furthers a general public interest. However, commercial market research is unlikely to be covered, unless one meets this requirement. The remainder of the law follows a similar path as that for journalism and art, in so far as the data subject should not be identifiable, with appropriate measures taken to safeguard the data from being used for other purposes.

It is worth noting that although personal information can be pseudonymised or anonymised, care should be taken. In their *article*[46] in *'Nature Communications'*, Luc Rocher, Julien M. Hendrickx and Yves-Alexandre de Montjoye from Imperial College London and Belgium's Université Catholique de Louvain (UCLouvain) *show*[47] how data can be reverse engineered to identify discrete individuals with a small number of data points.

POLICY RECOMMENDATION 32

As fintechs are using more and more data to identify better ways to lend, or to detect suspicious actors, the data they are using will potentially fall into the category of research, especially if that data is then used to create synthetic data which is then processed by other parties. As such, guidance on pseudonymisation and anonymisation will be beneficial. As highlighted, the fact that anonymous data can be easily traced back to individuals' care should be taken to further clarify the risks.

POLICY RECOMMENDATION 33

The UK ICO has provided a good baseline on how to manage the needs of data created for research. It has clarified that research should be in the public interest, but the methods used should be demonstrable and scientifically rigorous. More information can be found in the section "(j) Archiving, research and statistics[48]" in their documentation "What are the conditions for processing." Singapore's PDPC also provided guidance on anonymisation and how to gain consent for research in their paper in response to a request for clarity from a medical institution.[49]

46 *https://www.nature.com/articles/s41467-019-10933-3*

47 *https://www.imperial.ac.uk/news/192112/anonymising-personal-data-enough-protect-privacy/*

48 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions10*

49 *https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Practical-Guidance-Provided-by-PDPC/2016-07-medical-research-institution-pg.pdf*

DAPA
30 (b), 52, 53
A data controller or data processor shall **not** process personal data, **unless** the processing is necessary for the purpose of **historical, statistical, journalistic, literature** and **art** or **scientific research.** **Journalism, literature and art** - The principles of processing personal data shall not apply where: processing is undertaken by a person for the publication of a literary or artistic material; the data controller reasonably believes that publication would be in the public interest; and the data controller reasonably believes that, in all the circumstances, compliance with the provision is incompatible with the special purposes. This shall only apply where it can be demonstrated that the processing is in compliance with any self-regulatory or issued code of ethics in practice and relevant to the publication in question. The Data Commissioner shall prepare a code of practice containing practical guidance in relation to the processing of personal data for purposes of journalism, literature and art. **Research, history and statistics.** The further processing of personal data shall be compatible with the purpose of collection if the data is used for historical, statistical or research purposes and the data controller or data processor shall ensure that the further processing is carried out solely for such purposes and will not be published in an identifiable form. The data controller or data processor shall take measures to establish appropriate safeguards against the records being used for any other purposes. Personal data which is processed only for research purposes is exempt from the provisions of this Act if data is processed in compliance with the relevant conditions; and results of the research or resulting statistics are not made available in a form which identifies the data subject or any of them. The Data Commissioner shall prepare a code of practice containing practical guidance in relation to the processing of personal data for purposes of research, history and statistics.

GDPR	CCPA
Article 5 (1), 9 (2), 14 (5), 17 (3), 21, 89	**105 (d), 140 (d, aa, ab) 145 (c)**
Has provisions for "scientific or historical research," as well as for "statistical purposes," with scientific research being interpreted in a "broad manner." The GDPR provides for exceptions in this field, which include specific requirements regarding the lawful basis for processing, considering that processing for scientific research purposes is compatible with processing for any initial purpose and can thus rely on the lawful ground for that initial purpose, and a specific exception to the right of erasure. Member States are allowed to provide for derogations from the rights of the data subject where personal data are processed for scientific or historical research purposes.	"**Research**" means scientific analysis, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for **other purposes is considered compatible** with the business purpose for which the personal information was collected.

GDPR	CCPA
Article 5 (1), 9 (2), 14 (5), 17 (3), 21, 89	**105 (d), 140 (d, aa, ab) 145 (c)**
The GDPR requires that technical and organisational measures are put in place for processing of personal data for research purposes, and the data should be de-identified and minimised for example by pseudonymisation. "**Scientific research** should be interpreted in a **broad manner**" and it should include technological development and demonstration, fundamental research, applied research, privately funded research and studies conducted in the public interest in the area of public health. The GDPR also refers to "historical research," which should also include research for genealogical purposes. Article 5(1)(b) of the GDPR requires that personal data shall be collected for specified, explicit and legitimate purposes and **not further processed for incompatible purposes**. However, it also specifies that further processing for scientific or historical research purposes "shall not be considered incompatible" with the original purpose. The GDPR provides that processing for research purposes must be subject to "**appropriate safeguards**" for the rights of the data subject, which shall ensure that technical and organizational measures are put in place in particular to **ensure data minimisation. Pseudonymisation** is given as an example of such measures. One of the permissible uses of special categories of personal data, other than on the basis of consent of the data subject, is where processing is necessary for scientific or historical research purposes on the basis of Union or Member State law, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.	The CCPA imposes specific safeguards for research conducted on consumer information collected initially for other purposes, such as that the personal information: ▪ should be subsequently **pseudonymised and de-identified;** ▪ should be made subject to **technical safeguards** that prohibit re-identification of the consumer to whom the information may pertain; there is a specific requirement that it should be subject to **additional security controls** that allow access to this information only as are necessary to conduct the research; ▪ should be made subject to business processes that specifically **prohibit re-identification of the information and protected from any re-identification attempts**; ▪ should be made subject to business processes to **prevent inadvertent release of de-identified information**; ▪ should be used **solely for research purposes that are compatible** with the context in which the personal information was collected; and ▪ **not** be used for any **commercial purpose**. Undertaking internal research for technological development and demonstration is defined as a "business purpose." Clinical trials are excluded from its scope as these are covered by other legislation.

2.4 Accuracy: What can a consumer do if the data is not accurate?

A fundamental right in all legislation is for a customer to be able to correct or erase information that is incorrect but subsequently processed. As mentioned earlier, there is no clarity in DAPA on how a customer would identify inaccurate data, without a Data Subject Access Request Process, but once that is clarified the DAPA requires the correction or erasure to be done quickly - specifically "without delay."

Many of these rights are defined in the right of rectification and erasure. The data concerned can be inaccurate, out-dated, incomplete, or misleading. Data that is no longer authorised to be retained, irrelevant, excessive, or obtained unlawfully should be erased or destroyed. If the data has been shared with others, this shared data should be treated the same way. If the data is required for evidence, its processing should be restricted, and the data subject should be informed. This clause is highly relevant to financial services as financial institutions will need to keep key data to uphold their duties. But what is important to note is that not all information will be required for evidence. For example, KYC data will be stored but if financial institutions are capturing further information such as device IP address or "device fingerprinting", that information will not be needed if the customer stops being a customer as they will no longer be assessing the risks.

Once a data processor is aware of the need to correct data, they should restrict processing of that data, whilst the data is being verified – this is at both the data controller or processor. To ensure there is little room for confusion, DAPA provides further clarity on the restrictions – data processing is still allowed for a legal claim, protection of the rights of another, or public interest. Before they remove the restrictions, the processor should notify the data subject.

The data processor should implement mechanisms to ensure that time limits are observed for the rectification, erasure or restriction of processing and also for periodic reviews of the need for storage. However, the expected time limits on these activities are not defined.

The GDPR includes the option for the data controller to have incomplete data completed, including by means of providing a supplementary statement, and the CCPA reinforces the need for the data subject to be verified, to prevent rogue actors from making amendments to data that leads to false data being introduced.

POLICY RECOMMENDATION 34

As part of their guidance, the Data Protection Commissioner should ensure that a data processor or controller has a clear retention policy for any data held and provides a clear reason if the time period for retention seems excessive, and that the controller or processor have a process for rectifying inaccurate data. Take as an example a pension policy that captures a person's name and address, as well as the company the data subject worked for at time of registration. If the recipient of the pension has moved to a new company and a new location but did not notify the pension company, it could be several years for this inaccuracy to come to light. Once the recipient has provided evidence the pension company will update its records but may still wish to retain the original employer's details for accountability on the source of funds. The historic address however is now likely irrelevant so can be deleted.

POLICY RECOMMENDATION 35

The Data Protection Commissioner should provide guidance for when an inaccuracy is still not rectified to the satisfaction of the data subject. Providing guidance such as Section 15.45 of Singapore's PDPC document on "Advisory Guidelines on Key Concepts in the Personal Data Protection Act"[50] or "Your Right to Get Your Data Corrected"[51] by the UK's ICO will not only provide the data subject with a framework for escalation of the complaint, but also explain why data may not be corrected in the way the data subject expected. Equivalent guidance for data controllers or processor and examples to help explain the approach to take are provided in the overview of "Principle (d): Accuracy"[52].

50 *https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en*

51 *https://ico.org.uk/your-data-matters/your-right-to-get-your-data-corrected/*

52 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/*

DAPA
25 (f) 26 (d, e), 34. 40
Every data controller or data processor shall ensure that personal data is **accurate** and, where necessary, **kept up to date**, with every **reasonable step** being taken to **ensure** that any **inaccurate** personal data is **erased** or **rectified** without delay; A data subject has a right to correction of false or misleading data; and to deletion of false or misleading data about them. A data controller or data processor shall, at the request of a data subject, **restrict** the **processing** of personal data where: **accuracy** of the personal data **is contested** by the data subject, for a period enabling the **data controller** to **verify** the accuracy of the data. Where processing of personal data is restricted under this section: the personal data shall, unless the data is being stored, **only** be processed **with** the data subject's **consent or** for the establishment, exercise or defence of a **legal claim**, the **protection** of the rights of **another person** or for reasons of **public interest**; and the data controller shall **inform** the data subject **before withdrawing** the **restriction** on processing of the personal data. The data controller or data processor shall implement **mechanisms** to ensure that **time limits** established for the rectification, erasure or restriction of processing of personal data, or for a periodic review of the need for the storage of the personal data, is **observed**. A data subject may request a data controller or data processor: to **rectify without** undue **delay** personal data in its possession or under its control that is **inaccurate**, **out-dated**, **incomplete** or **misleading**; to **erase** or **destroy** without undue delay personal data that the data controller or data processor is **no longer authorised** to retain, **irrelevant**, **excessive** or **obtained unlawfully**. Where the data controller has shared the personal data with a third party for processing purposes, the data controller or data processor shall take all reasonable steps to **inform third parties** processing such data, that the data subject has **requested**: the **rectification** of such personal data in their possession or under their control that is inaccurate, out-dated, incomplete or misleading; **or** the **erasure** or **destruction** of such personal data that the data controller is no longer authorised to retain, irrelevant, excessive or obtained unlawfully. Where a data controller or data processor is required to rectify or erase personal data but the personal **data** is **required** for the purposes of **evidence**, the data controller or data processor shall, instead of erasing or rectifying, **restrict** its **processing** and inform the data subject within a reasonable time.

GDPR	CCPA
Article 5 (1), 16	**106**
Every **reasonable step** must be taken to **ensure** that personal data that are **inaccurate**, having regard to the **purposes** for which they are processed, are **erased** or **rectified** without delay ('accuracy'); The data subject shall have the right to obtain from the controller without undue delay the **rectification** of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have **incomplete** personal data **completed**, including by means of **providing** a **supplementary statement**.	A consumer shall have the right to request a business that maintains **inaccurate** personal information about the consumer to **correct** that inaccurate personal information, taking into account the **nature** of the personal information **and** the **purposes** of the processing of the personal information. A business that receives a **verifiable** consumer **request** to correct inaccurate personal information shall use **commercially reasonable efforts** to correct the inaccurate personal information as directed by the consumer.

2.6 Users right to be forgotten

This is one of the most feared rights – as it conjures up the image that a consumer can have absolute anonymity – but it actually is misunderstood as although it is the strongest right afforded to a customer, its purpose is to provide a mechanism for guaranteeing the privacy of a data subject. It includes the right to withdraw consent, to object to processing, and for the deletion, but there are exceptions where the obligations of the data controller or processor can outweigh those of the data subject. As mentioned earlier, there is no clarity in DAPA on how a customer would know what data they might wish to object to being processed, without a Data Subject Access Request Process, but DAPA requires the correction or erasure to be done quickly - specifically "without delay". Many of these rights are also defined in the right of rectification and erasure.

Data that is no longer authorised to be retained, irrelevant, excessive or obtained unlawfully should be erased or destroyed. If the data has been shared with others, this shared data should be treated the same way. If the data is required for evidence, its processing should be restricted and the data subject should be informed. This clause is highly relevant to financial services, as they will need to keep key data to uphold their duties. But what is important to note is that not all information will be required for evidence.

Once a processor is aware of the need to correct data, they should restrict the processing of that data, whilst the data is being verified – this is at both the data controller and or third-party processor. To ensure there is little room for confusion, DAPA provides further clarity on the restrictions – data processing is still allowed for a legal claim, protection of the rights of another, or public interest. Before they remove the restrictions, the processor should notify the data subject. The processor should implement mechanisms to ensure that time limits are observed for the rectification, erasure or restriction of processing and also for periodic reviews of the need for storage. However, the expected time limits on these activities are not defined.

The GDPR includes the option for the data controller to have incomplete data completed, including by means of providing a supplementary statement, and both the GDPR and the CCPA reinforce the need for the data subject to be verified, to prevent rogue actors from making amendments to data that leads to false data being introduced. All legislation provides for the protection of erasure under research if erasure is likely to impair the achievement. The CCPA adds the condition – if the consumer has provided informed consent. Both the GDPR and CCPA provide for the exercising of this right to be free of charge – a fee can be charged if the requests are unfounded, excessive or repetitive.

In addition to the exemptions already identified in DAPA, the CCPA and the GDPR allow for exemption due to free speech or freedom of information. The CCPA provides further exemptions, most notable to: detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity; fulfil the terms of a written warranty or product recall conducted in accordance with federal law. It is worth noting that data used in research is not necessarily subject to erasure. If the work is sufficiently advanced and the request for removal after giving consent arrives when the research has concluded and been processed, might make the removal complex.

Credit/ Privecstasy-Unsplash

> Data that is no longer authorised to be retained, irrelevant, excessive or obtained unlawfully should be erased or destroyed. If the data has been shared with others, this shared data should be treated the same way.

DAPA
34 (1) 40 (1, 2
A data controller or data processor shall, at the request of a data subject, **restrict** the **processing** of personal data where the data subject has **objected to the processing**, **pending verification** as to whether the **legitimate interests** of the data controller or data processor overrides those of the data subject. A data subject may **request** a data controller or data processor to **erase** or **destroy,** without undue delay, personal data that the data controller or data processor is no longer authorised to retain, is irrelevant, excessive or obtained unlawfully. Where the data controller has shared the personal data with a third party for processing purposes, the data controller or data processor shall take all reasonable steps to inform third parties processing such data, that the data subject has requested the erasure or destruction of such personal data that the data controller is no longer authorised to retain, is irrelevant, excessive or obtained unlawfully. Where a data controller or data processor is required to rectify or erase personal data but the personal data is required for the purposes of evidence, the data controller or data processor shall, instead of erasing or rectifying, restrict its processing and inform the data subject within a reasonable time.

GDPR	CCPA
Article 12 (3), 17	**105 (a, b, c) 130 (a), 145 (h)**
Requirement under the "right to erasure" or "right to be forgotten": ▪ Data subjects have a right to request erasure to the controller as provided under Article 17. ▪ Upon a valid request for erasure, controllers are obligated to take reasonable steps to have processors erase data. Generally, processors must support the controller to comply with data subjects' rights if required by the controller.	Requirement under "right to deletion": ▪ Shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.
The **right to erasure** does **not** apply to the extent that the processing is necessary for scientific or historical research purposes if erasure "is likely to render impossible or seriously impair the achievement of the objectives of that processing."	This does not apply to research, "When the business' deletion of the information is likely to render impossible or seriously impair the ability to complete such research, if the consumer has provided informed consent."
This right can be exercised **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character. The GDPR specifies that data controllers must have in place **mechanisms** to ensure that the request is made by the data subject whose personal data is to be deleted. Data subjects must be informed that they are entitled to ask for their data to be erased. **Exceptions**: among the exceptions to the right of erasure provided by the GDPR are: ▪ **freedom of expression** (free speech), freedom of information; ▪ processing for research purposes of personal data that, if erased, would impair the objectives of the research; ▪ **establishment**, **exercise** or **defence** of legal claims; and	This right can be exercised **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character. Businesses must have in place **mechanisms** to ensure that the request is made by the consumer whose personal information is to be deleted. The privacy notice must inform consumers that they are entitled to ask for the deletion of their personal information. **Exceptions**: among exceptions to the right of deletion provided by the CCPA are: free speech or another right provided by law; ▪ processing for **research purposes** ▪ processing of that personal information is necessary to protect against **illegal activity or prosecute those responsible for the activity;** and

GDPR **Article 12 (3), 17**	CCPA **105 (a, b, c) 130 (a), 145 (h)**
▪ for **complying with a legal obligation.** The right to erasure only applies if any of the following grounds apply, such as where consent is withdrawn and there is no other legal ground for processing, or when personal data is no longer necessary for the purpose for which it was collected.	▪ for complying with a **legal obligation.** ▪ to perform a **contract between the business and the consumer;** ▪ **detect security incidents,** protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity; ▪ **debug to identify and repair errors that impair existing intended functionality;**
Data subjects' requests under this right must be replied to without "undue delay and in any event within **one month** from the receipt of the request." The deadline can be extended to **two additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request. Methods to submit a request include **writing, orally and by other means which include electronic means** when appropriate. The scope of this right is not limited to the data controller, but also impacts **third parties**, such as recipients, data processors and sub-processors that may have to comply with erasure requests. If the controller has made the personal data public, controller must take "reasonable steps, including technical measures," to inform other controllers that are processing the personal data that the data subject has requested the erasure of any links to, or copy or replication of, those personal data. **Exemptions**: in addition to the exceptions enumerated under "Similarities", a data controller is also exempted to comply with erasure requests for reasons of **public interest in the area of public health**.	▪ **to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business;** ▪ otherwise use the consumer's personal information, internally, in **a lawful manner that is compatible with the context in which the consumer provided the information;** ▪ fulfil the terms of a written warranty or product recall conducted in accordance with federal law; and ▪ where personal information reflects a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, non-profit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding providing, or receiving a product or service to or from such company, partnership, sole proprietorship, non-profit, or government agency. The CCPA does not limit the scope of this right to specific situations, categories of personal information or purposes. The right generally applies to personal information that a business has collected from the consumer and the consumer does not have to justify his or her request – although there are "excessive use" clauses. The deadline to respond to a right request is **45 days** from the receipt of the consumer's request. The deadline can be extended an **additional 45 days** when reasonably necessary, if the consumer is informed within the first 45 days, according to Section 1798.130(a). **However**, there seems to be an inconsistency in the current text of the law. In another provision, which generally refers to exceptions to the law (Section 1798.145), the CCPA states that "the time period to respond to any verified consumer request may be extended by up to **90 additional days** where necessary, taking into account the complexity and number of the requests."

POLICY RECOMMENDATION 36

As part of the creation of guidance, the Data Protection Commissioner can provide clarification on how a data subject can withdraw consent to processing – for example if the process of confirmation is simple, should the option to withdraw be equally as simple. It is also important to establish the mechanism for requesting the withdrawal of consent, for example in writing, orally or by other means which might include electronic means, ensuring that the data subject is identified as part of this process.

POLICY RECOMMENDATION 37

As part of the guidance created, the Data Protection Commissioner should provide example use cases on what to expect when requesting data be deleted. For financial services such a use case would be retention of KYC data that is captured at time of on-boarding, but potentially still required for seven years after the last transaction, or indefinitely if there is a balance on the account. For services such as pensions or life insurance, these periods are much longer. A customer could wrongfully assume that a request for deletion would lead to this data being removed immediately.

The UK's ICO provide guidance for the Data Controller or processor "**Right to Erasure**"[53] and for the Data Subject "

Your Right to Get Your Data Deleted"[54].

POLICY RECOMMENDATION 40

All parties also need to understand if fees can be applied, and if not for the initial request, whether fees be applied for unfounded, excessive or repetitive requests. In both cases – the fees will need further guidance and oversight by the Data Protection Commissioner to prevent potential abuse.

POLICY RECOMMENDATION 39

Once a request has been submitted, data controllers and processors should have a clear timeline for the assessment and processing provided by the Data Protection Commissioner. The GDPR gives the processor one month, but this can be extended to an additional two months, if the erasure is complex. To reduce the number of challenges that might be escalated, the Data Protection Commissioner should provide good examples on what reasons a request might be denied, for example where the data is used to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity or for warranty or product recall purposes.

POLICY RECOMMENDATION 41

For data that is used for research, the Data Protection Commissioner should also provide case studies - for example if the consent is withdrawn before the research has been concluded, what should the data subject reasonably expect?

53 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/*
54 *https://ico.org.uk/your-data-matters/your-right-to-get-your-data-deleted/*

2.6 Integrity & Confidentiality / Security

The use of anonymisation and pseudonymisation is proposed as part of the controls to ensure confidentiality – however, please review Section on "2.3.7 Historical or scientific research" on the considerations in this matter.

DAPA promotes the goal of data protection by design or default and provides implementation guidance on technical and organisational measures. These measures should be designed to implement the data protection principles in an effective manner; and to integrate necessary safeguards for that purpose into the processing. These measures should be applied when deciding how to process the data, and when actually processing the data. By ensuring that only data required for a specific purpose and taking into account the amount of data collected, what processing is required, how long it is stored for, how accessible it is and the cost of processing the data and the technologies and tools used.

To give effect to this section, the data controller or data processor shall consider a number of measures. A risk assessment of the foreseeable internal and external risks to personal data, having identified the risks, to then maintain appropriate safeguards against these risks such as pseudonymisation and encryption of personal data are required. In the event of a physical or technical incident, the data processor and control should ensure the ability to restore the availability and access to personal data in a timely manner. There should be a process of verifying that the safeguards are effectively implemented and to ensure that the safeguards are continually updated in response to new risks or deficiencies.

We discuss the specific requirements for the DPIA in Section 2.7.3.4 Data Protection Impact Assessment.

From an operational perspective, DAPA also provides guidance for an organisation. When providing the service over a network, the data controller should consider the state of technology available; the cost of implementing security, any special risks from the processing and the nature of the data being processed. If a data processor is used, the controller should select a processor who provides sufficient guarantees for the organisational matters, as well as ensuring that the contract binds the processor to only act on the instructions received from the data controller and perform all the obligations of a controller. If the processor acts independently of the instructions of the controller, they will be deemed to be a controller with all the attendant obligations such as ensuring consent, among others. The controller and processor should also ensure their employees or representatives comply with these measures.

POLICY RECOMMENDATION 41

When preparing guidance for data controllers or processors, the Data Protection Commissioner can assist these companies with a detailed checklist of the minimum things that should be considered. Key areas such as:

- Risk assessment of processing;
- What is the state of the art, and the cost of implementation?
- A clear Information Security Policy with proper enforcement;
- Use of an established framework such as **Cyber Essentials**[55] the **Open Source Security Foundation**[56] or for fintechs the **Cyber Resilience and Financial Organisations: A Capacity-building Tool Box**[57] from the Carnegie Endowment for International Peace (CEIP);
- The use of encryption or pseudonymisation;
- Recovery process;
- Regular testing of tools and procedures.

Singapore's PDPC has provided a **"Guide to Securing Personal Data in Electronic Medium"**[58] and the UK's ICO has provided a dedicated overview with guidance on "Security"[59].

55 *https://www.ncsc.gov.uk/cyberessentials/overview*
56 *https://openssf.org/*
57 *https://carnegieendowment.org/specialprojects/fincyber/guides*
56 *https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guidetosecuringpersonaldatainelectronicmedium0903178d-4749c8844062038829ff0000d98b0f.pdf?la=en*
59 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/*

DAPA
2, 41, 42
"**Anonymisation**" means the removal of personal identifiers from personal data so that the data subject is no longer identifiable; "**Pseudonymisation**" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, and such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person; **Data protection by design or by default.** Every data controller or data processor shall implement **appropriate technical** and **organisational measures** which are designed: to **implement** the data protection principles in an **effective manner**; and to **integrate necessary safeguards** for that purpose into the processing. This applies both at the **time** of the **determination** of the **means of processing** the data and at the **time of the processing**. A data controller or data processor shall implement appropriate technical and organisational measures for ensuring that, by default, **only** personal **data** which is **necessary for** each **specific purpose** is processed, taking into consideration the **amount** of personal data **collected**; the **extent** of its **processing**; the **period** of its **storage**; its **accessibility**; and the **cost** of **processing** data and the **technologies** and **tools** used. To give effect to this section, the data controller or data processor shall consider measures such as: to identify **reasonably foreseeable** internal and external **risks** to personal data under the person's possession or control; to **establish** and **maintain** appropriate **safeguards** against the identified risks; to the **pseudonymisation** and **encryption** of personal data; to the ability to **restore** the **availability** and **access** to personal data in a timely manner in the event of a physical or technical incident; to **verify** that the safeguards are **effectively** implemented; and to ensure that the **safeguards** are continually **updated** in response to **new risks** or deficiencies. **Particulars of determining organisational measures.** In determining the appropriate measures, in particular, where the processing involves the **transmission of data** over an information and communication network, a data controller shall have regard to: the **state** of **technological development** available; the **cost** of implementing any of the security measures; the **special risks** that exist in the processing of the data; and the **nature** of the **data** being processed. Where a data controller is **using** the services of a data **processor**: the data controller shall opt for a data processor who provides **sufficient guarantees** in respect of organisational measures for the purpose of complying; and the data controller and the data processor shall enter into a **written contract** which shall provide that the data processor shall act **only** on **instructions** received **from** the **data controller** and shall be bound by **obligations** of the data controller. Where a data **processor** processes personal data **other than** as **instructed** by the data controller, the data processor **shall be deemed** to be a **data controller** in respect of that processing. (4) A data controller or data processor shall take all reasonable steps to ensure that any **person employed** by or **acting under the authority** of the data controller or data processor, **complies with** the relevant **security measures**.

GDPR	CCPA
Article 4 (5), 6 (4), 25, 32 (1)	
It is worth noting in Recital 26, the following - "personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered as information on an identifiable natural person."	"**Pseudonymisation**" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that

GDPR	CCPA
Article 4 (5), 6 (4), 25, 32 (1)	
It is worth noting in Recital 26, the following - "personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered as information on an identifiable natural person." The controller cannot be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purposes of complying with the GDPR, if the purposes of that processing do not or do no longer require the identification of a data subject by the controller. However if a data subject provides the additional/missing information the controller has to **re-identify** a dataset in order to comply with **requests for the rights of the data subject.**	the additional information is kept separately and is subject to technical and organisational measures to ensure that the personal information is not attributed to an identified or identifiable consumer. Other than the definition, there is little confirmation on whether pseudonymisation reduces the burden on an entity. Its rules cannot be construed "to require a business to re-identify or otherwise link information that is not maintained in a manner that would be considered personal information."
Implement appropriate technical and organisational measures: processors must ensure security for processing data, which could include encryption or pseudonymisation practices.	

2.7 Accountability: Impact of Non-Compliance

If a decision taken by a data controller or processor leads to a data subject becoming aggrieved, the data subject can lodge a complaint with the Data Protection Commissioner orally or in writing. DAPA also confirms that the Data Protection Commissioner can carry out periodical audits of the processes and systems of the data controller or processor to ensure compliance with the Act. The Data Protection Commissioner has yet to prescribe a process for the periodic audits, but outlines what information needs to be captured and the investigation be concluded within 90 days.

If an investigation is required, the Data Protection Commissioner has the authority to order any person to attend a meeting to be examined orally, or provide a written statement setting out all the information required. The person attending may also be required to provide further evidence in their possession – unless another Act prevents them. A person failing to provide the necessary statement or information or if the information provided is false or misleading, such person commits an offence.

When the Data Protection Commissioner is satisfied that a person has failed or is failing, an enforcement notice may be served. The notice will confirm what portions of the Act the person needs to address, the measures they should take and a time frame (of not less than 21 days) in which they need to rectify the situation, and any right of appeal. Any person who, without reasonable excuse, fails to comply with an enforcement notice commits an offence and is liable on conviction to a fine up to 5 million KES (US$ 45,000 at time of writing) or to imprisonment for up to two years, or to both.

The Data Protection Commissioner can obtain a search warrant from a Court of law to enter and search any premises for the purpose of discharging any function or exercising any power under DAPA. A person will be committing an offence if they:

- Obstruct or impede the Data Protection Commissioner;
- Fail to provide assistance or information requested;

- Refuse to allow the Data Protection Commissioner (or those with the Commissioner) to enter any premises;
- Give information which is false or misleading in any material aspect.

On conviction, the person will be liable to a fine not exceeding 5 million KES (US$ 45,000 at time of writing) or to imprisonment for a term not exceeding two years, or to both. If the Data Protection Commissioner is satisfied that a person has failed or is failing, the Data Protection Commissioner may also issue a penalty notice requiring the person to pay to the Office of the Data Protection Commissioner up to 5 million KES), or in the case of an undertaking, up to one per centum of its annual turnover of the preceding financial year, whichever is lower.

In determining whether or not to give a penalty notice to a person and amount to be applied of the penalty, the Data Protection Commissioner shall consider:

- The nature, gravity and duration of the failure;
- The intentional or negligent character of the failure;
- Any action taken by the data controller or data processor to mitigate the damage or distress suffered;
- The degree of responsibility of the data controller or data processor, taking into account technical and organisational measures;
- Any relevant previous failures by the data controller or data processor;
- The degree of co-operation with the Data Protection Commissioner, in order to remedy the failure and mitigate the possible adverse effects of the failure;
- The categories of personal data affected by the failure;
- The manner in which the infringement became known to the Data Protection Commissioner, including whether, and if so to what extent, the data controller or data processor notified the Data Protection Commissioner of the failure;
- The extent to which the data controller or data processor has complied with previous enforcement notices or penalty notices;
- Adherence to approved codes of conduct or certification mechanisms;
- Any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly);
- Whether the penalty would be effective, proportionate and dissuasive.

All of these elements are articulated within DAPA – ensuring that a failure can be verified against expected behaviour.

The Office of the Data Protection Commissioner has issued their *Complaints Management Manual*[60] to provide further clarity on the procedures that they will take to receive, validate and progress a complaint, with legal action also having started independently of the Office of the Data Protection commissioner as "public spirited" citizens and organisations have challenged existing rollouts. The Office of the Data Protection Commissioner have also clarified some of the personnel that will be performing these tasks.

A Complaint may be lodged by: a Complainant in person; a person acting on behalf of the Complainant; a group of persons; any other person authorized by law to act for the complainant. A complaint can also be anonymous, but this can introduce complexity if not enough information is available to support an assessment.

The "person acting on behalf of the complainant" opens the door for organisations to potentially act as consumer champions - and the creation of class law suits. Whilst this could be challenging for data controllers or processors, a similar issue was expected under GDPR but a high volume of notifications to the data commissioner created a large backlog, and in the UK the requirement to create a law suit was further complicated. Although DAPA does not have a specific provision for class actions (or representative suits), under Kenyan law representative suits are instituted where many persons have the same interest in any proceedings. In such instances, one or more of such persons may commence representative proceedings under Order 1, rule 8, Civil Procedure Rules 2010.

The test for a representative suit is that of common interest, as claims that do not demonstrate common interest cannot be pooled into a representative suit. Parties on whose behalf a claim is commenced can

60 *https://www.odpc.go.ke/download/odpc-charter/?wpdmdl=7622*

apply to the court to opt in to the suit. The recent data protection case against the rollout of National Integrated Identity Management System (NIIMS) popularly known as *Huduma Namba*, was brought by Katiba Institute a research and public interest NGO operating in Kenya. Expressing the rights afforded in Articles 22 and 23 of the Constitution – the right to any person to sue on behalf of themselves and others whenever any right in the Bill of Rights (Chapter 4 of the Constitution) is infringed or threatened with infringement. Privacy is protected under article 31 of the Constitution, as part of the Bill of Rights.

In the *High Court Judgment*[61], decided on 14 October 2021, the civil society organisation was allowed in the judicial review proceedings on grounds that although the organization was not a data subject for purposes of section 56 of the Act to lodge a complaint, it had shown sufficiency of interest. This may open the doors for other "public spirited entities" raising an issue, but prior evidence of such "public spirit" may also be required.

> *"The 1st applicant falls into any of these categories; it may not be 'a public spirited citizen raising a serious issue of public importance' but it is, for all intents and purposes, a public spirited entity raising an issue of public interest. It can also be recognised as a pressure group in the 'implementation of Kenya's 2010 Constitution and generally to seek the development of a culture of constitutionalism in Kenya'...I would say the same of the 1st applicant. It is true, as the interested party submitted, the 1st applicant lacked standing to lodge a complaint to the Data Commissioner under section 56 of the Data Protection Act, but it certainly had the necessary locus to lodge these proceedings because of sufficiency of interest...For the reasons I have given, I am satisfied that the 1st applicant has properly invoked the judicial review jurisdiction of this honourable court and therefore its application is tenable and deserves to be considered on its own merits."*

Complaints may be lodged through: Walk in - in person in the Office Headquarters in Nairobi; By letters through the post office; Online via email, web posting or through a designated complaints management system; By calling the Office of the Data Protection Commissioner; Telephone / fax; In writing including Braille & other methods for other persons with disability; Text message short SMS message to a dedicated number. The Office may also initiate complaints including those that are: Relevant to its mandate exposed through media (open source) or an anonymous persons; and by private actors including Civil Society Organisations.

A complaint to the Office should preferably be made in writing but oral complaints are also possible. A complaint may be made anonymously or treated in order to protect the identity of or particulars of, the complainant. A complaint form is set out in the manual, which must be completed and relevant supporting documentation provided.

When lodging a complaint, the complainant will provide the following: Capacity in which the complaint is lodged i.e. in person or on behalf of a third party etc.; Provide personal information to identify the complainant; Date of occurrence of the alleged infringement; The nature of the complaint; Identify any other persons that can provide further information; any person or institution that has previously made attempts to resolve the matter; Any actual or potential harm or any urgency to be taken note of; any supporting documents to be used in the investigation process; any redress/relief the complainant is anticipating. Further time may be allowed to provide further information, but no more than 21 working days from the date of receipt of the complaint. Any Complaint received will be acknowledged immediately but not later than 7 working days from date of receipt. All complaints received by the Office will be handled with confidentially. Including allowing the complainant to have their details kept confidential in communication with the respondent(s).

If the Office has received request for confidentiality but is of the opinion that disclosure of the particulars is necessary for resolving the dispute; the Office will inform the complainant and ask for approval for their particulars to be disclosed. If the complainant declines to give such consent, the Office shall decline to process the complaint and mark it as closed and inform the complainant of the decision not to proceed. If necessary the Office will also liaise with the Witness Protection Agency to accord protection as provided by the Witness Protection Act 2006.

Although there is a Screening Allocation and Categorisation process, and a maximum seven days for acknowledgment, there is not an SLA provided

61 *http://kenyalaw.org/caselaw/cases/view/220495/*

for allocation and categorisation. A complaint once entered into the register will be forwarded for allocation to a complaints handling officer for screening and preliminary inquiry. The complaint handling officer after preliminary inquiry will advise the complainant in writing if the matter is admissible or will refer it to others as appropriate or reject the complaint - informing the complainant within 21 days. The complaint handling officer will preliminarily verify allegations of the complaint through the following means: reviewing the documents provided, and/or Preliminary research, and/or Phone calls, emails, face-to-face interrogations and letters. The complaint-handling officer will identify the category of inaction or violation and indicate if it fits into the categorization of the mandate of the Office.

The complaints handling officer will: Communicate with the respondent requesting their comments on the complaint. The respondent will have 14 days to respond to the claim. If after 14 days there is no response, the complaints handling officer will write a reminder giving a further seven (7) days to comply. If there is still no response then a final reminder will be issued giving the respondent another final seven (7) days to respond. At the end of 28 days (assumed to be from when the first communication was issued, the Office will issue Notice to Show Cause why the Office cannot proceed without the respondent's response. If the respondent fails to respond, the Office may: Progress the complaint to investigation without the respondent; Institute legal proceedings against the respondent; Report the respondent in the Office's annual statutory report.

Once the complaint handling officer has considered that the admissibility criteria has been met, and categorisation has been done, preliminary Inquiry will commence. A complaint's handling officer who has any interest in the matter allocated to them must put on record the interest they have in the matter. Where a preliminary assessment determines that the complaint does not fall within the jurisdiction of the Office, the complaint handling officer will: Advise the complainant of the alternative legal or practical remedies; Recommend referral to an appropriate institute; Issue notice of inability to proceed for reasons given; Offer the complainant an opportunity to appeal the decision within 30 days; The appeal will be made in prescribed form and addressed to the Commissioner; A copy of the advisory letter will be filed in the general file.

The Complaint screening officer upon receipt of an admissible complaint that is simple and straight forward in nature and requires urgent attention will: Notify the Director Complaints and Investigations of the urgency of the matter; Discuss the proposed quick intervention proposed i.e. telephone call, Email or visit the respondent's office for a quick clarification; Commence preliminary Inquiry for Frontline resolution that should be completed within 5 working days; The complaint screening officer will record the terms of resolution (the outcome) and any action taken and file on General File in the registry; The screening officer will notify the complainant of the outcome from the frontline; If the complaint is not resolved within 5 days working days period, the complaint will proceed through the normal processes of handling complaints

The Office shall keep a register of complaints. The registry will keep a database of complaints received and handled by recording the reference number, the category of complaint, relevant dates of action and the resolution.

The Office shall not charge any fee for lodging and determining a complaint. The Office may reimburse any witness summoned to the Office to give evidence.

Where two or more complaints are lodged at the Office bearing similar allegations and same respondents, the Office may: Order consolidation of such complaints; Inform the complainants of the same; Treat one complaint as a test complaint and stay further action on the other complaints till resolution of the test complaint; The decision on the test case shall apply to the other complaints that are consolidated; The complainants in all the consolidated matters will be notified of the resolution by the Office. A complainant may withdraw a complaint pending before the Office at any stage during consideration. The Office may continue with the investigation of the complaint if such investigation is in the public interest.

A complaint is concluded in the following circumstances: If found inadmissible and rejected; If it is resolved; If withdrawn by the Complainant; or If the complaint lapses. The Office may resolve the complaint through: Conduct inquiry; Request and obtaining information or documents; Further investigation; Undertaking mediation, negotiation and conciliation; Constitute a hearing panel; Write or summon any persons to attend; Obtain warrant of arrest for breach of any summons or orders of the Office: Obtain orders from court authorizing search and seizure

At the conclusion of the assessment and after gathering evidence, the Complaint handling officer will write

a report on the process and determination making appropriate recommendation. If a person is aggrieved by an action taken against them by the Data Protection Commissioner including in enforcement and penalty notices, they have the right to appeal against the enforcements in the High Court.

POLICY RECOMMENDATION 42

The better the guidance provided by the Data Protection Commissioner on the minimum standards required, the easier enforcement will be and hopefully the less likely there will be a breach as all parties are aware of their responsibility and how they need to adhere to it. All guidance can then also be referenced by the enforcement notice, to reduce the administrative burdens in such a task.

To ensure that organisations are aware of the action that can be taken, the UK's ICO has provided guidance on the action they can take in their section on "Enforcement"[62]. To ensure that parties are compliant, they also provide a regular update of the "Enforcement Action"[63] they have taken as well. Similarly, Singapore's PDPC publish its "Enforcement Decisions"[64].

2.7.1 Penalties from the Data Protection Commissioner

Any person who, without reasonable excuse, fails to comply with an enforcement notice commits an offence and is liable on conviction to a fine of up to five million shillings (approx.US$ 45,000 at time of writing) or to imprisonment for up to two years, or to both. If there is not a clear penalty defined for a specific offence, on conviction the person will be liable to a fine not exceeding three million shillings (US$ 27,000 at time of writing) or to imprisonment for a term not exceeding ten years, or to both. In addition, the Court may order the forfeiture of any equipment or article used or connected in any way with the commission of the offence; or order or prohibit the doing of any act to stop a continuing contravention.

The value of these fines in Kenyan terms might appear substantial, but when compared to both the GDPR and CCPA, they are a relatively small amount and may not be a sufficient deterrent to ensure that data controllers and processors invest in improving their data protection. A simple cost benefit analysis by an organisation might lead to a decision to pay the fine, rather than invest in the necessary controls.

DAPA appears to infer that fines will be on a per incident basis, so the same maximum penalty would be applied if the enforcement notice penalty were to be applied to a company managing 100 or one million data subjects. The interpretation of a fine per violation under the CCPA is currently under review. It is clear that US$2,500 per violation is not a serious penalty if the data of one million customers was breached (although civil damages per data subject would definitely have an impact) – if the Kenyan Data Protection Commissioner applied an interpretation that the fine was per customer, and not per event then the 5 million KES limit would become a healthy deterrent, but when coupled with the one per centum of the previous year's turnover, it does not appear that this is the current expectation. As with the CCPA, the actual implications will become clear once the first cases are prosecuted, and subsequently appealed.

The GDPR has taken the stance to allow scope for a much higher penalty to be applied, although the intention is to create a clear deterrent than seek out and punish at whim. The GDPR takes the approach that rather than starting with a percentage that reaches a cap, they apply an amount that can increase for larger companies as a percentage of global turnover of the group of the company – not just the subsidiary that might have performed the breach in a country. The aim of gaining maximum compliance from people looking after their citizen's data.

- 2% of global annual turnover or €10 million (1,330M KES), whichever is higher; or
- 4% of global annual turnover or €20 million (2,660M KES), whichever is higher for breaches of data subjects' rights and freedoms.
- US$2,500 for each violation.
- US $7,500 for each intentional violation.
- DAPA gives an offender a minimum of 21 days to remediate any failings identified, however the CCPA gives a maximum of 30 days.

Table 1: Fines and penalties

62 *https://ico.org.uk/for-organisations/the-guide-to-nis/enforcement/*

63 *https://ico.org.uk/action-weve-taken/enforcement/*

64 *https://www.pdpc.gov.sg/Enforcement-Decisions*

	Turnover	5,000,000 KES	5,000,000,000 KES	70,000,000,000 KES
DAPA	Lower of 1% or 5M KES	50,000 KES	5,000,000 KES	5,000,000 KES
GDPR	Higher of 2% or1,330M KES	1,330,000,000 KES	1,330,000,000 KES	1,400,000,000 KES

Although the GDPR fines might seem excessive in relation to turnover, they set the sanctions in the most extreme cases.

Where an organisation does not attempt to protect the data subjects - if the organisation is small enough, it can be easily closed down. And if it is large enough, the penalties applied are sufficient to make them reconsider their actions. It is worth noting that the PDPC financial penalties will be increased in February 2022 to up to S$1 million or 10% of the organisation's annual turnover in Singapore, whichever is higher. This is an increase from the previous maximum of S$1 million. This change is more in line with the GDPR's.

In the recently issued "*The Data Protection (Compliance and Enforcement) Regulations, 2021*"[65], the Data Protection Commissioner has provided more information on the process of administering and overseeing the complaints process, investigations, any potential mediation or conciliation and subsequent enforcement provisions such as enforcement notices or the application of penalties.

POLICY RECOMMENDATION 42

Given the fact the lower limits are applied to the fines available, it is possible that a rapidly growing and successful organisation could have an extremely low fine – irrespective of the number of customers that the company may have been affected. Additionally, for large organisations the fine might be a lower cost than the cost of implementing a proper solution in the short to medium term. Only the threat of a prison sentence could be a sufficient deterrent, but since a legal entity/person is the recipient of the penalty rather than a natural person, this can also be a complex process.

Contrast this approach to the UK fine of Marriott International Inc. for £18.4million[66] (approx. 3Bn KES) for failing to keep secure the personal data of 339 million customers worldwide.

It is recommended that the Data Protection Commissioner reviews interpretation of the fines that can be applied, to ascertain if this fine limit could be set per data subject, rather than per offence of an organisation. This approach would create a stronger enforcement option and act as a clear deterrent as the amount applied could be increased for repeat offences.

In Section 9 (1) (b), of the "The Data Protection (Compliance and Enforcement) Regulations, 2021"[67], the Data Protection Commissioner has identified that a single complaint might be consolidated, or treated as a test complaint – this separation, and application of a Penalty notice in Section 13 (3) (b), provides a foundation for a "per complaint" level application of the penalties. This view is further enhanced in section 19 (3) – where the regulation states, "The administrative fine levied under paragraph (2) (c) shall consider each individual case and have due regard to factors or reasons outlined under section 62 (2) of the Act."

65 *https://www.odpc.go.ke/wp-content/uploads/2021/04/THE-DATA-PROTECTION-COMPLIANCE-AND-ENFORCEMENT-REGULATIONS-2021.pdf*

66 *https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf*

67 *https://www.odpc.go.ke/wp-content/uploads/2021/04/THE-DATA-PROTECTION-COMPLIANCE-AND-ENFORCEMENT-REGULATIONS-2021.pdf*

DAPA

23, 56, 57, 58, 59, 61, 62, 63, 64

The Data Commissioner may carry out **periodical audits** of the processes and systems of the data controllers or data processors to ensure compliance with this Act.

A data **subject** who is **aggrieved** by a decision of any person under this Act may **lodge a complaint** with the Data Commissioner in accordance with this Act. A person who intends to lodge a complaint under this Act shall do so **orally** or in **writing**. Where a complaint is made orally, the Data Commissioner shall cause the complaint to be recorded in writing and the complaint shall be dealt with in accordance with such procedures as the Data Commissioner may prescribe. A complaint lodged shall contain **such particulars as** the Data Commissioner **may prescribe**. A complaint made to the Data Commissioner shall be **investigated** and **concluded** within **90 days**.

The **Data Commissioner** may, for the purpose of the investigation of a complaint, **order** any person to: **attend** at a specified time and place for the purpose of being **examined orally** in relation to the complaint; **produce** such **book**, **document**, **record** or **article** as may be required with respect to any matter **relevant to** the **investigation**, which the person is **not prevented** by any **other enactment** from disclosing; or **furnish a statement** in writing made under oath or on affirmation setting out all information which may be required under the notice. Where material to which an investigation relates consists of information stored in any mechanical or electronic device, the Data Commissioner may require the person named to produce or give access to it in a form in which it can be taken away and in which it is visible and legible. A person who, without reasonable excuse, **fails or refuses to comply** with a notice, or who **furnishes** to the Data Commissioner any information which the person knows to be **false or misleading**, **commits an offence**.

Where the Data Commissioner is **satisfied** that a person has **failed**, or is **failing**, **to comply** with any provision of this Act, the **Data Commissioner** may **serve** an **enforcement notice** on that person requiring that person to **take** such **steps** and **within** such **period** as may be specified in the notice. An enforcement notice served shall: specify the provision of this Act which has been, is being, or is likely to be, contravened; **specify** the **measures** that shall be taken to remedy or eliminate the situation which makes it likely that a contravention will arise; specify a **period** which shall **not** be **less** than **21 days** within which those measures shall be implemented; and state any **right** of **appeal**. Any person who, without reasonable excuse, **fails to comply** with an enforcement notice **commits an offence** and is liable on conviction to a fine **not exceeding** KShs **five million** or to **imprisonment** for a **term not exceeding two years**, or to both.

For the purpose of gathering information or for any investigation under this Act, the Data Commissioner may **seek** the **assistance** of such **person** or **authority** as they **deem fit** and as is **reasonably necessary** to assist the Data Commissioner in the discharge of their functions.

The Data Commissioner, upon obtaining a **warrant** from a Court, may **enter and search** any premises for the purpose of discharging any function or exercising any power under this Act.

A **person** who, in relation to the exercise of a power : **obstructs** or **impedes** the Data Commissioner in the exercise of their powers; **fails** to **provide assistance** or **information** requested by the Data Commissioner; **refuses to allow** the Data Commissioner to **enter any premises** or to take any person with them in the exercise of their functions; **gives** to the Data Commissioner any **information** which is **false or misleading** in any material aspect, **commits** an **offence** and is liable on conviction to a **fine not exceeding Kshs five million** or to **imprisonment** for a term **not exceeding two years**, or to **both**.

If the Data Commissioner is satisfied that a **person** has **failed** or is **failing**, the Data Commissioner may issue a **penalty notice** requiring the person to pay to the Office of the Data Commissioner **an amount specified** in the notice. In deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Data Commissioner shall, so far as relevant, **have regard**: to the **nature**, **gravity** and **duration** of the **failure**; to the **intentional** or **negligent** character of the failure; to any **action** taken by the data controller or data processor **to mitigate** the damage or distress suffered by data subjects; to the **degree of responsibility** of the data controller or data processor, taking into account **technical** and **organisational measures**; to any relevant **previous failures** by the data controller or data processor; to the **degree of co-operation** with the Data Commissioner, in order to remedy the failure and mitigate the possible adverse effects of the failure; to the **categories** of personal data **affected** by the failure; to the **manner** in which the **infringement became known** to the Data Commissioner, **including whether**, and if so to what extent, the data controller or data processor **notified** the Data Commissioner of the failure; to the **extent** to which the data controller or data processor has **complied** with **previous** enforcement **notices** or penalty notices; to **adherence** to **approved codes** of conduct or certification mechanisms; to any other aggravating or mitigating factor applicable to the case, **including financial benefits gained**, or **losses avoided**, as a result of the failure (whether directly or indirectly); to whether the penalty would be **effective**, **proportionate** and **dissuasive**.

In relation to an infringement of a provision of this Act, the **maximum amount** of the penalty that may be imposed by the Data Commissioner in a penalty notice is **up to five million shillings**, or in the case of an undertaking, **up to one percent of its annual turnover of the preceding financial year**, whichever is lower.

A person against whom any administrative action is taken by the Data Commissioner, including in enforcement and penalty notices, **may appeal to the High Court**.

GDPR	CCPA
Article 82 (1), 83	**150, 155**
Liability and consequences of **non-compliance**: ▪ Data subjects have the right to bring an action against processors and **claim damages** for **"material or immaterial damage"** suffered as a result of an infringement of the processor obligations under the GDPR. ▪ Processors are only **liable for damage caused by processing in failure of their contractual obligations.**	A business shall be in **violation** of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be subject to an **injunction** and liable for a civil penalty.

2.7.2 Civil Remedies

DAPA confirms that a data subject who suffers damage, either financial or distress, is entitled to compensation from the data controller or the data processor. The controller will be liable for damage caused by the processing, and a processor will only be liable for damage if they have not complied with the regulations, or they have acted contrarily to the data controller's instructions. If either party can prove that they are in no way responsible for the event, then they will not be held liable. The GDPR has established that an organisation that has, as its statutory objective, the protection of data subject's rights can represent a data subject. This allows for organisations to act as data subject champions.

The CCPA only allows this remedy if non-encrypted or non-redacted personal information is accessed due to violation of the business' security obligations. The business is provided 30 days to "cure" the violation – and if this is achieved, no further action can be pursued.

If a data subject has experienced actual pecuniary damage, then no notice is required for an action to take place. The amount of damages is established by statute. Damages could be in an amount not less than $100 and not greater than $750 per consumer, per incident, or actual damages, whichever is greater. As an example, if the data of one million Californian residents is breached, the minimum damages would be $100 million.

POLICY RECOMMENDATION 44

Currently, there is no guidance on the minimum or maximum damages that can be applied for civil remedies. If the Data Protection Commissioner adopts an approach similar to that of the CCPA where there is a minimum remedy and a maximum that can scale to the full extent of actual damages, a data controller (or processor) will need to consider the costs of implementing security measures against the threat of strong civil remedies.

DAPA
65
A **person** who **suffers damage** by reason of a contravention of a requirement of this Act is **entitled to compensation** for that damage **from the data controller or the data processor**. A data **controller** involved in processing personal data is **liable for any damage** caused by the processing; and a data **processor** involved in processing personal data is liable for damage caused by the processing **only if** the processor: has **not complied** with an obligation under the Act specifically **directed at data processors**; or has **acted outside**, or **contrary to**, the **data controller's** lawful **instructions**. A data controller or data processor is **not liable** in the manner specified if the data controller or data processor **proves** that **they** are **not in any way responsible** for the event giving rise to the damage. In this section, "damage" **includes financial loss** and damage not involving financial loss, **including distress**.

GDPR	CCPA
Article 82	**150**
Any violation of the GDPR can trigger the claim for judicial remedies. Data subjects can claim both **material and non-material damages**. Member States are to provide for the possibility for data subjects to give a mandate for representation to a non-for-profit association, association or organisation that has as its statutory objective the protection of data subject rights. The GDPR does not provide any figure for potential damages.	This remedy is only allowed when non-encrypted or non-redacted personal information is subject to an unauthorised access and exfiltration, theft, or disclosure as a result of the business's violation of security obligations. Prior to initiating any action against a business for statutory damages on an individual or class-wide basis, businesses are provided 30 days' written notice including a reference to the alleged violations. If the violation is "cured" within 30 days and no further violation is claimed, no action is initiated. The CCPA further states that "no notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement." The amount of damages is established by Statute. **Damages** could be in a**n amount not less than $100 and not greater than $750** per consumer per incident or actual damages, whichever is greater.

2.7.3 Supervisory Authority

Legislation includes creation of the "Office of Data Protection Commissioner." This includes the rights of that office, and the process of appointing the Data Protection Commissioner - with Immaculate Kassait being sworn in as the country's first ever Data Protection Commissioner on 16th November 2020.

The Office will establish and maintain a register of data controllers and data processors and oversee the implementation of the Act (DAPA) among data controllers and data processors. The Office is also charged with promoting awareness of the Act among the general public; receiving and investigating complaints for data subjects; as well as promoting international co-operation. At least two fees are charged at submission of the application to register. One to cover the size of the organisation, then another based on their Annual Turnover. There is a third fee if an organisation meets the "special category" for Personal Data Intensive sectors – likely to impact those in Financial Services.

The GDPR does not regulate how data protection authorities are funded, this being left to Member States to decide. The UK's ICO charges a registration fee ranging from 6,000 KES to 440,000 KES (£40 to £2,900) depending on the size of an organisation.

The GDPR states that data protection authorities must act in "complete independence when performing their tasks."

POLICY RECOMMENDATION 45

As the duties of the Data Protection Commissioner include working with other countries, making Kenyan organisations aware of the legislation of other countries would be seen as a strong lever when seeking enforcement of international breaches. If a Kenyan organisation is based online or deals with tourists or international business travellers, it is likely that these organisations will be dealing with personal data that is the subject of external legislation. By looking to harmonise guidance with this other legislation, it will also reduce the burden of activity for a business as it would know the steps it needs to take to protect the data of Kenyan data subjects as of high enough a standard to meet the challenges of these other pieces of legislation.

DAPA
5, 8 (b, c, d, e, f, g, i)
Legislation includes the creation of the "Office of Data Protection Commissioner". This includes the rights of that office, and the process of appointing the Data Commissioner with Immaculate Kassait being sworn in as the country's first ever Data Commissioner on 16th November 2020. The Office will **establish** and **maintain** a register of data controllers and data processors; exercise **oversight**; promote **self-regulation; conduct an assessment** for the purpose of ascertaining whether information is processed according to the act; receive and **investigate** any **complaint;** take such measures as may be necessary to **bring the provisions** of this Act **to the** knowledge of the **general public**; and promote **international cooperation.**

GDPR	CCPA
Article 4 (21, 22), 40, 41,42, 43, 51, 52, 53. 54	**150, 155, 185**
Data protection authorities have the task to **promote awareness and produce guidance** on the GDPR. Data protection authorities have **investigatory powers** which include to: "conduct data protection audits, access all personal data necessary for the performance of its tasks, obtain access to any premises of the data controller and processor, including equipment and means." Data protection authorities have **corrective powers** which include: "issuing warnings, reprimands, to order the controller and processor to comply, order the controller to communicate a data breach to the data subject, impose a ban on processing, order the rectification or erasure of data, suspend the transfer of data and impose administrative fines." The GDPR does not regulate how data protection authorities are funded, this being left to the Member States to decide. The GDPR states that data protection authorities must act in "**complete independence when performing their tasks**," which also means that they must be free from financial control by having a separate and dedicated budget.	The Attorney General of California is expected to create regulations "on, but not limited to," specific areas of the CCPA. The Attorney General has the power to **assess a violation** of the CCPA. The CCPA does not specify which activities are included in this assessment. The Attorney General has the power to assess alleged violations of the CCPA and to bring action before the court for civil penalties, which include **monetary penalties and injunctions**. The monetary penalties collected through civil actions under the CCPA form the **Consumer Privacy Fund**, which funds the activities of the Attorney General in this sector. The Attorney General has the power to **independently start investigations** and actions against alleged non-compliance from businesses.

2.7.4 Additional duties

2.7.4.1 Applying to be a data controller or processor

Under DAPA a data controller or data processor is required to register, and they shall apply with the Data Protection Commissioner. When they register, they will be required to provide the following information:

- a description of the personal data to be processed;
- a description of the purpose for which the data is to be processed;
- the category of data subjects;
- contact details of the data controller or data processor;
- a general description of the risks, safeguards, security measures and mechanisms to protect the data;
- any measures to indemnify the data subject from unlawful use of data by the data processor or data controller;
- and any other details as may be prescribed by the Data Protection Commissioner.

Although there is no specific requirement to appoint a data protection officer, it is assumed that these contact details will be provided when the contact details of the data controller or processor are provided. It is worth noting that providing false or misleading information as part of this application is an offence, and these details should be updated as there is a change; failing to do so is an offence. In "*The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021*"[68], the Data Protection Commissioner confirmed that fees would be applied for registration, and that applications for registration will be submitted through the Data Protection Commissioner's Office website. The registration will be renewed every year, with the renewal application being submitted 30 days before the expiry of the certificate of registration, and the renewal is also subject to a fee.

The legislation also confirms that companies which have an annual turnover of less than 5 million KES and have less than ten employees are exempt from mandatory registration. There are however, thresholds for mandatory registration, which include those organisations: operating credit bureaus; hospitality industry firms; faith based or religious institutions; and provision of financial services.

The fees proposed in Schedule 2 are outlined below, and fees are cumulative, where applicable, from Stage 1 to 3:

Further fees are provided to cover other costs, including certification, but some of these fees will be subject to the actual task that needs to be undertaken.

In Section 14 of the Regulation, it is also clarified that any changes must be notified to the Data Protection Commissioner within 14 days of the change.

POLICY RECOMMENDATION 46

DAPA registration is not free– A small company will face a charge of at least KES 4,000 and a large organisation a fee of KES 40,000. In the UK, the fee ranges from KES 6,000 to KES 440,000 (£40 to £2,900) depending on the size of the organisation. There is also a fine for failing to register. Guidance is provided to help identify if an organisation must register with a simple self-assessment at the "Data Protection Fee"[69] page. The fees are also explained in the section "Data Protection Fee: A Guide for Data Controllers"[70]. Similar insight is recommended for implementation by the Office of the Data Protection Commissioner

Table 2: Proposed fees from Stages 1 to 3

		Registration fee	Renewal fee (after one year)
Stage 1: Base payment (all data controllers and processors unless exempted)	for organisation with 1-9 employees	KES 2,000	KES 1,000
	for organisation with 10-49 employees	KES 6,000	KES 5,000
	for organisation with 50-99 employees	KES 10,000	KES 8,000
	for organisation with more than 99 employees	KES 15,000	KES 12,000
Stage 2: Annual Turnover (excludes public authorities and charities)	if organisation has less than KES 2,000,000 annual turnover	KES 2,000	KES 1,000
	if organisation has KES 2,000,001 -5,000,000 annual turnover	KES 6,000	KES 5,000
	if organisation has KES 5,000,001-10,000,000 annual turnover	KES 10,000	KES 8,000
	if organisation has KES 10,000,001-50,000,000 annual turnover	KES 15,000	KES 12,000
	for organisation with more than KES 50,000,000 annual turnover	KES 25,000	KES 20,000
Stage 3: Special Category Data Charge (Personal Data intensive sectors)		KES 20,000	KES 20,000

68 *https://www.odpc.go.ke/wp-content/uploads/2021/04/Data-Protection-Registration-of-data-controllers-and-data-processor-Regulations.pdf*
69 *https://ico.org.uk/for-organisations/data-protection-fee/*
70 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-fee/*

POLICY RECOMMENDATION 47

Given the value of creating a structured set of documentation, the Data Protection Commissioner should consider using the Record of Processing Activities (ROPA) as defined under the GDPR to allow any investigation or assessment of a controller or processor to be against a structured and documented process. The expectation of a "Record of Processing Activities"[71] is provided by the UK ICO, a series of examples and expectations are laid out over a number of sections. The ROPA would be an extension of the Data Protection policy identified in Section 22 - Data Protection Policy of the recently released "Data Protection (General) Regulations 2021"[72]

DAPA

18, 19

A data controller or data processor **required to register** shall apply to the Data Commissioner.

An application shall provide the following particulars: a **description** of the personal data to be processed by the data controller or data processor; a description of the **purpose** for which the personal data is to be processed; the **category** of **data** subjects, to which the personal data relates; **contact details** of the data controller or data processor; a **general description** of **the risks**, **safeguards**, **security measures** and **mechanisms** to ensure the protection of personal data; any **measures** to **indemnify** the data subject from unlawful use of data by the data processor or data controller; and any other details as may be prescribed by the Data Commissioner.

A data controller or data processor who knowingly supplies any false or misleading detail under sub-section commits an offence.

The Data Commissioner shall issue a certificate of registration where a data controller or data processor meets the requirements for registration.

A data controller or data processor shall **notify** the Data Commissioner of a **change** in any particulars outlined above.

A data controller or data processor who **fails** to **comply** with the provisions of this section **commits an offence**.

2.7.4.2 Appointing a Data Protection Officer

Under DAPA, a Data Protection Officer may be appointed – this can be a standard employee that also performs other tasks as long as they do not result in a conflict of interest. The data protection officer needs to have relevant academic or professional qualifications that might include knowledge and technical skills that helps them in their role. If a data protection officer is appointed, their contact details should be made available on the company website, and shared with the Data Protection Commissioner, so it is also made available on the official website.

Amongst the key tasks of the Data Protection Officer include providing advice to the company and employees of the requirements of the law; ensuring compliance with the law; and ensuring staff involved in data processing are well aware of their duties. They also advise on the data protection impact assessment.

71 *https://ico.org.uk/for-organisations/accountability-framework/records-of-processing-and-lawful-basis/record-of-processing-activities-ropa/*
72 *https://www.odpc.go.ke/wp-content/uploads/2021/04/Data-Protection-General-regulations.pdf*

The GDPR insists upon a Data Protection Officer, when the organisation is processing data on a large scale.

Although appointment of a data protection officer (DPO) is not mandatory for DAPA, the expectation of the GDPR was to put the protection of data subjects at the forefront of a company's Executives, as evidenced in the fines possible and the insistence of have a Data Processing Officer when operating at scale. It is important that the Data Protection Commissioner highlights the importance of the role, and it is critical that this role is taken up by a senior person within an organisation so as to ensure that the correct priority is given to their tasks.

The CCPA does not consider the role of a Data Protection officer.

POLICY RECOMMENDATION 48

Although the appointment of a data protection officer (DPO) is not mandatory under DAPA. To drive the importance of the Act it is important that the Data Protection Commissioner highlights the importance of the role, and the seniority of the person in an organisation to ensure that the correct priority is given to their tasks. The UK ICO provides further guidance in their section on "Data Protection Officers"[73]. Singapore's PDPC also recognises the need for Data Protection Officers, and provide specific guidance in their overview for "Data Protection Officers"[74] – they also provide clear guidance on how an outsource "Data Protection as a Service".

DAPA

24 (1, 2)

A data controller or data processor may **designate or appoint** a **data protection officer**. A data protection officer **may** be a staff member of the data controller or data processor and may fulfil **other tasks** and duties provided that any such tasks and duties **do not result in a conflict of interest**.

A person may be designated or appointed as a data protection officer, if that person **has relevant academic** or **professional** qualifications which may include **knowledge** and **technical skills** in matters relating to data protection.

A data controller or data processor shall **publish** the **contact details** of the data protection officer **on the website** and **communicate** them to the Data Commissioner who shall ensure that the **same information** is available on the **official website**.

A data protection officer shall: **advise** the data **controller** or data **processor and** their **employees** on data processing requirements provided under this Act or any other written law; **ensure** on behalf of the data controller or data processor that this **Act is complied with**; facilitate **capacity building of staff** involved in data processing operations; provide **advice** on **data protection impact assessment**.

GDPR

Article 30(1-5)

Appointing a DPO (Data Protection Officer): Processors must designate a data protection officer when required by the law, including where the processor processes personal data on a large scale.

73 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/*

74 *https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/business-owner/data-protection-officers*

2.8 Transferring Data Outside Kenya: Data Sovereignty

A clause much feared in Kenya, is whether there is the option to host services outside Kenya. The preferred approach is always to host within Kenya, but the availability of Data Centres will make this challenging at least in the short term.

DAPA does allow for normal personal data outside Kenya – only when there is proof of adequate data protection safeguards or consent from the data subject. The proof needs to be provided to the Data Protection Commissioner, to ensure sufficient security and protection – the countries to be included must have commensurate data protection laws. Taking as an example on 16th July 2020, the Court of Justice of the European Union (ECJ) in its Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (otherwise known as "Schrems II case") cast doubt over the protection of the data – as the data could be accessed by U.S. intelligence agencies in violation of the GDPR.

Sensitive personal data however can only be processed when both consent and appropriate safeguards are confirmed. The Data Protection Commissioner can also insist that these safeguards be demonstrated, or that there be existence of compelling legitimate interests. It is within the control of the Data Protection Commissioner to prohibit, suspend or apply further conditions. Financial information, such as balances or income, and KYC data, such as identification documents, will fall into this category of sensitive personal data.

In the "*Data Protection (General) Regulations 2021*"[75], the Data Protection Commissioner provides clarity on hosting in Kenya as mandatory for those providing a "Public Good", which is defined, and include "managing any electronic payments systems licensed under the National Payment Systems Act 2011". The provision of banking and financial services, payment and settlements systems and instruments are defined as part of protected computer systems in terms of section 20 of the Computer Misuse and Cybercrime Act, 2018 and therefore subject to hosting in Kenya.

For non-Kenyan organisations in Section 25 of the recently released "*Data Protection (General) Regulations 2021*", the Data Protection Commissioner identifies which systems MUST be hosted in Kenya at this time. None of these categories are likely to apply to non-Kenyan organisations. Therefore, other than a later mandate from the Cabinet Secretary that requires these organisations must host in Kenya, non-Kenyan organisations that clarify the data they are capturing, and ensure they have the appropriate consents are not obliged to host in Kenya. These organisations should however, still safeguard the data of Kenyan data subjects, in line with the requirements of DAPA. The CCPA provides clear guidance on when the regulation will apply to entities "doing business in California" – those defined as making profit or pecuniary gain under the California Franchise Tax board. But there are also thresholds to determine the businesses covered. Those with revenues over $25M, managing the data of more than 50,000 consumers, households or devices, or those who derive more than 50% of revenue from selling the information. Similar guidance for these entities will ensure appropriate protection of the data of Kenyan data subjects.

The Cabinet Secretary also can insist on processing through a server or a data centre located in Kenya based on grounds of strategic/national interests of the state or protection of revenue.

POLICY RECOMMENDATION 49

Similar to the EU court cases now challenging the use of Data Centres in the US, early clarification by the Data Protection Commissioner on whether an equivalent Schrems II case would be seen as valid in Kenya or not, will assist all parties in making a clear risk assessment on their current approach to hosting. If countries with sufficient data protection adequacy such as Europe – were also clearly "identified" then data controllers could ensure their focus was on the technical and operational processes.

The UK's ICO has published guidance on "International Data Transfers"[76], given the changes required post-Brexit, an adequacy ruling is still being assessed with the draft decisions – this approach could be insightful for the Data Protection Commissioner when considering the assessment of hosting in other territories. In their "Advisory Guidelines on Key Concepts in the Personal Data Protection Act"[77] Singapore's PDPC provides examples of hosting of data outside Singapore in sections 6.22 to 6.23 to ensure that data intermediaries apply equivalent controls.

75 *https://www.odpc.go.ke/wp-content/uploads/2021/04/Data-Protection-General-regulations.pdf*

76 *https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/international-data-transfers/*

77 *https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en*

POLICY RECOMMENDATION 50

For non-Kenyan organisations, further clarity from the Data Protection Commissioner on when they are expected to host in Kenya will ensure appropriate protection of Kenyan citizens.

DAPA

48, 49, 50

Data will **not** be **transferred outside Kenya**, **unless** there is **proof of adequate data protection safeguards or consent** from the data subject.

A data controller or data processor may transfer personal data to another country only where the data controller or data processor has given **proof** to the Data Commissioner on the **appropriate safeguards** with respect to the s**ecurity and protection** of the personal data; the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including **jurisdictions** with **commensurate data protection laws**;

The **transfer** is **necessary**: for the **performance** of a **contract** between the data subject and the data controller or data processor or implementation of pre-contractual measures taken at the data subject's request; for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person; for any **matter of public interest**; for the establishment, exercise or defence of a **legal claim**; in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or for the purpose of **compelling legitimate interests** pursued by the data controller or data processor which are **not overridden by** the **interests**, **rights** and **freedoms** of the data subjects.

The **processing** of **sensitive personal** data out of Kenya shall only be effected upon **obtaining consent** of a data subject **and** on obtaining **confirmation of appropriate safeguards**. The **Data Commissioner may request** a person who transfers data to another country to **demonstrate** the effectiveness of the **security safeguards** or the existence of **compelling legitimate interests**. The Data Commissioner **may**, in order to protect the rights and fundamental freedoms of data subjects, **prohibit**, **suspend** or **subject the transfer** to such **conditions** as may be determined. The Cabinet Secretary may prescribe, based on **grounds of strategic interests of the state** or **protection of revenue**, certain nature of processing that shall **only be effected** through a server or a data centre **located in Kenya**.

GDPR

Article 44

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

2.9 Data Protection Impact Assessment

DAPA identifies the need for a data controller or data processor to carry out a data protection impact assessment – before they start processing. This assessment should include a systematic description of the planned operations and the purposes of the processing. It should capture what legitimate interests are being pursued by the data controller

or data processor and then assess if the collection is necessary and proportional to the service being offered. Once that is done, the data controller or processor needs to assess the risks to the rights and freedoms of the data subjects.

Once the risks are identified, the data controller or processor need to address these risks with appropriate safeguards, security measures and mechanisms to ensure the protection of personal data. If the data controller or data processor believes that the processing would result in a high risk to the rights and freedoms of a data subject, they should consult the Data Protection Commissioner prior to commencement of any processing. The data impact assessment reports should be submitted to the Data Protection Commissioner 60 days prior to processing of data.

The GDPR also mandates the use of a Data Protection Impact Assessment when there is a high risk to the rights of freedoms of Individuals, in their guidance on "*When is a Data Protection Impact Assessment (DPIA) Required?*"[78] they also provide example scenarios where the DPIA is and is not required.

The DPIA is also not seen as a one-off exercise to capture the initial view, it should be viewed a living document – meaning it should be revisited and if necessary, updated on a regular basis. The Commissioner's Office has provided a *Guidance Note on Data Protection Impact Assessment*[79] in which they provide further clarity on the expectations of an Impact Assessment that is to be submitted to the Office of the Data Protection Commissioner before processing data:

A Data Protection Impact Assessment (DPIA) is designed to identify risks arising out of the processing of personal data and to minimise these risks. Performing a DPIA should help to identify and manage these risks. It should allow a company to comply with legal and policy requirements and ensure that data controllers and data processors implement appropriate technical and organisational measures to minimize negative impacts on the privacy of data subjects. This assessment should also provide the input to the design for privacy protection (necessary to meet privacy by design or default obligations).

The submission to the Office of the Data Protection Commissioner, allows the Office to see that a data controller or processor have appropriate measures in place to ensure compliance with the provisions of the Act. The office will be looking for:

a. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller or data processor;

b. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c. an assessment of the risks to the rights and freedoms of data subjects."

Not everyone is expected to complete and submit a DPIA, but they must complete one if it is "likely to result in a high risk to the rights and freedoms of data subjects". The rights and freedoms are primarily focussed on the rights to data protection and data privacy but can extend to cover the rights as enumerated in Chapter Four of the Constitution of Kenya 2010. As companies and processes evolve the data controller or processor must continuously assess the risks created by their

DPIA required	DPIA Not required
A bank screening its customers against a credit reference database; a hospital about to implement a new health information database with patients' health data;a bus operator about to implement on-board cameras to monitor drivers' and passengers' behaviour.	A community doctor processing personal data of his patients. In that case, there is no need for a DPIA since the processing by the community doctors is not done on a large scale in cases where the number of patients is limited.

78 *https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_en*

79 https://www.odpc.go.ke/download/odpc-protection/?wpdmdl=7628

processing activities. A DPIA should be assessed against the following eight criteria:

1. Automated decision making with legal or similar significant effect. Profiling and predicting of individuals – a credit assessment or financial crime assessment will definitely fall under this category.

2. Systematic monitoring: where a data controller or processor is likely to observe, monitor or control data subjects, where the data subject may not be aware of who is collecting their data – this is highly likely in a financial crime assessment, where Dark Web data may be used to check a user. It may be impossible for a data subject to avoid being subject to such processing in public (or publicly accessible) space(s) so care should be taken to ensure that a subjects rights are protected.

3. Sensitive personal data or matters of a private nature

4. Data processed on large volumes or large scales

    a. The number of data subjects concerned;

    b. The volume of data and/or the range of different data items being processed;

    c. The duration, or permanence, of the data processing activity;

    d. The geographical extent of the processing activity.

5. Matching or combining datasets: personal data originating from two or more data processing operations performed for different purposes and/ or by different data controllers in a way that would exceed the reasonable expectations of the data subject.

6. Data concerning vulnerable data subjects: individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children.

7. Innovative use or applying new technological or organisational solutions: This can include novel forms of data collection and usage, possibly with a high risk to data subjects' rights and freedoms. Which is likely to affect all fintechs.

8. When the processing itself prevents data subjects from exercising a right. For example refusing data subjects' access to a service or entry into a contract.

If a data controller or data processor does not believe a DPIA is required, they must seek concurrence from the Office or the Data Protection Commissioner and should justify the reasons the data controller and/ or data processor does not believe a DPIA is necessary.

Once completed the DPIA must be submitted 60 days prior to the commencement of processing, but for those already processing data, the DPIA should still be submitted as the DPIA will be taken into consideration in the event of a breach, or other factor likely to attract an administrative fine/penalty. Although no timeline is provided, the expectation is likely to be as quickly as possible – as failure to do so will risk an administrative fine or penalty. It is clear that failure to complete a DPIA will lead to activity being deemed illegal. As evidenced in the case against the National Integrated Identity Management System (NIIMS) popularly known as *Huduma Namba* which had begun in November 2020. The *court found the rollout had been illegal*[80] as it had not been preceded by a data protection impact assessment in line with the Act

It is possible for a data controller or processor to use a single assessment to address a set of similar processing operations. A joint DPIA should set out which party is responsible for the various measures designed to address the risks. Each data controller and/or data processors should express its needs and share useful information without either party compromising secrets. If the processing implementation has changed and it is likely to result in a high risk, a DPIA should be completed

A DPIA is required after a change of the risks or if personal data is being used for a different purpose. The organisational or societal context should also be considered – for example when the effects of an automated decision becomes more significant or new categories of data subjects become vulnerable to discrimination i.e. extending the product to children

80 *http://kenyalaw.org/caselaw/cases/view/220495/*

The DPIA should be started as early as is practicable in the design of the processing operation even if some of the processing operations are still unknown. This will assist in the implementation of data protection by default / design.

(i) The DPIA must address the following matters: the amount of personal data collected;

(ii) the extent of processing of the personal data;

(iii) the period and method of storage of the personal data and its accessibility;

(iv) the state of technological development available for processing;

(v) the special risks that exist in the processing of the data;

(vi) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller or data processor;

(vii) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(viii) an assessment of the risks to the rights and freedoms of data subjects; and

(ix) the measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act, taking into account the rights, and legitimate interests of data subjects and other persons concerned (section 31(1){d).

The Office of the data protection commissioner also provides a sample DPIA template – the expectation that companies will complete this as part of their submission.

In the *recent ruling on the rollout of National Integrated Identity Management System (NIIMS)*[81] popularly known as *Huduma Namba*, which the Attorney General has vowed to appeal, the court found the rollout had been illegal as it had not been preceded by a data protection impact assessment in line with the Act. Importantly, the court stated:

> *"Reading the preamble to the Act [DAPA] together with Section 3 thereof on the Act's object and purpose, it is clear that the Act was intended to be retrospective to such an extent or to such a time as to cover any action taken by the state or any other entity or person that may be deemed to affect, in one way or the other, the right to privacy under Article 31 (c) and (d) of the Constitution. Needless to say, the need to protect the constitutional right to privacy did not arise with the enactment of the Data Protection Act; the right accrued from the moment the Constitution was promulgated."*

The GDPR also states that the supervisory authorities have to establish and publish a list of processing operations which always require a data protection impact assessment in their jurisdiction (positive list). They are also free to publish a list of processing activities which specifically do not require a privacy impact assessment (negative list).

POLICY RECOMMENDATION 51

Although the timeline for submission of a data processing impact assessment is clear (at least 60 days before the starting of processing), there is no clarity on the timeline for completing this for existing businesses, or the impact of the same where these assessments are not sufficient. When the timeline for registration is clear, this will ensure that data controllers and processors complete and submit the DPIA within sufficient time for approval by the Data Protection Commissioner.

In the definition of DAPA, a number of the tasks identified fit under the Record of processing activities (ROPA) as well as a DPIA. The UK ICO provides a thorough overview of the systematic description and purposes of the processing under the "Record of Processing Activities (ROPA)"[82], and then provides an overview of the Impact Assessment in their section "What is a DPIA?"[83].

After the risk assessment has been completed, the UK guidance does not require subsequent consultation with the ICO unless there is a residual high risk as clarified in their section "Do We Need to Consult the ICO?"[84]. Adoption of a similar approach will reduce the administrative burden on the Office of the Data Protection Commissioner.

81 *http://kenyalaw.org/caselaw/cases/view/220495/*

DAPA

31

Where a processing operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes, a data controller or data processor shall, prior to the processing, **carry out a data protection impact assessment**.

A data protection impact assessment shall include the following: a **systematic description** of the **envisaged processing** operations and the **purposes** of the processing, including, where applicable, the **legitimate interest pursued** by the data controller or data processor; an **assessment** of the **necessity** and **proportionality** of the processing operations in **relation** to the **purposes**; an assessment of the **risks** to the **rights and freedoms** of data subjects; the **measures** envisaged to address the **risks and the safeguards**, **security measures** and **mechanisms** to ensure the protection of personal data and to **demonstrate compliance** with this Act, taking into account the rights, and legitimate interests of data subjects and other persons concerned.

The data controller or data processor shall **consult** the Data Commissioner prior to the processing **if** a data protection **impact assessment** prepared under this section **indicates** that the processing of the data would result in a **high risk** to the rights and freedoms of a data subject.

For the purposes of this section, a "data protection impact assessment" means an assessment of the impact of the envisaged processing operations on the protection of personal data.

The **data impact assessment reports** shall be **submitted 60 days prior** to the **processing of data**.

The Data Commissioner shall **set out guidelines** for carrying out an impact assessment under this section.

GDPR

Article 35

Where a processing operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes, a data controller or data processor shall, prior to the processing, **carry out a data protection impact assessment**.

The controller shall **seek the advice** of the **data protection officer**, where designated.

A data protection impact assessment shall be required in the case of: a **systematic** and **extensive** evaluation of personal aspects which is based on **automated processing**, **including profiling**, and on which decisions are based that produce **legal effects** or **significantly affect** the natural person; **processing on a large scale** of **special categories** of data, or of relating to **criminal convictions** and **offences**; or a **systematic monitoring** of a **publicly accessible area** on a large scale.

The supervisory authority shall make **public** a **list of the kind of processing operations** which require a data protection impact assessment.

The supervisory authority **may** also establish and make public a list of the kind of processing operations **for** which **no data protection impact assessment** is required.

82 *https://ico.org.uk/for-organisations/accountability-framework/records-of-processing-and-lawful-basis/record-of-processing-activities-ropa/*

83 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/*

84 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/*

GDPR

Article 35

The assessment shall contain at least: a **systematic description** of the **envisaged processing** operations and the **purposes** of the processing, including, where applicable, the **legitimate interest pursued** by the data controller or data processor; an **assessment** of the **necessity** and **proportionality** of the processing operations in **relation** to the **purposes**; an assessment of the **risks** to the **rights and freedoms** of data subjects; the **measures** envisaged to address the **risks and the safeguards**, **security measures** and **mechanisms** to ensure the protection of personal data and to **demonstrate compliance** with this Act, taking into account the rights, and legitimate interests of data subjects and other persons concerned.

Where necessary, the controller shall **carry out a review** to assess if processing is performed in accordance with the data protection impact assessment at least **when there is a change of the risk represented** by processing operations.

Keep records of data processing activities: processors are required to maintain a record of data processing activities. The record should contain the categories of processing and any data transfers outside of the European Economic Area (EEA).

The need to keep records of data processing shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10

2.10 Responding to a security breach

DAPA, similar to the GDPR, also provides guidance on what an organisation should do once data is accessed or acquired by an unauthorised person, or a security breach has been identified. Unauthorised access is defined as where personal data has been accessed or acquired by an unauthorised person, and there is a real risk of harm to the data subject. This definition of unauthorised person can include employees who should not have access to data, gaining access to the data. Once the unauthorised access has been identified, a data controller shall notify the Data Protection Commissioner within seventy-two hours of becoming aware of such breach and communicate this to the data subject if they can be identified. Where a data processor becomes aware of a personal data breach, the data processor shall notify the data controller within 48 hours of becoming aware. The data controller may delay or restrict communication as necessary and proportionate for purposes of prevention, detection or investigation of an offence by the concerned relevant body.

It is important that the data subject has sufficient information to allow them to take protective measures. So, DAPA requires the processor or controller to provide a description of the data breach and the measures that the data controller or data processor intends to take or has taken to address the data breach. The controller should also provide recommendation on the measures to mitigate the adverse effects of the security compromise; where applicable, the identity of the unauthorised person who may have accessed or acquired the personal data; and the name and contact details of the data protection officer or other contact point from whom more information could be obtained.

The Data Protection Commissioner can apply to a court for a preservation order for the preservation of personal data including traffic data where there is reasonable ground to believe that the data is vulnerable to loss or modification (i.e. further breaches). It is important that a data controller and processor understand they risk committing an offence if the controller discloses personal data in a manner that is incompatible with the purpose for which such data has been collected commits an offence, or if the processor processes without the prior authority of the data controller.

A person commits an offence if they obtain access to personal data without prior authority of the data controller or data processor or discloses personal data to third party. A person who offers personal data obtained in a breach for sale or indicates that it might be

for sale commits an offence. An advertisement indicating that personal data is or may be for sale constitutes an offer to sell the personal data.

POLICY RECOMMENDATION 52

The response times identified by DAPA are in line with global best practices – and ensure that a data controller or processor responds quickly to minimise the potential damage to a data subject whose data is accessed. In the creation of further guidance, the Data Protection Commissioner can consider the approach taken by the UK ICO on "Unauthorised Access"[85], where they provide a practical checklist for companies on the things they and their employees should do. They also provide guidance and a self-assessment process on when to "Report a Breach"[86].

DAPA

43

Where personal **data** has been **accessed** or **acquired** by an **unauthorised person**, and there is a real **risk of harm** to the data subject whose personal data has been subjected to the unauthorised access, a data controller shall: notify the Data Commissioner **without delay**, **within 72 hours** of becoming aware of such breach; and **communicate** to the data **subject** in writing within a reasonably practical period, **unless** the **identity** of the data subject **cannot be established**.

Where the notification to the Data Commissioner is **not made within 72 hours**, the notification shall be accompanied by **reasons for the delay**.

DAPA

43

Where a data processor becomes **aware** of a personal **data breach**, the data processor shall notify the data controller without delay and where reasonably practicable, **within 48 hours** of becoming aware of such breach.

The data controller may delay or **restrict communication** as necessary and proportionate for **purposes of prevention**, **detection** or **investigation** of an offence **by** the concerned **relevant body**.

The notification and communication shall provide **sufficient information** to allow the data subject to take **protective measures** against the potential consequences of the data breach, including: description of the **nature of the data breach**; description of the **measures** that the data controller or data processor **intends to take** or has taken to address the data breach; **recommendation** on the measures to be taken by the data subject to **mitigate** the **adverse effects** of the security compromise; where applicable, the **identity** of the unauthorised person who may have **accessed or acquired the personal data**; and the **name** and **contact details** of the data protection officer where applicable or other contact point from whom more information could be obtained.

The communication of a breach to the data subject shall **not** be **required** where the data controller or data processor has implemented **appropriate security safeguards** which may include **encryption of affected personal data**.

Where and to the extent that it is not possible to provide all the information at the same time, the **information** may be **provided in phases** without undue delay.

The data controller shall record the following information in relation to a personal data breach: the **facts** relating to the breach; its **effects**; and the **remedial action** taken.

85 *https://ico.org.uk/for-organisations/accountability-framework/records-management-and-security/unauthorised-access/*
86 *https://ico.org.uk/for-organisations/report-a-breach/*

DAPA
43
The Data Commissioner may apply to a court for a preservation order for the expeditious preservation of personal data including traffic data, where there is reasonable ground to believe that the data is vulnerable to loss or modification.
A data controller who, without **lawful excuse**, **discloses** personal data in any manner that is incompatible with the purpose for which such data has been collected **commits an offence**. A data processor who, without lawful excuse, discloses personal data processed by the data **processor without** the prior **authority** of the data controller **commits an offence**. A person who: **obtains access** to personal data, or obtains any **information** constituting such data, **without prior authority** of the data controller or data processor by whom the data is kept; or **discloses** personal data **to third party**, **commits an offence**. Subsection (3) **shall not apply to a person** who is an **employee** or **agent** of a data controller or data processor **acting within the scope** of such mandate. A person who **offers to sell** personal data where such personal data has been **obtained in breach commits an offence**, an **advertisement** indicating that personal data is or may be for sale **constitutes an offer to sell** the personal data.
GDPR
Article 34
Notify the controller of any data breach: processors are required to notify the controller of any breach without undue delay after becoming aware of a breach. **Notify the data subject of any data breach**: processors are required to notify the data subject of any breach if it is likely to result into a high risk to their rights and freedoms. The communication to the data shall describe in **clear and plain language** the nature of the personal data breach; **unless** the controller has **implemented technical** and **organisational protection measures**, and those measures were **applied to** the personal **data affected** by the personal data breach.

Chapter 3

Guidance given by Regulators

In order to assist the Data Protection Commissioner's office in the creation of their guidance to Businesses and Consumers, we have assessed the guidance and support given by other Data Protection Commissioners.

3.1 The United Kingdom (UK)

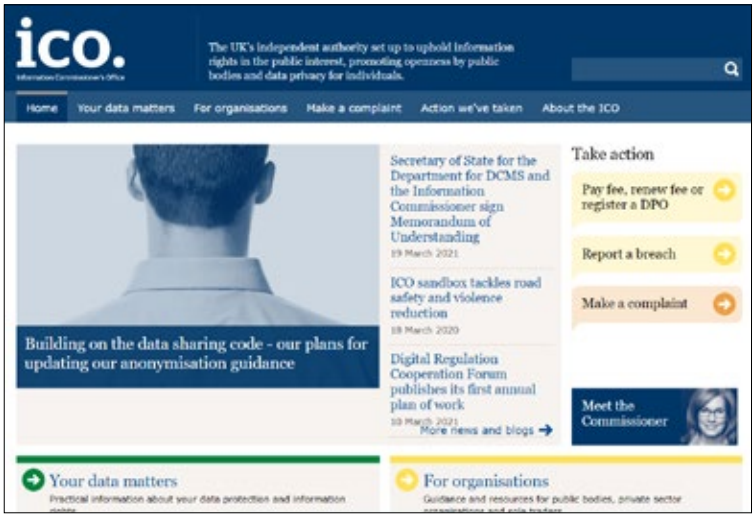
As identified with the volume of examples provided in the earlier regulatory overview, the UK Information Commissioner's Office (ICO) is a very good example to follow and below we have provided a number of examples that are highlights and viewed as extraordinary customer centric approaches when compared to other Data Protection Commissioners. What is noticeably obvious, are the online assessments, form and processes and tools i.e. self-assessments etc. that a business may use. There is no need for a consumer or business to leave the ICO website to initiate key processes or obtain more information.

The *Information Commissioner's Office*[87] (ICO) has many examples and guidance for consumers and businesses. It has been the leading authority when it comes to providing a data subject and data controller and processor-centric approach. The commissioner makes the data subject feel "taken care of" as the first knowledge area available is the *"Your data matters". The ICO allows for the theory of the legislation to be put into practice with interactive tools that help guide the consumer and business alike.*

"The pay fee, renew fee or register a DPO" in the "Take action" box is an example of an interactive tool for a data controller and processor to assess whether they need to register, and also what fees would be applied.

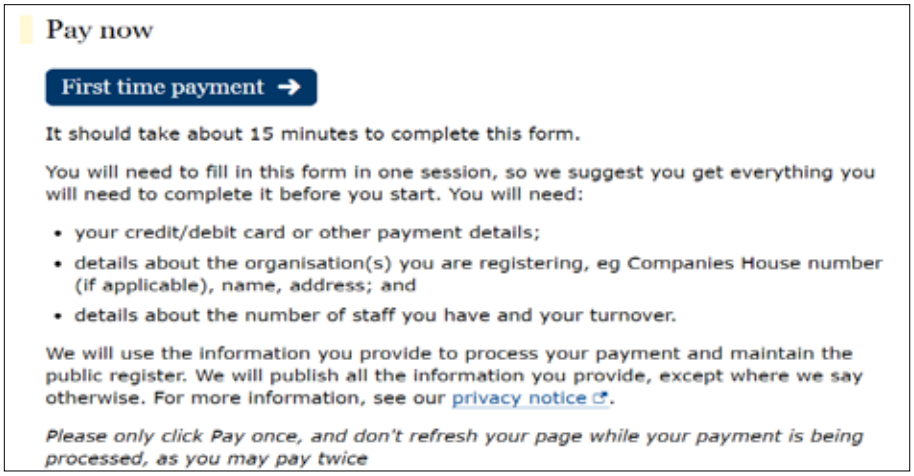
The below are example screenshots from the" The Pay Fee, Renew Fee or Register a DPO"[88] page that provide access to the tools:

1. First time payment has an online form for you to complete; there is no manual process of printing a pdf document completing it, scanning it back and sending it to a generic email address. An indicator on the time required to complete is also provided, which assists the user from a time management perspective and ensures they can complete the tasks in the time they have available, before starting and therefore potentially have to abandon and start again later.

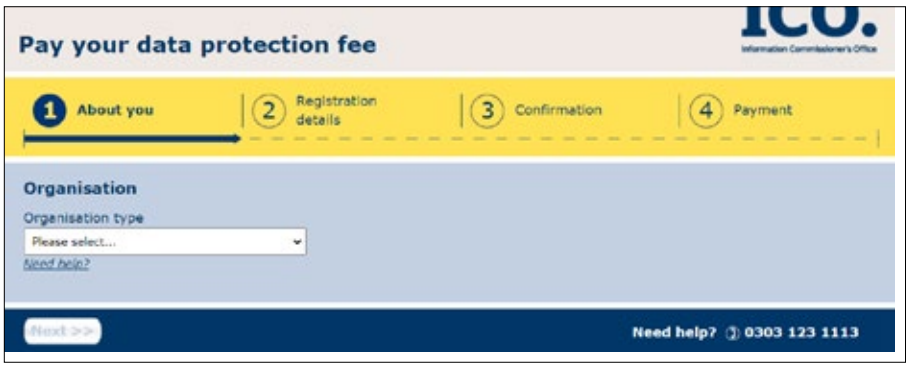


87 https://ico.org.uk/
88 https://ico.org.uk/for-organisations/data-protection-fee/

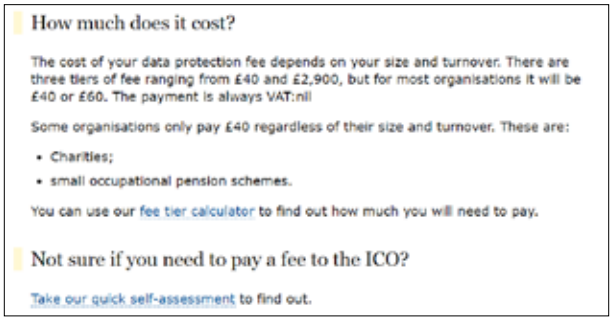
“Reading the preamble to the Act [DAPA] together with Section 3 thereof on the Act’s object and purpose, it is clear that the Act was intended to be retrospective to such an extent or to such a time as to cover any action taken by the state or any other entity or person that may be deemed to affect, in one way or the other, the right to privacy under Article 31 (c) and (d) of the Constitution. Needless to say, the need to protect the constitutional right to privacy did not arise with the enactment of the Data Protection Act; the right accrued from the moment the Constitution was promulgated.”



a. A breadcrumb flow details the steps you will go through to complete the first-time payment process.



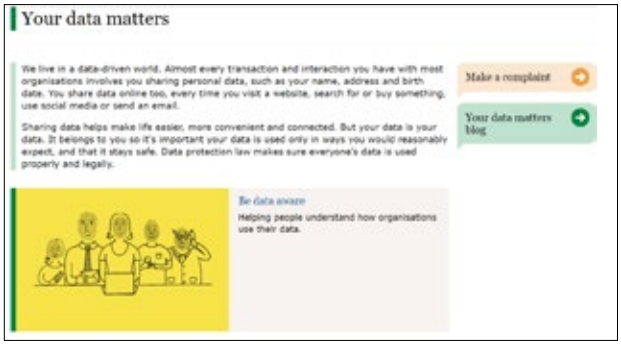
1. If you need to renew your registration, you are taken to the "Pay your data protection fee" online form with no need for manual intervention. In the initial registration and renewal, the "Pay your fee" section provides a fee tier calculator and an assessment tool to determine if you need to pay a fee to the ICO, as not all organisations need to register – but all organisations are contacted by Companies House and advised of their need to check if they should be paying the fee.



2. There is also an option to add a DPO and the ICO provides a self-assessment to determine whether you need a DPO or not.

Navigation via the top menu, brings you to the "*Your data matters*[89]" page that also has a lot of visual aids and acts as a reference to key points for a data subject and a guide to how they should expect to be treated by different businesses.

- a "Be data aware" link is available that takes you to a video that brings a simple message to highlight to data subjects how their online activity is being tracked and what it could mean to them. The "Be data aware" page also provides a launch point to more information and advice on how to get back in control of your data.



The Information Commissioner uses the visuals to aid in the education of the consumer and businesses in terms of what rights the consumer has and the advice that is available for a specific topic. The "Your rights" topics address the foundational principles of GDPR and are provided in layman's terms with a visible focus on customer centricity and making the education of GDPR accessible. This addresses the scenario of "all you needs at your fingertips".

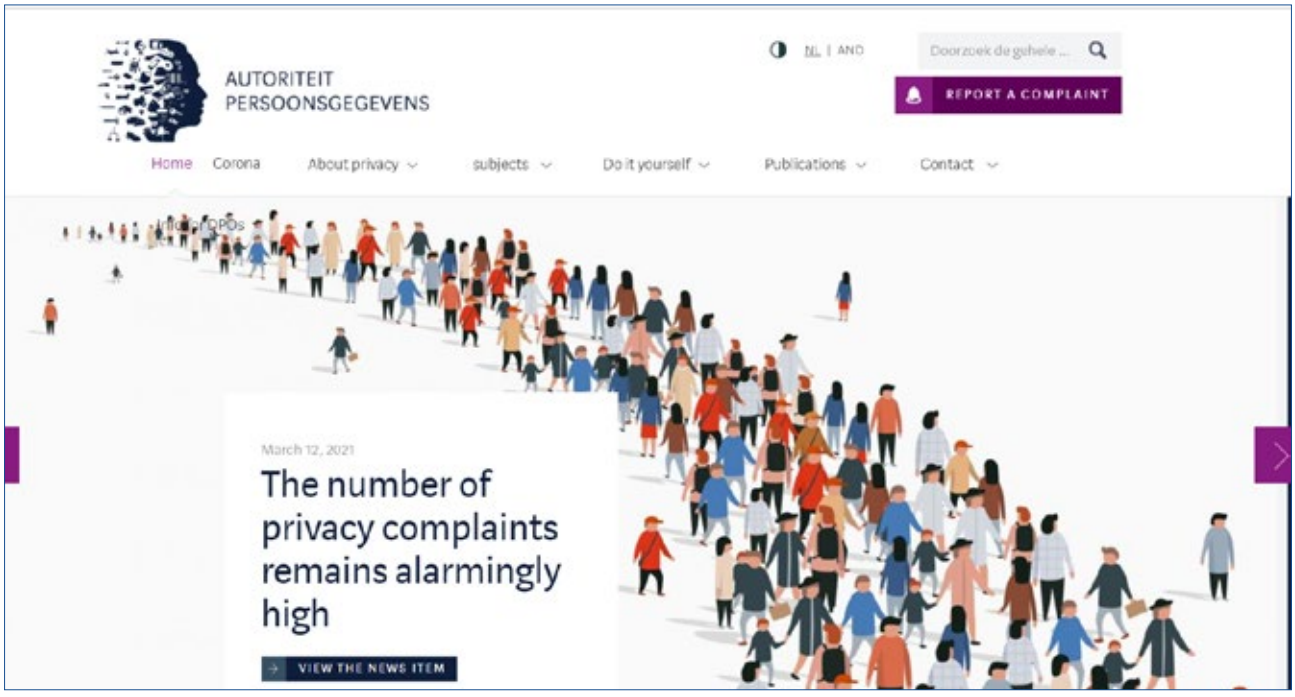
Via the top menu, you also reach a section dedicated to businesses "*For Organisations*"[90]. In addition to the guides to the GDPR legislation, the resources and support section provides access to tools, online forms, webinars and podcasts. Everything a business needs to know is accessed from this one page. With the ability to search and find more information if it is not immediately visible.

In the "*Action we've taken*[91]" section, there is a resource-rich page filled with pertinent and useful information on the enforcement, decisions, audits and monitoring reports, as well as key statistics on the day-to-day activity of the Commissioner. Practical "real life" scenarios are used to explain how the processes, procedures and practices are delivered and that will either enable a business or result in heavy penalties.

89 *https://ico.org.uk/your-data-matters/*
90 *https://ico.org.uk/for-organisations/*
91 *https://ico.org.uk/action-weve-taken/*

3.2 The Netherlands

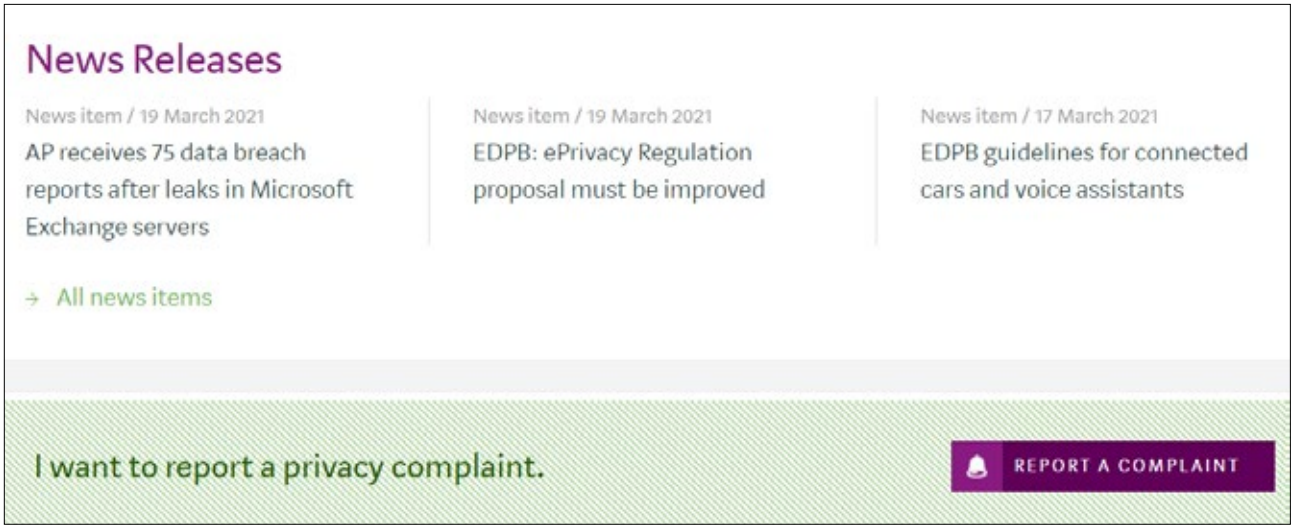
The *Dutch Data Protection Authority (DDPA)*[92] of the Netherlands is another good example of a customer and business-centric approach to how they apply the data protection policy both from a theoretical and practical experience. The Dutch regulator's homepage immediately makes a consumer and business aware of the impact of privacy issues. The homepage is dynamic, and once a new topical press release is available, the homepage image and press release



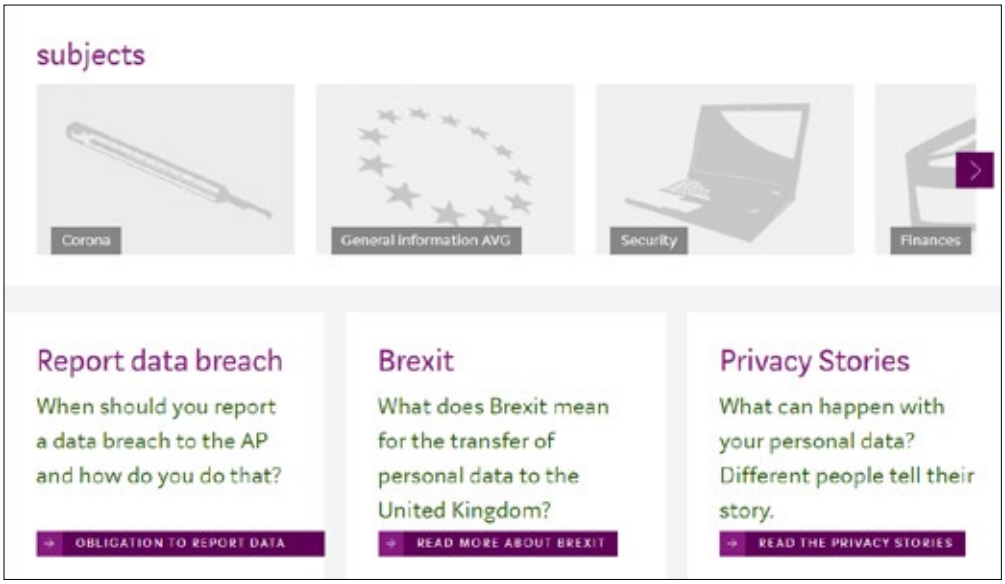
92 *https://autoriteitpersoonsgegevens.nl/en*

news item changes. This particular visual of the home shows a line of impacted consumers, highlighting that families and their children are impacted. The font used is very legible and they provide a link to the News item in this example related to the statistics, the types of complaints, fines after the complaints, and how many complaints are in the backlog still to be addressed. The visual for the most recent news item takes up the entire window of your device.

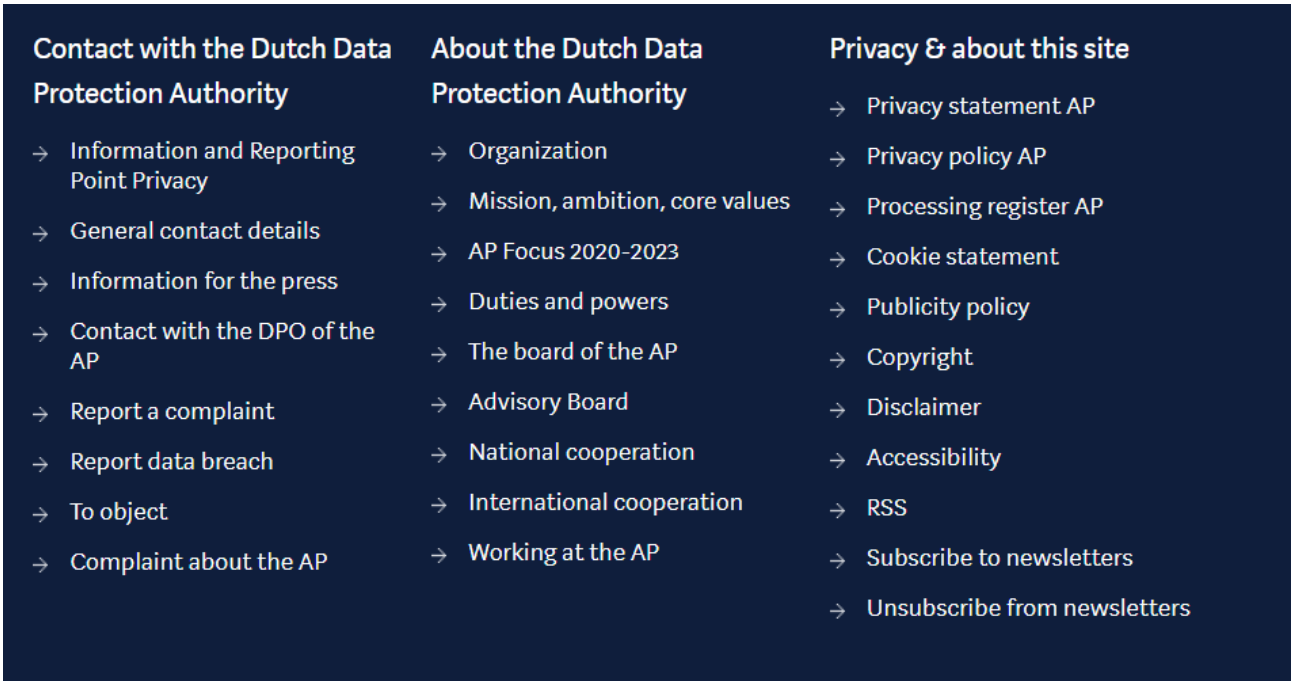
The homepage then provides a banner to report a complaint, as the first action item after the News Release banner. The Dutch regulator continuously drives the message to the consumer that they have rights, and to the business that there are consequences for failing to provide adequate protection of the data they have.



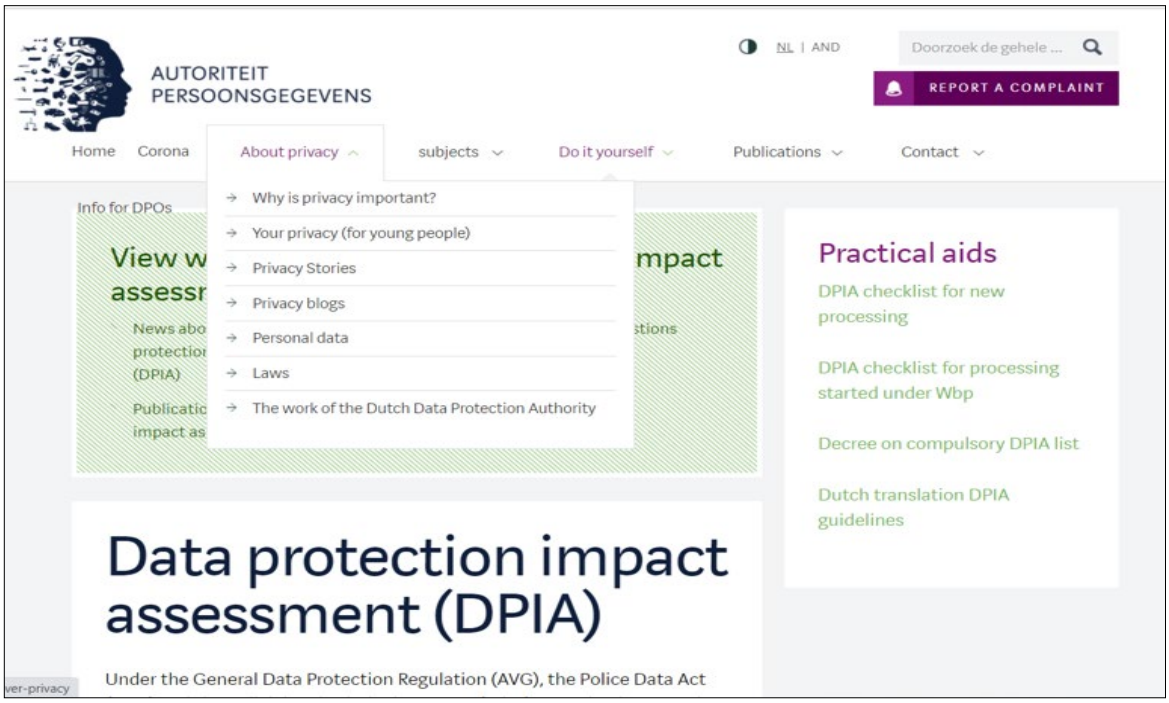
In addition to the latest news, different topical or high priority subjects are provided to the consumer and businesses, allowing the specific data privacy requirements to be grouped easily together.



The regulator also provides the following quick link to relevant processes that support the consumer and businesses on how to contact the DDPA and different non privacy related items to assist the consumer and business.

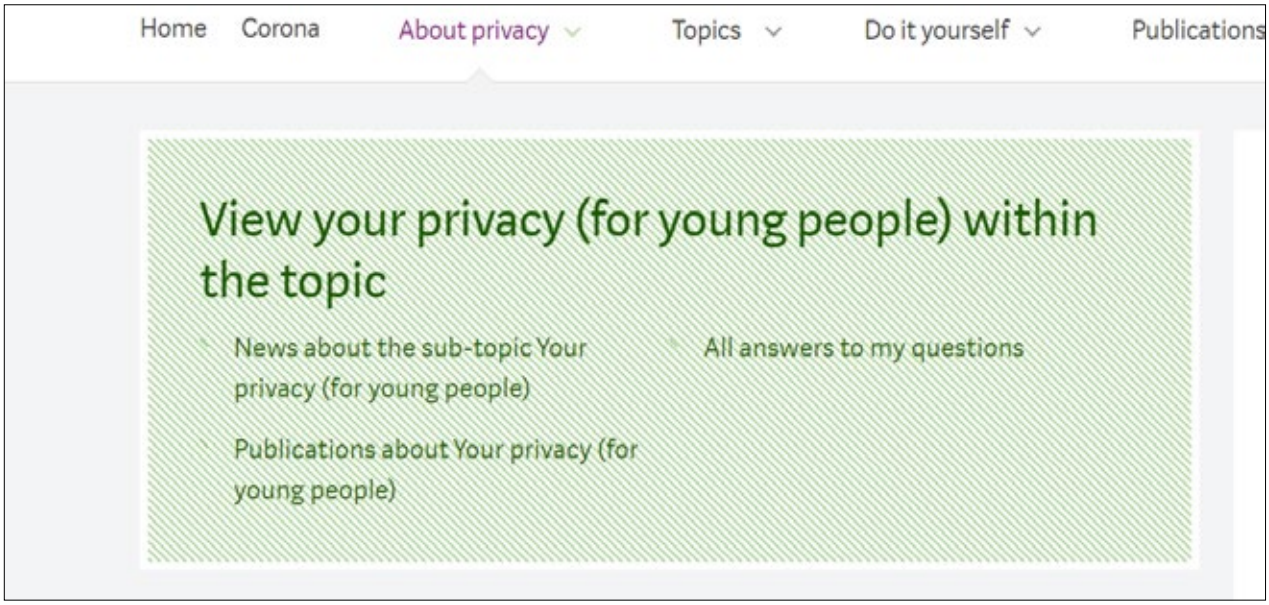


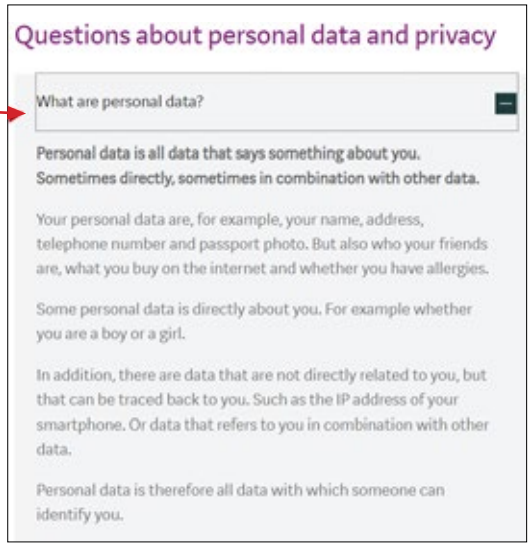
The menu at the top of the page provides easy access to further resources, making for simple site navigation. Throughout the site there is no use of legal jargon, except for legislation documentation, making the site very accessible to all. Every knowledge point has detailed subject areas and provides information for the DPO, consumer and businesses. Throughout the roles and responsibilities for the protection authority (AP), DPO, consumer and business are clearly defined. Practical aids are provided where relevant i.e., when a consumer or business selects the "View the Data" protection assessment, a practical aid box is displayed to various topics that can help businesses under different situations.



The first menu option on Corona provides insights for DPOs such as "How do we deal with privacy and the GDPR during the corona crisis?", as well as providing practical guidance on what is and is not acceptable.

The next menu option "About Privacy" provides a number of subjects to choose from which expands the subject in the page that is opened. We selected "*Your privacy (for young people)*"[93] *as an example of what the DDPA is doing to keep consumers, particularly the young, informed. It also includes advice for parents and teachers and keeps businesses informed, up to date and compliant. The page has the following structure:*





a. The ability to jump to other sections of the document in the green highlighted area.

b. A good overview of the challenges for young people

   i. Privacy stories relevant to the topic.

   ii. Information as to why privacy online is important, as most of the youth are online.

   iii. You can do this yourself, provides useful tips that can be used to protect personal data.

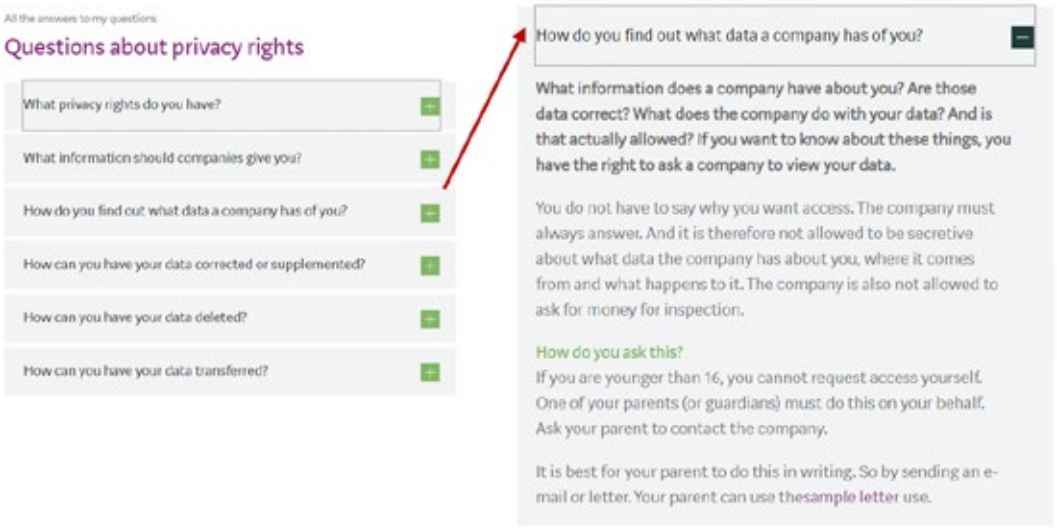
   iv. Information for teachers and parents.

c. News, applicable to the subject.

d. Key questions about personal data and privacy applicable to the subject that is being discussed.

e. Key questions about privacy rights.

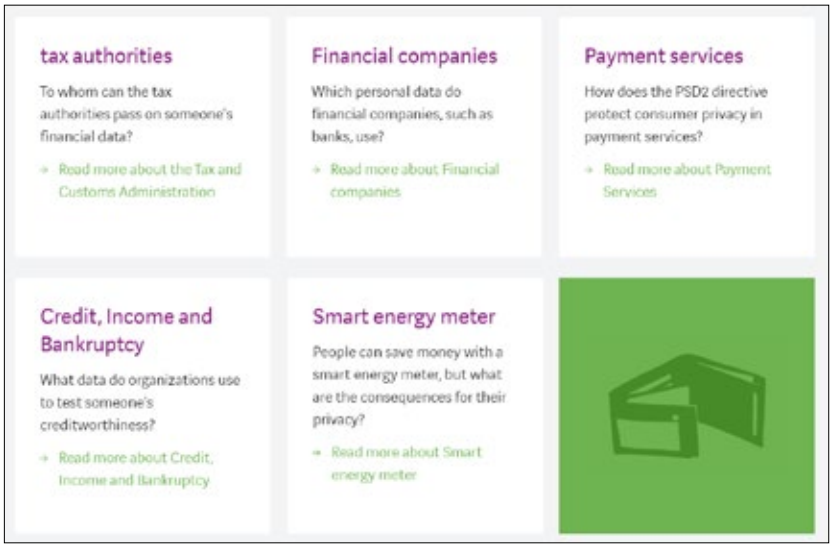
93 *https://autoriteitpersoonsgegevens.nl/nl/over-privacy/jouw-privacy-voor-jongeren*



The "Topics" section also has a dedicated section for different types of key subjects, under *Finances*[94] they explore the different types of Financial Data and the organisations that might hold this data.

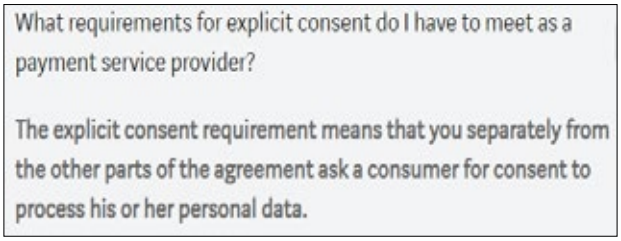
The "Finances" homepage opens with *"Financial data is* ***sensitive*** *personal data..."*

It then explores how each of these organisations might use your data, and what a data subject should expect – using the same format as we outlined above in "Your Privacy (for Young People)".



94 *https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/financien*

Exploring the topic of *payment services*[95], and more specifically as it relates to:


What requirements for explicit consent do I have to meet as a payment service provider?

The explicit consent requirement means that you separately from the other parts of the agreement ask a consumer for consent to process his or her personal data.

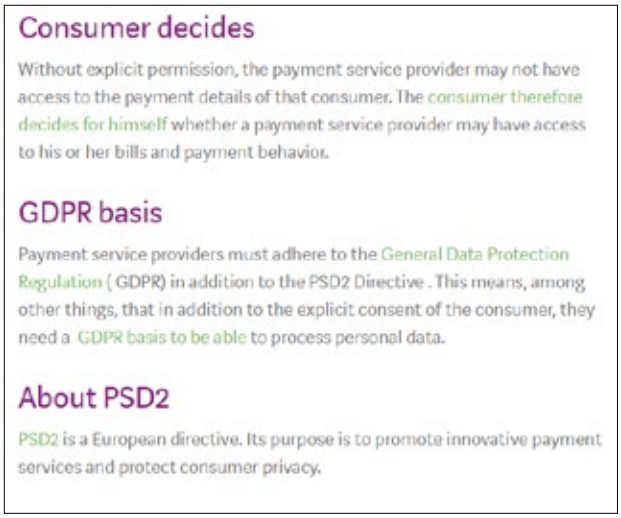
a. *Explicit consent*[96] *under PSD2*

b. *For the each of the topics below the items in green font actually hyperlink to the relevant consumer questions, providing clear guidance on what a consumer can expect and actions to follow if the data subject believes that their data is not used as prescribed.*

1.1 *Consumer decides*[97]

1.2 *GDPR basis*[98]

1.3 *About PSD2*[99]


Consumer decides

Without explicit permission, the payment service provider may not have access to the payment details of that consumer. The consumer therefore decides for himself whether a payment service provider may have access to his or her bills and payment behavior.

GDPR basis

Payment service providers must adhere to the General Data Protection Regulation (GDPR) in addition to the PSD2 Directive . This means, among other things, that in addition to the explicit consent of the consumer, they need a GDPR basis to be able to process personal data.

About PSD2

PSD2 is a European directive. Its purpose is to promote innovative payment services and protect consumer privacy.

The "Do it yourself" knowledge area provides access to everything a business or data subject would need. From an overview of the rights, sample letters, how to register a DPO, as well as processes, procedures, to do checklists to validate your compliance as a business or log a complaint.

1. The publication subject area has the following topics,
   a. Facts and figures on the activity in the DDPA
   b. Reports on the complaints and data breaches
   c. Research – providing individual reports on decisions, and guidance material
2. Information for FGs (DPOs) provides access to key resources for DPOs.

3.3 South Africa

The Information regulator of South Africa still has some way to go with helping consumers and business to understanding the basic context of the Protection of Personal Information Act (POPIA) i.e. *"What is POPIA and how will it affect me?"*

When a consumer or business goes to the Information regulator's website the following knowledge areas (leaving "Contact us" out) are available.

The "Documents" knowledge area provides several different subject areas as mentioned below, none of which really helps a consumer or business to know where to navigate to do as to understand in layman's terms what the Act is.

1. Government gazette
2. Legislation
3. Strategic and performance plans
4. Invite to comment
5. Annual report plans
6. Relevant judgements
7. Other documents
8. Forms
9. Policies, guidance notes and notices
10. Terms of reference for committees

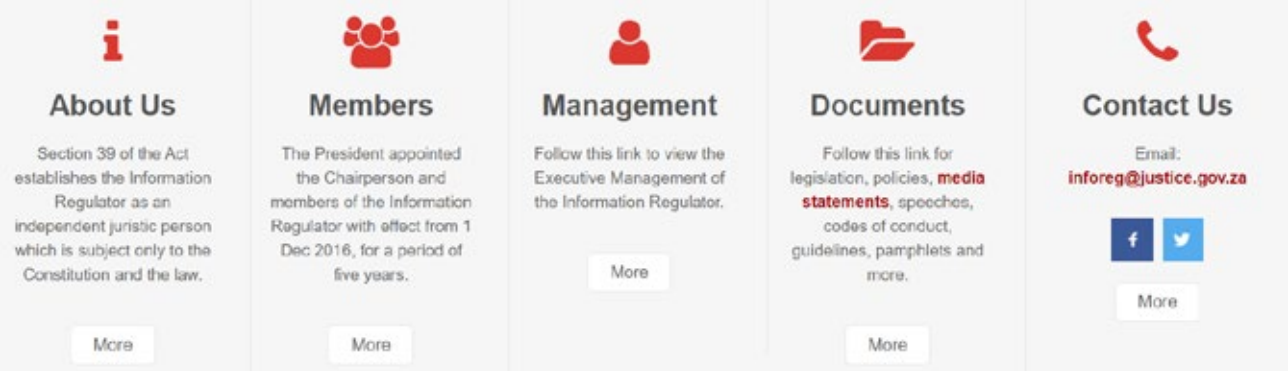
95 *https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/financien/betaaldiensten*

96 *https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/financien/betaaldiensten#aan-welke-eisen-voor-uitdrukkelijke-toestemming-moet-ik-als-betaaldienstverlener-voldoen-6871*

97 *https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/financien/betaaldiensten#hoe-komt-een-nieuwe-betaaldienstverlener-aan-mijn-betaalgegevens-6857*

98 *https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/financien/betaaldiensten#wanneer-mag-ik-als-betaaldienstverlener-persoonsgegevens-verwerken-6873*

99 *https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/financien/betaaldiensten#waarover-gaat-de-psd2-richtlijn-6853*

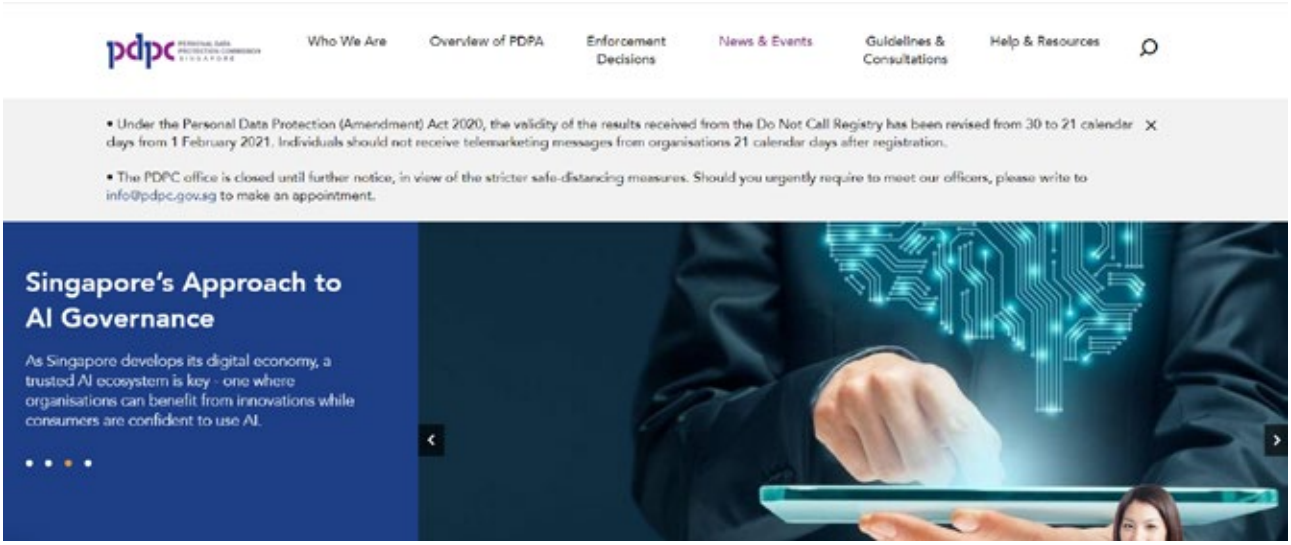


It is currently not consumer or business centric, as it is not as simple as "click and the information is readily available." A consumer must navigate very legislative heavy jargon. Frequently asked questions (FAQ's), checklists, and basic information do not exist. A basic site search function is not available where you can search using keywords. All the documents are in pdf format and are only available in English and Afrikaans, even though the Act states that all businesses that collect and use data need to make the policy available in English and in two of the other 11 official languages in South Africa.

In the "Strategic and performance" subject area, the orientated goals to achieve the successful enactment is visually defined. Although this is information that should be available, and could act as the jump point to a data subject's "Rights regarding the protection of personal information."

In summary the following improvements are recommended for what a consumer or business needs at their "fingertips" to be educated, informed and complaint:

1. Quick links to FAQ's i.e., provide basic laymen's information that anyone can access and understand:
    a. What is POPIA?
    b. What does personal information mean?
    c. What are my rights as a consumer?
    d. Who needs to POPIA compliant?
    e. By when does POPIA come into effect?
    f. What are the penalties for not being compliant?
    g. What are the foundational principles and the key areas that need to be implemented that will make a business compliant?
    h. Why is a DPO appointed and what role do they play?
    i. What processes, procedures and functionality need to be put in place that supports point (f) above?
2. Provide a business checklist that can validate whether their business needs to comply, and if they do, a summary of what needs to be put in place is displayed.
3. List of the seven foundational principles, what they mean for a consumer vs. a business.
4. What processes and procedures are in place to help consumers and businesses? Are there currently "good" examples, or media links to businesses that have not complied and the impact not only from the penalties applied, but from a reputational perspective as well?
5. Site search functions by keyword.
6. More structure to content that highlights what is important, changed or added.



3.4 Singapore

The *Personal Data Protection Commission (PDPC)*[100] of Singapore is another good example of a customer centric approach to the theoretical and practical application of the privacy legislation. Whilst functionally a lot of the procedures to request or lodge a complaint are manual, they are available as part of the process.

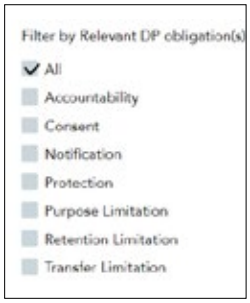
On opening the homepage, the regulator immediately provides the consumer and businesses with information appropriate changes. The below banner is dynamic and displays current regulatory topics that are global and country related:

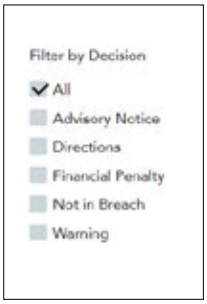
- Singapore's approach to AI governance
- Data sharing agreements
- DPO competency framework and training roadmap
- Enhanced PDPA for businesses

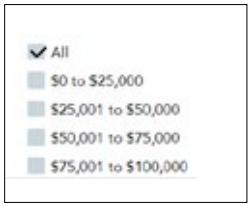
In the Overview section in the menu options at the top of the homepage a business and consumer have the following available to them:

1. The PDPC provides a clear and concise overview of the PDPA: What is personal data; What is the PDPA; what are the objectives of the PDPA; and the scope of what the protection of personal data is.
2. A timeline of the development of the PDPA
3. A link to the Act and other regulation

The PDPC in the *"Enforcement Decisions"*[101] *also provides view on the decisions on actual businesses or where an audit has been conducted. When you drill into the advanced search different filters are provided that outline the different categories of decisions. With the "Commission's decisions"*[102] reviewing the actions taken, and *"Undertakings"*[103] to monitor those implementing remediation plans.







100 *https://www.pdpc.gov.sg/*
101 *https://www.pdpc.gov.sg/Enforcement-Decisions*
102 *https://www.pdpc.gov.sg/Commissions-Decisions*
103 *https://www.pdpc.gov.sg/Undertakings*

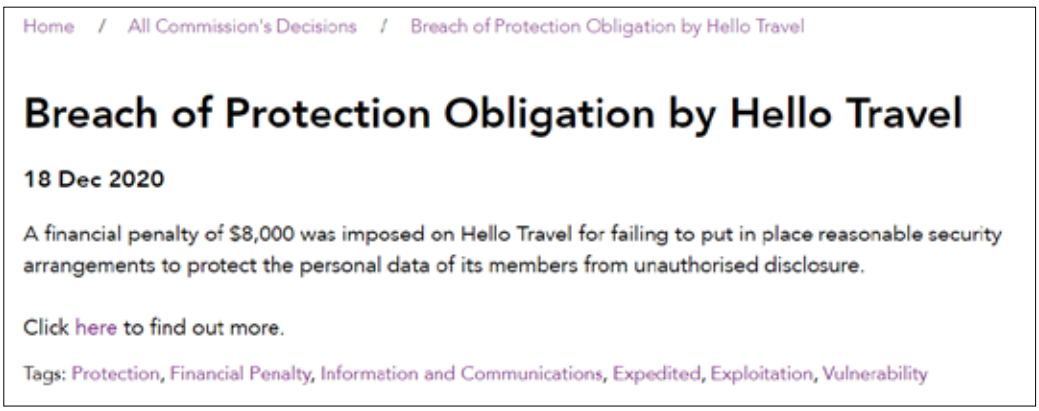
Examples of some of the decisions have been provided below, with examples of a "Warning", "Financial Penalty", "Directions" or a "warning".

Breach of the Protection Obligation by Water + Plants Lab
Nature of Breach: Protection
Decision: Warning
Published Date: 18 Dec 2020

Breach of the Protection Obligation by The Future of Cooking
Nature of Breach: Protection
Decision: Financial Penalty
Published Date: 14 Jan 2021

Breach of the Accountability and Protection Obligations by Everlast Projects, Everlast Industries (S) and ELG Specialist
Nature of Breach: Accountability, Protection
Decision: Directions
Published Date: 18 Dec 2020

Breach of the Protection Obligation by R.I.S.E Aerospace
Nature of Breach: Protection
Decision: Warning
Published Date: 18 Dec 2020


Home / All Commission's Decisions / Breach of Protection Obligation by Hello Travel

Breach of Protection Obligation by Hello Travel

18 Dec 2020

A financial penalty of $8,000 was imposed on Hello Travel for failing to put in place reasonable security arrangements to protect the personal data of its members from unauthorised disclosure.

Click here to find out more.

Tags: Protection, Financial Penalty, Information and Communications, Expedited, Exploitation, Vulnerability

The decisions, when expanded, provide more insight on why a fine (in this example) has been applied.

Under their "Help and Resources Section" PDPC also provides *DPO's with important information*[104] (this is expanded below). Two subject areas that provide the most customer centric approach are the "Kick-starting Your Data Protection Journey" and "Capability Building". To deliver the requirements of the Act, the PDPC understands that this is a resource intensive undertaking and the DPO requires support at an executive level and the resources to implement, monitor and maintain the requirements of the Act.

1. *Building Awareness*[105]
    a. Provides an overview of the foundational principles and more insight on the Act and the obligations of the DPO

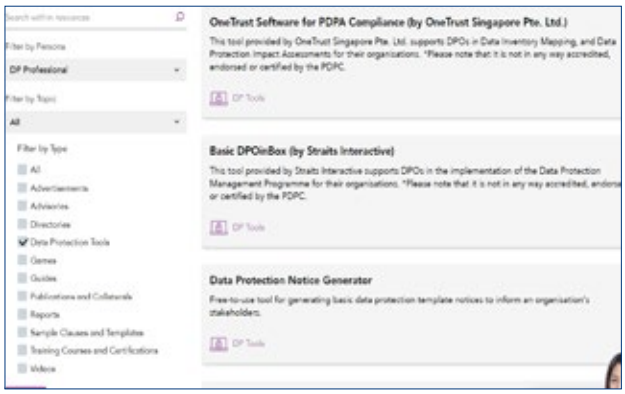
104 *https://www.pdpc.gov.sg/Help-and-Resources-Menu/Resource-DP-Professional*
105 *https://www.pdpc.gov.sg/DP-Professional/Building-Awareness*

2. *Kick-starting Your Data Protection Journey*[106]
    a. Provides learning materials and support available:
        i. an e-learning Programme,
        ii. DPO connect – a regular newsletter
        iii. PDPA briefings for Industry
    b. Resources available
        i. A Starter kit
        ii. Consultations for free on the PDPA with DPO's
        iii. Legal assistance

The PDPC collaborates with five SME Centres to offer free consultation on the PDPA. The centres are located at the following business associations:

1. Association of Small and Medium Enterprises (ASME): enquiries@smecentre-asme.sg
2. Singapore Chinese Chamber of Commerce and Industry (SCCCI): enquiry@smecentre-scccl.sg
3. Singapore Malay Chamber of Commerce and Industry (SMCCI): advisory@smecentre-smccl.sg
4. Singapore Indian Chamber of Commerce and Industry (SICCI): query@smecentre-sicci.sg
5. Singapore Manufacturing Federation (SMF): query@smecentre-smf.sg

    c. IT tools available to assist your business



3. *Capability Building*[107]
    a. A DPO competency framework
    b. a training roadmap and recommended courses starting from the basics
    c. Other training that is closely aligned, but not endorsed by the PDPC

Introduction

Data protection professionals such as data protection officers (DPOs) play an important role in ensuring sound personal data management policies and practices that can increase business efficiency and effectiveness, boost customer confidence and enhance the organisation's public image.

A typical data protection journey typically progresses through the following stages:

1) Building Awareness

Get to know your organisation's obligations under the PDPA to safeguard personal data entrusted to you by your customers and employees.

2) Kick-starting Your Data Protection Journey

Take the first step to kick-start the implementation of data protection policies and processes for your organisation using PDPC's free-to-use resources such as sample clauses, templates, communication materials and tools.

3) Capability Building

Find out more on the career pathway from entry-level data protection executives to regional data protection senior management roles, as well as the core competencies and proficiency required at each level to perform your job functions effectively in an organisation.

What is the PDPA about and how does it apply to my organisation?

What is expected of me as a Data Protection Officer (DPO)?

106 *https://www.pdpc.gov.sg/dp-professional/kick-start-your-dp-journey*
107 *https://www.pdpc.gov.sg/DP-Professional/Capability-building*

The regulator's *"Guidelines & Consultations"*[108] provide very clear and practical guides as to how to plan and implement the specific knowledge area. Not to focus too much on the DPO, the regulator, in a pdf, documents provides a *project plan outline and uses a case study of how to implement the Act*[109], a theoretical and practical way of guiding both a DPO and by doing so assisting the business and protecting the consumer.

PDPC makes the *annual and quarterly enquiry and complaints figures*[110] available to the public and they go back to the inception of the Act, which is different from other good regulators.

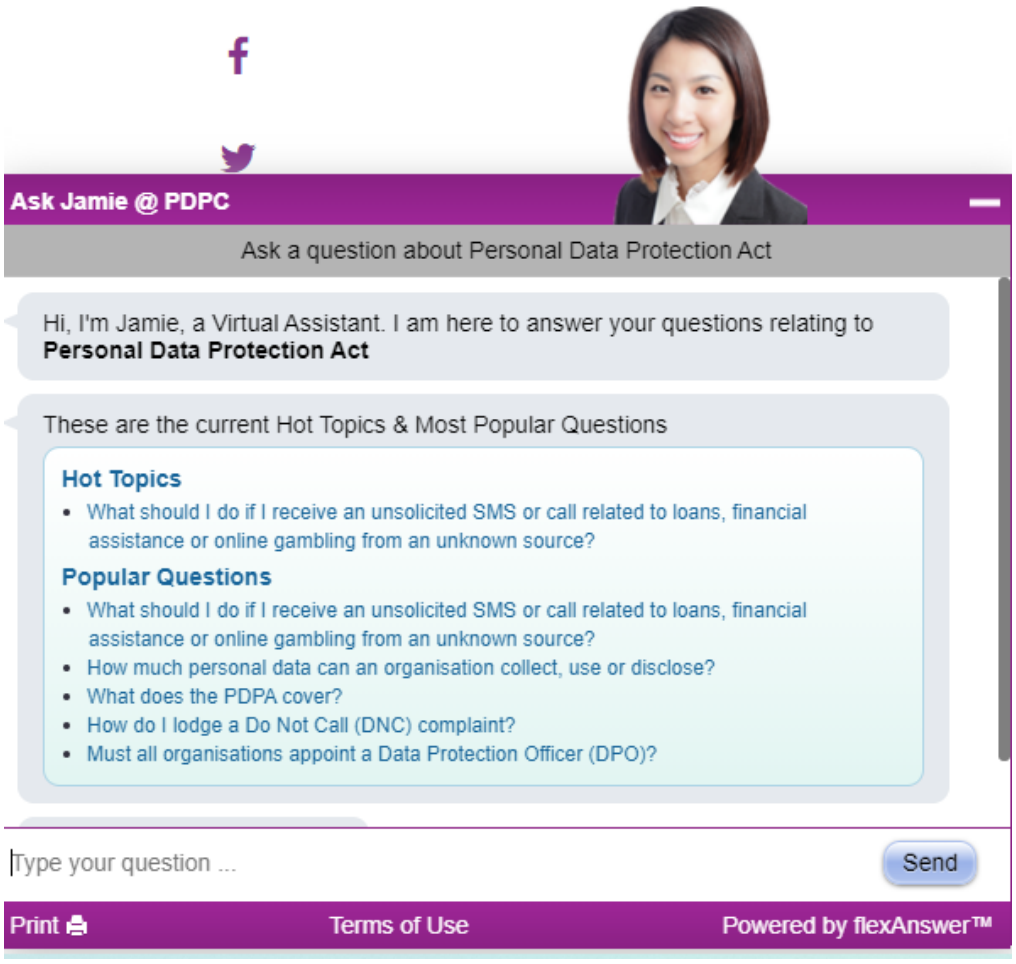
On all pages, they offer a virtual assistant called Ask Jamie @PDPC. This is another customer centric channel for consumers and businesses alike to ask questions. Instead of navigating the site or using the search functionality. When we selected "Ask Jamie", it shows key information and issues that consumers are currently facing.

Enquiry and Complaint Figures

2020

	Jan-Mar	Apr-Jun	Jul-Sep	Oct-Dec
Total Enquiries	13,200	3,100	5,300	3,600
Complaints	1,600	900	1,600	2,000

Figures are rounded to the nearest hundred.



108 *https://www.pdpc.gov.sg/Guideline-and-Consultation-Menu*

109 *https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPMP/Guide-to-Developing-a-Data-Protection-Management-Programme-(18-Nov-2020).pdf?la=en*

110 *https://www.pdpc.gov.sg/help-and-resources/2020/04/enquiry-and-complaint-figures*

FSD Kenya

Data Privacy and Protection in Kenya: A Regulatory Review

Credit/ pexels-Anna-Nekrashevich

DAPA specifically ensures that the data is limited to what is necessary in relation to the purposes for which it is processed, kept in a form which identifies the data subjects for no longer than is necessary, as well as ensures that the data use is explicitly defined. It goes on to further ensure that the data is only processed for the purposes agreed or that the processing is necessary or required by key exceptions (both from a public interest and legal perspective) or for the purposes of historical, statistical, or scientific research.

fsd Kenya

Creating value through
inclusive finance

Riverside Green Suites
Palm Suite, Riverside Drive
Nairobi, Kenya

info@fsdkenya.org

+254 20 513 7300

fsdkenya.org