OFFICE OF THE DATA PROTECTION COMMISSIONER

GUIDANCE NOTE FOR DIGITAL CREDIT PROVIDERS

DECEMBER 2023

TABLE OF CONTENTS

DEFINITIONS

Digital credit providers or DCPs - means any person or business entity that provides loan services through the internet, mobile services, computer devices, applications or other digital systems as may be prescribed by CBK.

Central Bank of Kenya or CBK - means the Central Bank of Kenya as defined in the Central Bank of Kenya Act, Cap 491.

Consent - means any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject.

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.

Data Processor - means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

Data subject - an identified or identifiable natural person who is the subject of personal data.

Innovation - the practical implementation of ideas that result in the introduction of new goods or services or improvement in offering goods or services.

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 or social identity.

Personal Data – means information relating to an identified or identifiable natural person.

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.

Processing - means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as (a) collection, recording, organisation, structuring; (b) storage, adaptation or alteration; (c) retrieval, consultation or use; (d) disclosure by transmission, dissemination, or otherwise making available; or (e) alignment or combination, restriction, erasure or destruction.

Retention period - refers to the length of time that certain records or data are kept before they are deleted or destroyed. This period may be determined by legal, regulatory, or organisational requirements. The purpose of a retention period is to ensure that important information is available when needed for legal, historical, or operational purposes, while also protecting privacy and reducing the risk of data breaches.

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.

Underserved-means underserved population refers to a group of people who have limited or restricted access to necessary services, such as healthcare, education, financial services, or technology. These limitations could be due to various factors, including socioeconomic status, geographic location, race, ethnicity, or other demographic characteristics.

THE OFFICE

The Office of the Data Protection Commissioner, is a government agency established to uphold and enforce data protection laws in Kenya. Its primary purpose is to protect the privacy, security, and fundamental rights of individuals concerning the processing of their personal data. The Office oversees the implementation and enforcement of the Data Protection Act, ensuring compliance by data controllers and data processors established in Kenya or targeting data subjects located within the country. Through its regulatory efforts, the Office strives to safeguard the confidentiality and integrity of personal data, promoting responsible and transparent data processing practices in both private and public sector organizations.

The Office plays a vital role in ensuring that individuals have control over their personal data and that organisations processing personal data, respect individuals' privacy rights. The Office's work involves monitoring and enforcing compliance with data protection regulations, investigating data breaches, and imposing sanctions on entities that violate data protection laws. In addition, the Office also has a duty to raise public awareness about data protection issues and educate individuals about their rights and organisations on how to protect personal data. With the growing importance of data collection and data processing activities in our digital age, the Office of the Data Protection Commissioner is a critical institution in maintaining trust and confidence in our data-driven society.

The Office of the Data Commissioner is uniquely positioned to facilitate both the government and private sector entities in achieving the Government's strategic goals under the "Bottom Up Economic Transformation Agenda ("BeTA") and, in particular, its digital superhighway initiative. As the digital landscape expands, the need for robust data protection mechanisms becomes paramount. The Office, with its mandate to oversee, regulate, and ensure lawful data processing, plays a pivotal role in this transformation. Kenya remains at the cutting edge of digital transformation while maintaining stringent data protection standards. The Office of the Data Commissioner serves as a key stakeholder and regulator in guiding the nation's digital superhighway journey by ensuring that as we advance technologically, the rights and privacy of individuals remain safeguarded.

INTRODUCTION

Personal data is becoming increasingly important in our economy and society. While new technologies and responsible data use provide significant societal and economic benefits, the abundance, granularity, and persistence of personal data create new challenges.

Due to the growing adoption and usage of technology-enabled innovations, financial services have undergone a radical digital transformation over the recent years. New technological disruptors who use digital innovations to create new business models, applications, processes, and products are largely responsible for this transformation. These innovations have made it easier for the underserved and unserved to access financial services. They also have fundamentally changed how consumers and businesses interact with and experience financial services.

Technology is a major force behind the transformation of financial services. The nature of financialservices, including credit and lending is being impacted. The greatest impact of this developmenthas been experienced in the lending space, where we have witnessed the introduction of Digital Credit Providers (DCPs). DCPs have emerged in Kenya riding on the growth in mobile money use and the increased demand for quick, easy to access, unsecured loans for the many Kenyans who lack a steady source of income.

DCPs have leveraged on technology to serve the underserved population in various ways, which include:

- DCPs are able to rely on alternative data sources to assess creditworthiness of individuals. Traditional lenders rely heavily on credit history and other traditional data to evaluate creditworthiness. However, many underserved populations, such as low-income individuals and small business owners, may not have established credit histories or collateral. For instance, they can use sources, such as mobile phone usage, social media activity, and transaction history, to assess creditworthiness and provide loans to underserved individuals.

- DCPs have been able to streamline the loan application process. Traditional loan applications have been time-consuming requiring extensive documentation. This has been a barrier for underserved individuals who may not have access to the necessary documentation or who may not have the time or resources to complete a lengthy application process. The streamlined application allows individuals to apply for and receive loans entirely through their mobile devices, within a matter of minutes. Overall, technology has disrupted traditional banking systems by offering new and more efficient ways to perform financial transactions and manage money.

- DCPs include both traditional financial institutions, such as banks and credit unions, as well as new players such as fintech start-ups and online lenders. They may offer a variety of loan products, including personal loans, business loans, and credit cards, and may also provide other financial services such as savings accounts, insurance, and investment products. These modifications in the offering of traditional financial services have had a significant impact on this sector and the lives of the Kenyans it serves.

DATA PRIVACY CONCERNS

Both the financial services industry and financial services consumers are impacted by these trends. The ability of financial services providers to collect, store, combine, and analyse a much wider range of customer data, from their current or previous location to customer behaviours andpreferences, has significantly improved thanks to technological advancements. Consumers are able to benefit from this, but there may also be new risks that are specific to the Digital Credit Providers' services industry and that may call for a focused policy response.

Human nature dictates that we skip over product terms and conditions because they are too long,too complex, or we are in a hurry. As a result, consumers may consent to terms which they wouldn't have otherwise agreed to, had the terms been clearer and specific. DCPs have published privacy policies in an attempt to comply with the Data Protection Act.However, the policies combined with the practices such as data sharing with third parties may at times not meet the compliance requirements outlined under the DPA.

The Kenyan Constitution of 2010 guarantees citizens the right to privacy, stating in Article 31 that "everyone has the right to privacy, which includes the right not to have information relating to their family or private affairs required or revealed unnecessarily." In this case,the DCP may be in violation of this provision if it ever publishes information relating to a data subject without a lawful basis.

DCPs assures its customers through a privacy policy that their personal data will not be shared with third parties without their consent, as required by the Data Protection Act (DPA). However, investigations reveal that some DCPs have been routinely sharing customer data with marketing companies without consent. This practice violates the DPA and infringes on customers' right to privacy, as guaranteed by the Kenyan Constitution.

Based on loan recipients' acceptance of terms and conditions, these lenders' processes result in the collection of a large amount of customer information, including their call and SMS logs, phone information, and even their photos and Facebook contacts. Consumers are frequently unaware that they are signing away their privacy rights.

The way decisions are made is changing, which has an effect on market products, final outcomes, and DCPs' bottom-line. This also implies a change on how data subjects are treated with respect to their personal data consequently jeopardizing the individuals' privacy. Data subjects are increasingly becoming unaware of how their personal data is captured,stored, and used in ways that were not anticipated at the time of collection and creation.

All actors in the digital credit sector should take into account the need to protect the human right to privacy and their compliance with the Data Protection Act. This should be an essential element of financial technologies. In order to do so, DCPs dealing with personal data should involve comprehensive privacy impacts assessments, consider the impact on other human rights such as equality, non-discrimination and economic, social and cultural rights.

In order for digital credit solutions to outlive the innovators, data subjects should be at the centre of the solutions, not their product. They should have meaningful access to, and control of, their personal data, including data collected or derived from the profiles that have been generated by third parties, and information about how it was obtained. Where consent is relied on as the lawful basis of processing, it should be free, informed, meaningful, and specific/granular enough to allow the data subject's control of the different possible uses of their information. The Data Protection Act ensures that data subjects' personal data should be used to empower them,

not to justify exclusionary practices or surveillance schemes.

SCOPE AND PURPOSE OF THE GUIDANCE NOTE

This guidance note sets out the compliance requirements that DCPs must implement in the processing of personal data in line with the administration of digital credit and in compliance with the DPA.

The guidance note starts with a highlight of the Office of the Data Protection Commissioner, outlining the mandate of the Office, its visions and its mission. Subsequently, the guidance note provides a background on the operations of DCPs by highlighting their contributions to society as well as the privacy requirements in the administration of digital credit. This guidance note also provides an overview of some of the legislative frameworks that govern DCPs.

These guidelines aim to provide a roadmap for how DCPs should safeguard the right to privacy and data protection for data subjects while at the same time supporting responsible innovation and sound operations within their sector.

These guidelines ought to be viewed as a tool for facilitating compliance with the provisions of the Data Protection Act and the Data Protection Regulations by the DCPs.

LEGISLATIVE FRAMEWORK

Globally, DCPs have become crucial tools for financial inclusion. Financial technologies have been and continue to be instrumental in fostering financial inclusion and development, particularly by enabling the fit-for-purpose, cost-effective, and readily available services that have been added to the infrastructure of mobile and digital platforms. The regulatory approach to DCPs in Kenya continues to evolve, involving a multi stakeholder approach with various regulatory bodies being involved in the regulation.

Similar to many other jurisdictions, Kenya implements its DCPs regulation through both general legislation that affects all sectors and sector-specific financial services regulation, which results in a multiplicity of regulations and regulators for digital credit provision.The assessment below provides an outline of the summary of some of the legislative and regulatory framework that governs the operations of DCPs in Kenya:

CENTRAL BANK OF KENYA AMENDMENT ACT (2021)

The Central Bank of Kenya Act establishes the Central Bank of Kenya (CBK) as the regulatory authority with the mandate of regulating financial service providers, including DCPs owing to the CBK Amendment Act of 2021. The Central Bank of Kenya (Digital Credit Providers) Regulations were published by the CBK in March 2022 and included a clause affecting data protection. According to Section 4(3)(k), in order to apply for a license, digital lenders must submit a copy of their data protection policies and practices.

CENTRAL BANK OF KENYA (DIGITAL CREDIT PROVIDERS) REGULATIONS, 2022

The Central Bank of Kenya (Digital Credit Providers) Regulations 2022 aim to address public concerns about the recent significant growth of digital lending, particularly through mobile phones. These concerns are related to the predatory practices of previously unregulated DCPs, specifically their high costs, unethical debt collection practices, and misuse of personal information. The Regulations govern DCP licensing, governance, and lending practices,among other things. They also provide for consumer protection, credit information sharing, and outline the Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)obligations of DCPs.

CREDIT REFERENCE BUREAU REGULATIONS

Credit Reference Bureau (CRB) regulations refer to the guidelines that govern the operations of credit reference bureaus. These regulations are put in place to ensure that the CRBs operate in a transparent, fair and efficient manner, and protect the privacy of the individuals whose credit information they hold.

Some of the key provisions of CRB regulations include:

i. **Licensing**: CRBs are required to obtain a license from the relevant regulatory authority before they can commence operations. The license is renewable annually.
ii. **Privacy and Data Protection**: CRBs are required to protect the privacy of individuals whosecredit information they hold, and ensure that such information is used only for the purposes for which it was collected. They are also required to comply with data protection laws and regulations.
iii. **Disclosure and Access**: CRBs are required to disclose credit information only to authorisedparties, such as lenders or employers. Individuals have the right to access their credit reports from the CRBs and to dispute any inaccuracies or errors.
iv. **Accuracy and Timeliness**: CRBs are required to maintain accurate and up-to-date credit information, and credit reports within a reasonable timeframe.
v. **Complaints and Dispute Resolution**: CRBs are required to have a mechanism in place for individuals to lodge complaints or disputes regarding their credit information. They are also required to investigate and resolve such complaints within a reasonable timeframe.
vi. **Record Keeping**: CRBs are required to maintain proper records of their operations, including credit information, complaints and disputes, for a specified period of time.

DCPs are expected to share both positive and negative credit information of their customers with CRBs, where such information is relevant for the carrying out of the function of the DCP. The DCP is also expected to ensure that the information provided is accurate and up-to-date. Prior to sharing any negative information of a customer, the DCP is expected to notify the customer at least 30 days prior to the sharing of their intention to do so.

PROCEEDS OF CRIME AND ANTI MONEY LAUNDERING ACT.

The Proceeds of Crime and Anti-Money Laundering Act (POCAMLA) is a law designed to prevent and combat money laundering and the financing of terrorism in Kenya. The Act was passed in 2009 and came into effect in 2010.

Under the POCAMLA, financial institutions in Kenya including DCPs, are required to implement robust anti-money laundering measures, such as customer due diligence, record-keeping, and reporting of suspicious transactions. The law also requires the establishment of the Financial Reporting Centre (FRC) as the agency responsible for receiving, analyzing, and disseminating financial intelligence related to money laundering and terrorism financing. Some key provisions of the POCAMLA include:

- **Customer Due Diligence**: Financial institutions must identify and verify the identity of their customers, including beneficial owners, before conducting transactions with them.
- **Record Keeping**: Financial institutions must maintain records of all transactions for a period of at least seven years or such longer period as the Financial Reporting Centre may require in writing from the date the relevant business or transaction is completed or following the termination of an account or business relationship without prejudice to any other records to be kept by or under any other written law.
- **Reporting of Suspicious Transactions**: Financial institutions are required to report any transactions that they suspect to be related to money laundering or terrorism financing tothe FRC.
- **Training and Awareness**: Financial institutions are required to provide regular training to their employees on money laundering and terrorism financing, and to establish policies and procedures for the prevention of these crimes.

The penalties for non-compliance with the POCAMLA can be severe, including fines, imprisonment, orboth. Therefore, it is essential that financial institutions in Kenya to comply with the requirements of the law to prevent and combat money laundering and the financing of terrorism.

APPLICATION OF DATA PROTECTION PRINCIPLES

The principles of data protection are provided under section 25 of the Act and under Regulations 28 to 34 of the Data Protection (General) Regulations 2021. This section provides practical guidance of how DCPs can implement the principles into their processing operations.

NB: Happy Loans is a fictional example that will be used all through for illustration purposes only and does not represent any real Digital Credit Provider (DCP)

EXAMPLE

Happy Loans is a DCP company. It loans money to its subscribers/ members through the mobile money platforms. Its method of operation is different from the traditional banking loan systems and modes that require numerous securities and collaterals for the bank to extend a loan facility to a customer. For happy loans, that is a rigorous process and its aim is to demystify and simplify the provision of loan from a complex, rigid and structured system into an easy system.

In as much as there is no asset collateral for the loans extended to its customers like in the normal banking business, to happy loans, the collateral to their loans is the customers reputation and image to their friends, peers, colleagues, workmates and the general public. This is evident to the fact that before being given a loan, the customer must download the Happy Loan Application. Upon downloading and installing the application on their gadget, the customer has to accept and give access to Happy Loans to all the particulars in the customer's phone from phone contacts, call logs, pictures, location, messages, all mobile phone applications and everything in the phone. Upon being given this access, Happy loans extracts everything from the customers' phone and stores it in its servers as a 'collateral' for when the customer fails to pay up the loan extended to them. To Happy Loans, they need all this information in order for them to do a credit risk assessment in order to identify a customer's risk profile and provide the customer with the proper credit risk analysis.

As regards to the terms and conditions, Happy Loans has an extensive terms and conditions that incorporates everything they wish to capture. The terms and conditions are written in prose with no headings at all. The acceptance to terms and conditions for the loan is a one-step acceptance wherein by one click, the customer has accepted to be bound by all the contents in the terms of conditions.

As regards to the loan limits, the loan limits keep varying and the limit is dependent on the repayment time period wherein one repays the loan borrowed. If one borrows the loan and pays it promptly, the loan limit for that individual increases.

LAWFULNESS, FAIRNESS AND TRANSPARENCY

Personal data collected by a DCP must be processed fairly, in a transparent manner, and must only be processed in line with a specific lawful basis. In implementing the principle of lawfulness, DCPs are required to ensure that their processing operations, practices and policies comply with the applicable laws and regulations. This includes data protection laws and other laws the DCPs are subject to. DCPs are also expected to conduct regular audits to ensure that they remain compliant withall legal requirements.

The Principle of fairness requires that DCPs process personal data in a manner:

- That the effect of processing is proportional to the intended outcome and does not have any possible negative impact;
- That the data subject would reasonably expect their data to be processed and that data subjects are not mislead about the processing of their data
- That ensures that individuals accessing their platforms equally and without discrimination.

The principle of transparency requires DCPs to communicate openly and honestly with all the data subjects. DCPs are required to provide clear and concise information about their business operations, products and services. DCPs are also required to be transparent in their data collection and use practices and give data subjects the ability to control the use of their personal data. DCPs are also required to ensure that any information on the use of personal data is easily accessible and easy to understand, and that it is clear and in plain language.

Example on how to implement the principles of lawfulness, fairness and transparency:

A client is interested in getting a loan from Happy Loans. They are typically required to provide personal data such as their name, address, phone number, date of birth, email address and photograph during account opening. Prior to allowing the client to sign up onthe Happy Loans platform, Happy Loans should ensure that the client is informed in writing, in a language they understand, of the following:

- what personal data is being collected, by downloading and installing the application.
- what personal data will be required to sign-up to use the platform or application
- what lawful basis is being relied upon to process the personal data throughout the processing.
- the rights data subjects are entitled to.
- Who will be in charge of data processing and how customer can contact DCP.
- Who will receive the personal data of the customer and for what processes.
- Whether data will be transferred to another country as well as the name of the country.
- For how long will customer data be stored by the DCP.
- To what extent there will be automated decision-making or profiling.
- safeguards, including third party safeguards
- Contact details of the DCP

PURPOSE LIMITATION:

DCPs must ensure personal data is collected for explicit, specified and legitimatepurposes, and must not be used for purposes other than those specified at collection. DCPs are expected, at the point of collection, to specify the purpose for which personal data is required and communicate the same to the data subject. In doing so, DCPs must ensure that personal data is not processed in a way that is incompatible with the purpose for which it was collected.

- **Example 1 on Purpose Limitation**: where Happy Loans collects personal data from a client for purposes of processing their credit worthiness to ascertain whether to give them a loan. Happy Loans can not use the client's personal data to advertise a new product or service it is offering to them, without acquiring or obtaining their consent. The purpose for use of the collected personal information should be for loan purposes strictly and not any other purpose whatsoever.

- **Example 2 on Purpose Limitation**: where Happy Loans collects the personal data of a client for purposes of offering credit, including their profile picture for purposes of setting up her account. Happy Loans cannot in other instance advertise its services using the photograph of the client on a billboard unless they have received their explicit consent to do so. This would amount to the DCP using the personal information for other purposes other than those anticipated.

Purpose limitation is designed to protect data subjects from having their personal data used for purposes they did not expect or consent to. In ensuring compliance with the purpose limitation principle, DCPs must specify the purpose for which they are collecting and processing the personal data and ensure that any additional processing is compatible with the initial purpose of processing.

DATA MINIMIZATION:

DCPs must ensure that they collect, process and store only the minimum amount of personal data necessary to achieve the specified purpose. This principle is designed to ensure that DCPs collect only what is relevant thus limiting storage requirements, redundant personal information, and the amount of personal data that may be exposed in the event of a security breach.

- Example Data Minimization: DCPs may collect personal data such as the name and address of the customer as part of the onboarding process. It would be inappropriate for a DCP to process information on the family of the customer or their religious beliefs.

This principle requires DCPs to implement technical and organisational measures to ensure that they only collect and process personal data that is strictly necessary for their intended and disclosed purpose at the time of the collection. By doing so, DCPs also ensure that they are complying with the legal requirements. This will also help to build trust with the data subjects and improve their reputation.

This principle necessitates that DCPs implement technical and organizational measures to ensure they only collect and process personal data that is strictly necessary for the intended purpose. By doing so, DCPs can effectively reduce the risk of privacy breaches while also ensuring compliance with legal requirements.

ACCURACY

Personal data collected by DCPs must be accurate and be kept updated, with necessary steps being taken to ensure that inaccurate data is erased or rectified without undue delay. Compliance with the principle of accuracy will help DCPs to ensure that the personal data in their custody is reliable and up-to-date.

> **Example Accuracy:** Happy Loans must ensure that they have accurate records of a customer's personal data held by it in order to provide the customer with credit services. Inaccurate records can leadto errors involving credit recovery in instances where a customer has fully repaid credit offered to them.

Some of the ways in which DCPs can ensure that the principle of accuracy is observed is by:

- Collecting accurate data. DCPs should ensure that the personal data they collect is accurate, relevant and limited to what is necessary for the intended purpose.
- Verifying the personal data collected. DCPs should verify the accuracy and completeness of personal data and take any steps to correct any errors.
- Regularly updating the personal data in their custody to ensure that it remains accurate and relevant and correct any potential errors or discrepancies.
- Giving data subjects the opportunity to update their personal data.
- Implementing data controls procedures to ensure the accuracy and completeness of the personal data.

STORAGE LIMITATION

DCPs must ensure that data is kept in a form that identifies the data subject for no longer than is necessary for the purposes of processing.

> **Example:** Happy Loans may need to retain a customer's personal data for a certain period of time in order to provide dispute resolution services. However, once this data is no longerneeded, Happy Loans must delete it in order to minimise the amount of personal data that is being stored.
>
> Furthermore, Happy Loans should design and implement data retention policies that specifyhow long personal data is kept and for what purposes. They could equally delete inactive customer accounts or personal data that is no longer relevant to its business operations.

To comply with this principle, DCPs must therefore regularly review the personal data they hold and delete or anonymise it when it is no longer needed for its original purpose. However, there may be exceptions to these principles where personal data needs to be retained subject to legal or statutory requirements.

INTEGRITY AND CONFIDENTIALITY

DCPs should ensure that customer personal data is kept confidential, free from manipulation, loss and unauthorized disclosure. Integrity and confidentiality work hand in hand to ensure that personal data is kept secure and accurate.

Example 1

Sarah, a young professional, decided to explore the convenience of digital loans and chose Happy Loans mobile app for her needs. As she filled out her application, she entered personal data including: her ID number, income specifics, and bank account information. This is where the principle of confidentiality comes into play. Confidentiality ensures that Sarah's personal data remains shielded from prying eyes. Ideally, Happy Loans would employ robust encryption methods to safeguard her data, transmitting it over encrypted channels and allowing access only to authorized personnel. Any deviation, like an unauthorized employee peeking into her details, would be a breach of this trust.

A few months down the line, Sarah, feeling financially buoyant, decided to repay her loan ahead of schedule. She logged into the app, keyed in the repayment amount, and hit 'pay'. This action brings the principle of integrity to the forefront. Integrity ensures that Sarah's repayment amount remains unaltered and accurate during the entire process. Happy Loans should employ mechanisms like checksums to verify the accuracy of the transaction. If, due to a software glitch, the amount Sarah entered were to change during processing, it would be a glaring violation of data integrity.

Example on Integrity and Confidentiality

Due to the hard economic times, Romeo Has found it hard to repay the loan that he took from Happy Loans.

As part of its loan recovery strategy, Happy Loans uses the call logs and the phone contact information obtained from Romeo's phone when he downloaded and installed the Happy loans application and gave them the permission to access all the contents of his phone to call his colleagues, employer and relatives informing them that Romeo has defaulted in paying the loan he took from Happy Loans and that they should come in and help him pay and or repay the same on his behalf.

This approach by Happy Loans is against this principle. Happy Loans should not call employers or relatives of customer informing them that the customer has defaulted in repaying the credit services extended to him/ her.

To safeguard the trustworthiness and privacy of data, especially in the digital realm, there are several straightforward yet effective measures that organizations can adopt. One of the primary ways to ensure data remains unchanged and genuine is by using what's akin to a digital "seal" or signature. This signature confirms that the data you're seeing hasn't been tampered with since it was sent. Additionally, by applying a unique digital "fingerprint" to data, organizations can later check to make sure that the data remains in its original form, untouched and unaltered.

When it comes to keeping data confidential, think of tokenization as a method of using code names. Instead of displaying the real, sensitive information, a placeholder or "code name" is used, keeping the actual data hidden and secure. For those concerned about data being intercepted during transmission, imagine Virtual Private Networks (VPN) as secure, private tunnels on the internet. They ensure that data sent from one point to another remains shielded from prying eyes. Similarly, there are digital "handshakes" or protocols, like Secure Socket Layer (SSL)/Transport Layer Security (TLS), that ensure data remains private as it moves across the web.

Another layer of security is akin to having different keys for different rooms in a building. Not everyone has the key to every room; access is granted based on one's role or responsibility. This ensures that only the right people have access to specific data. To further tighten security, think of multi-factor authentication as a double-check system. It's like needing both a key and a password to access a safe. Even if someone gets hold of the key, they would still need the password.

Lastly, to prevent accidental leaks or sharing of sensitive information, there are tools that act like vigilant guards, monitoring data transfers and ensuring that important data doesn't leave the organization without proper clearance.

In essence, by integrating these straightforward measures, organizations can create a strong fortress around their data, ensuring it remains both genuine and private.

LAWFUL BASIS FOR PROCESSING PERSONAL DATA

As a principle of data protection, every DCP is required to ensure that personal data is processed lawfully, fairly and in a transparent manner. Section 30 of the Act outlines the various lawful bases that DCPs can rely on in the processing of personal data.

The lawful bases include when the data subject has consented to the processing for one or more specific purposes, the processing is necessary for the performance of a contract, for compliance with any legal obligation, to safeguard the vital interests of the data subject or another natural person, for the exercise of official authority granted to the controller, and for the data controller's or data processor's own legitimate interests.

When the lawful basis for processing digital credit data hinges on the processing being "necessary", this does not mean the processing has to be absolutely essential. However, it should be more than just convenient or standard practice. The processing should be a targeted and proportionate way of achieving a specific goal related to digital credit provision. If a digital credit provider could realistically achieve the same objective with less data or through methods that are less intrusive to the customer, then processing under the "necessary" criterion would not be valid. In such a case, the lawful basis will not apply.

DCPs typically rely on legal bases such as the necessity of processing for contract performance, compliance with legal obligations, and legitimate interests pursued by the DCP or a third party. These bases allow DCPs to collect data for providing credit services, meeting legal requirements, and offering tailored products while safeguarding data protection and privacy. It's crucial for DCPs to assess and document these legal bases to ensure transparency and compliance.

PERFORMANCE OF A CONTRACT

Performance of a contract is considered as a lawful basis of processing under section 30 of the Act. This means that processing personal data is necessary for the performance of a contract to which the data subject is a party or for taking steps at the request of the data subject prior to entering into a contract.

When a contract is formed between two parties, it may be necessary to process personal data in order to fulfil the terms of the contract. This may include collecting and storing personal information about the parties involved, such as names, addresses, and payment information

Example of the lawful basis of the performance of a contract

On downloading and signing up to use the services of the Happy Loans, Romeo is required to provide his personal information to enable the performance of a contract. This occurs when he requests Happy Loans to loan him some money at an agreed interest rate for a specific period of time, following which, Romeo agrees to pay it back as per the terms and conditions of the contract. The personal data being processed in this instance will be processed under the lawful basis of performing the contract between Romeo and Happy Loans.

It is important to note that the processing of personal data must be necessary for the performance of the contract. If the processing is not necessary or goes beyond what is required to fulfil the terms of the contract, then it may not be lawful.

DCPs should ensure that they are transparent about the personal data they collect and how it will be used for the performance of the contract, and what rights the data subject has. They should also ensure that they have appropriate data protection measures in place to safeguard the personal data they process.

LEGITIMATE INTEREST

Legitimate Interest is one of the lawful bases for processing personal data under the Act. It is used when a DCP has a legitimate interest in processing personal data, and the processing is necessary for that interest, and does not outweigh the rights and freedoms of the data subject.

Legitimate interests may include the legitimate interests of the DCP, or of third parties, such as commercial interests, fraud prevention, network and information security, and the protection of the data controller's legal rights.

When relying on legitimate interests as a lawful basis for processing personal data, the DCP must balance their legitimate interests against the interests, rights, and freedoms of the data subject. This means that they must consider whether the processing is necessary for the legitimate interest, and whether the data subject's interests or fundamental rights and freedoms override that interest (i.e. section 30(1)(b)(vii) of the DPA: "if the processing is unwarranted (…) having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject").

In determining whether to rely on legitimate interest as a lawful basis of processing, DCPs will be required to carry out a legitimate interest assessment. The assessment entails determining whether the DCP is pursuing a legitimate interest (purpose), secondly, whether the processing is necessary for achieving the identified purpose, and, lastly, whether the data subject's interests override the legitimate interest.

Additionally, data controllers must provide transparent information to data subjects about the processing of their personal data under legitimate interest, including the specific legitimate interest being pursued, the types of personal data being processed, and the rights of the data subject with respect to the processing. They must also provide a means for data subjects to object to the processing on the grounds of legitimate interest.

The data controller must balance their interests against the individual's interests. In particular, if they would not reasonably expect you to use data in that way, or it would cause them unwarranted harm, their interests are likely to override yours. However, their interests do not always have to align with the individual's interests. If there is a conflict, their interests can still prevail as long as there is a clear justification for the impact on the individual. If the data controller is processing personal data in ways that data subjects would not reasonably expect, or if it would likely cause them unwarranted harm, it is likely that their interests will override the data controllers' legitimate interest justification, unless there is a compelling need to proceed despite the potential harm. In this regard, the data controller and data processor must ensure that they are applying the principle of transparency by informing individuals of the processing activities, likely impact and any risks.

An example on the Legitimate Interest Assessment.

Happy Loans shares data about its customers with a Credit Reference Bureau. The scope of the data shared involves the payments made by the individual on any credit facility extended to them .This data is then shared with any other digital credit service provider that the data subject makes an application to. The purpose of the sharing is to assist the digital credit service provider carry out an assessment of the data subject's ability to repay a credit facility. In carrying out the legitimate interest assessment digital credit service provider;

Wants to accurately assess the likelihood that they will get back the money they lend out to the data subject. The benefit to Happy Lonas is that it will be able to minimize the risk of bad debts and ensure other lenders make sustainable lending decisions to achieve a reasonable overall rate of return

It is also in the interest of the data subject making an application that the digital credit provider makes responsible lending decisions and does not allow them to become overburdened with debt that they cannot afford.

It is in the interest of the public that digital credit service providers make accurate risk assessments when making lending decisions. Without this lender may be less willing to lend or at least lend at a reasonable interest rate.NB:the benefits outlined above are vital for the proper functioning of the credit system intended outcome for the data subject is that they will either be granted or refused credit on the basis of their ability to repay. The lenders comply with the relevant laws.

CONSENT

When relying on consent for certain processing activities, the DCPs should ensure that consent is in compliance with the conditions for consent set out in the Data Protection (General) Regulations, 2021. In doing so, DCPs should ensure that the terms and conditions are separate from the consent forms. The basis for separation is that consent would need to be proven separately to other lawful basis. Further, the data controller or the processor has an onus of proving valid, express, specific and informed consent was obtained.

DCPs should note that acceptance of the terms and conditions does not amount to the consent of the data subject in relation to processing of personal data. Consent must be freely given, informed, specific, and unambiguous. It must be a statement or clear affirmative action signifying agreement to the processing, and the person has the right to withdraw their consent at any time. Digital Credit Service Providers have the duty to keep a verifiable record of the consent

Example:

Happy Loans have developed a new product and they would like to market the product to the existing customers. In doing so, Happy Loans will be required to obtain consent for that processing activity. Therefore, the requirements of consent as stipulated in the Act and the Regulations must be satisfied. In demonstrating compliance with the conditions of consent, Happy Loans should demonstrate that it has informed the data subject of the following;

- The identity of the data controller
- The purpose of seeking consent to process the personal data
- What personal data is being relied on for the processing
- Whether the personal data being relied on is going to be used for automated decision making
- The safeguards to be relied on where personal data is going to be transferred to outside Kenya
- Whether the personal data will be shared with other third parties, and if so, the identity of those third parties
- The right to withdraw consent and the implications of providing or withholding or withdrawing consent
- The DCPs, should also put in place mechanisms to ensure that the data subjects have the capacity to give consent, that consent is given voluntarily and that consent is specific to the purpose of processing.

Note

The Office has published a Guidance Note on consent on www.odpc.go.ke. The Guidance Note includes what entails a consent, how the same can be sought, whose burden is it to prove consent sought among other consent requirements.

COMPLIANCE WITH A LEGAL OBLIGATION

Compliance with a legal obligation is one of the lawful bases for processing personal data. This means that DCPs, in their capacity as data controllers or data processors, need to process personal data in order to comply with a legal obligation.

However, it is important to note that simply having a legal obligation does not necessarily mean that all processing of personal data in connection with that obligation will be lawful. The processing must also be necessary and proportionate to achieving the specific purpose for which it is required. In other terms, if the data controller can reasonably comply with their legal obligation without processing the personal data, this basis does not apply.

In addition, DCPs must still provide certain information to data subjects about the processing of their personal data, such as the purposes for which it will be used and their rights in relation to the processing. Data subjects also have the right to access their personal data, rectify any inaccuracies, and object to certain types of processing. However, such objection is subject to

any legal obligations that the DCPs are subject to or any legal claim that that they wish to bring or defend.

Overall, compliance with a legal obligation can be a lawful basis for processing personal data, but it is important for data controllers and data processors to ensure that their processing activities are necessary and proportionate to the legal obligation, and that they provide data subjects with the appropriate information and rights. A specific legal obligation that DCPs must comply with is the requirement to obtain explicit consent from data subjects before processing their sensitive personal data. For example, if a DCP collects health-related information or biometric data from their customers, they must obtain explicit consent from those individuals to process such data

RIGHTS OF A DATA SUBJECT

Data subject rights refer to a set of legal rights that individuals have in relation to their personal data. These rights have been established in the Act, and aim to give individuals more control over their personal data. DCPs should separate the Data subjects' rights from the Terms and Conditions which should be listed separately.

Example:

In addition to separating the provisions for consent from data subjects from its extensive terms and conditions, Happy loans should also separate and/or remove the data subjects' rights from the terms and conditions and leave them to be distinct and headed differently. So, in a nutshell the headings should appear as follows for clarity:

i) Borrower's/ Data Subjects Rights

ii) Consent from data subjects

iii) Terms and Conditions

THE RIGHT TO BE INFORMED OF THE USE TO WHICH THEIR PERSONAL DATA IS TO BE PUT

The right to be informed is a fundamental right that ensures individuals have the right to know what information is being collected about them, how it will be used, and who will have access to t This right is an essential component of privacy and data protection.

In practice, the right to be informed requires organisations and businesses to be transparent about their data processing practices. They must inform individuals about the purpose of and lawful basis for the data processing, the types of personal data being processed, who the data will be shared with, and how long the data will be retained.

The DCPs should inform the data subjects of their privacy rights as envisaged in the constitution and the use to which their personal data is to be put to.

Example 1

As earlier stated, a client downloaded, installed and signed up to the Happy Loans Platform for purposes of taking a loan from Happy Loans.

At the point of signing up, Happy Loans should provide the client with clear and concise information about how their personal data will be collected, used and shared. This information includes but is not limited to:

- What personal data will be collected (e.g., name, address, phone number, e-mail address, gender, National I.D. Number);
- How the personal data will be used i.e., the specific purposes that the information collected will be used for e.g. for purposes of identification; for an assessment of the creditworthiness of the borrower etc.)
- What lawful basis is relied on in processing the personal data
- Whether the personal data will be shared with any third parties and if so, the identity of the third parties.
- How long the personal data will be retained (e.g. for the duration of the subsistence of the loan)
- Any third parties that will have access to this data and the safeguards the third party has adopted.
- Their right to access, be informed, rectify, and have their personal data deleted, and how to exercise these rights.
- The contact details of Happy Loans Data Protection Officer or other privacy point ofcontact.

The DCPs should collect the necessary data and refrain from collecting unnecessary data not directly related to the digital borrower. For instance, in the above example, Happy Loans should not collect from clients' phone/gadget phone numbers of other people that form part of their contact list. Such collection is unlawful and requires consent from the owners of the numbers.

Additionality, it is important for DCPs to ensure that their data collection practices are aligned with their purpose of processing. Happy Loans, for instance, should refrain from extracting all data from their clients' phones. While DCPs argue that comprehensive information is necessary for profiling and credit assessment, the extent of data collected from people phones and gadgets may be deemed to be excessive. DCPs should focus on specific transaction details e.g. mobile banking history and/or M-Pesa messages which may be deemed to be sufficient to gauge an individual's credit worthiness, as such, aligning with their core objective of collecting personal data.

In addition, Happy Loans should include information about any third parties the data will be transferred to, whether outside Kenya or not, as well as details about the technical and organizational security measures taken to ensure data integrity and confidentiality, in accordance with Section 25 of the Data Protection Act. This ensures that Romeo's personal data is protected and treated responsibly throughout the loan application and borrowing process.

To implement the right to be informed, DCPs should identify the purpose of data processing. DCPs must clearly state the purpose for which the data is being collected and processed. This purpose must be communicated to the data subject before any processing takes place. The information must be provided in a clear and concise fashion. DCPs must provide data subjects with clear and concise information about the data being processed, including the categories of data being processed, the purpose of processing, the legal basis for processing, and the recipients of the data.

Example 2

Further the purpose of Happy Loans is for the provision of credit facilities in the form of loans to Romeo. In a case where information relating to Romeo's professional body and hisregistration number is required, Happy Loans should inform Romeo of the purpose of collection and the lawful basis relied upon for such processing. Further, the processing should be limited to the intended purpose.

DCPs must provide data subjects with the information they need to make informed decisions about their personal data in a timely manner. This means providing the information at the point of collection, or as soon as practicably possible thereafter.

DCPs should use plain language. DCPs must use plain and easy-to-understand language to communicate information about data processing to data subjects. They should avoid using legaljargon or technical terms that individuals may not understand.

DCPs should also ensure that the information is easily accessible. DCPs should make sure that individuals can easily access the information they need to exercise their right to be informed. Thismeans providing the information in a format that is easy to read and understand, such as a privacy notice, data protection policy taking into consideration the modes with which this information will be provided.

Overall, implementing the right to be informed is a crucial aspect of data protection and privacy. DCPs should adopt a levelled approach to accessing the personal data based on the credit facility being extended. This means that DCPs should tailor their access to personal data based on the specific credit facility being offered to individuals. In other words, the amount and type of personal data accessed should be proportionate to the credit service being provided. By doing so, DCPs can ensure they only collect and process relevant data necessary for evaluating creditworthiness, thereby respecting individuals' privacy and building trust with their customers.

By providing individuals with clear and concise information about how their personal data is being processed, DCPs can build trust and ensure that individuals are able to make informed decisions about their personal data.

THE RIGHT TO ACCESS THEIR PERSONAL DATA IN THE CUSTODY OF THE DATA CONTROLLER OR PROCESSOR

The right to access personal data is a fundamental right that individuals have under the DPA. This right is also an absolute right. It allows individuals to request access to the personal data that organisations hold about them and to obtain certain information about how this data is being processed.

Example

Romeo is interested in knowing what personal data that Happy Loans has collected about him. The personal data collected includes his name, age, identity number, Phone number, e-mail address, mailing address, his bio-data etc.

Happy Loans must give Romeo an access to the personal data collected. By allowing Romeo easy access to the personal data collected, Happy Loans will be able to foster and control accuracy of the personal data collected.

In implementing the right to access, DCPs should develop and make accessible clear procedures for responding to access requests. DCPs should have a clear and well-defined procedure for handling access requests. This should include the steps that need to be taken to verify the identity of the requester, the timeframe for responding to the request, and the information that needs to be provided. Additionally, DCPs should also make information available on their website about how individuals can submit a Subject Access Request (SAR). By providing clear instructions on how to initiate an access request, individuals can easily exercise their right to access their personal data. This information should include the necessary steps, contact details, and any specific requirements for verifying the identity of the requester.

DCPs should also train their staff. All employees who handle personal data should be trained on the right to access and the procedures for responding to access requests. They should understand the importance of this right and how to handle requests in a timely and efficient manner.

DCPs need to verify the identity of the requester before providing access to personal data. This can be done through a variety of means,such as requesting for a copy of the identification document.

DCPs should also provide the requested information. Once a DCP has verified the identity of the requester, they should provide them with the requested information. A data subject has a right to obtain from the data controller or data processor confirmation as to whether or not personal data concerning them is being processed, and, where that is the case, access to the personal data and the information as to the purposes of the processing; the categories of personal data concerned; the recipients or categories of recipient to whom the personal data have been or will be disclosed, including recipients in other countries; where possible, the envisaged period for which the personal data may be stored, or, if not possible, the criteria used to determine that period; and where the personal data is not collected from the data subject, any available information as to the source of collection.

Lastly, DCPs should ensure that they respond within 7 days as provided for under the Data Protection General Regulations.

THE RIGHT TO OBJECT TO THE PROCESSING OF ALL OR PART OF THEIR PERSONAL DATA

The right to object to processing of personal data allows individuals to object to the processing of their personal data where it is not necessary, or where it is being used for purposes that they do not agree with.

Example

Romeo a customer of Happy Loans, recently received marketing emails from Happy Loans promoting a new loan offer. However, Romeo feels that they do not need any more credit at the moment and does not wish to receive further promotional emails.

Romeo has the right to object to the processing of their personal data for marketing purposes. They can exercise this right by contacting Happy Loans and expressing their objection to receiving marketing emails.

Example (of notice provided to customers as part of the privacy notice)

In the event you wish to lodge an objection to the processing of your personal data kindly reach us through the following contact happyloans@complaint.com (an email is preferable mode of contact as it shows the time and date wherein the complaint was lodged).
Please, note that your request will be actioned within 14 days from the date of the receipt ofyour request. Your request attracts no charges.

DCPs should provide a designated contact person such as a data protection officer or customer service representative, who can assist individuals in exercising their right to object.

DCP's should also provide a simple and user-friendly process for data subjects to object to the processing of their personal data. This may include providing an online form, a dedicated email address, or a phone number.

DCP's must respond promptly to objections and take appropriate action, which may include ceasing the processing of personal data or where the DCP disapproves with the request, provide a justification of why the processing is necessary.

THE RIGHT TO RECTIFICATION AND ERASURE

The right to rectification of personal data allows individuals to request that any inaccurate or incomplete personal data held by a DCP is corrected or updated. This includes personal data that is processed by automated means, as well as data that is processed manually. DCPs are required to rectify the data subjects' false or misleading information without undue delay.

Example 1

Romeo has found out that his monthly repayments are not being accurately captured by Happy Loans. According to Romeo's Records, he has duly paid all his monthly repayments to date, yet,the information on Happy Loans platform shows that he is still in arrears and has defaulted the repayments for 5 months.

In this case, Romeo has the right to request for correction of the misleading data. Happy Loans should therefore correct and update the monthly repayments accordingly.

Example 3

Happy Loans can include the following clause in the privacy policy:-
"In the event of false and/or misleading personal information, kindly contact us through the following contact happyloans@corrections.com (an e-mail is preferable mode of contact as itshows the time and date wherein the complaint was lodged)
Please, note that your request will be actioned within 14 days from the date of the receipt ofyour request. Your request attracts no charges."

Example 2

Romeo wants to make his monthly loan repayment to Happy Loans and he discovers that his contact information and bio-data have been altered and that they are not the ones that he had given out when he signed up to Happy Loans Platform.

Similarly in this case, Romeo has the right to request for correction of the inaccurate contact information and bio-data.

Further, Happy Loans, should provide in its Digital Credit platform, contact avenues that Romeo can use in order to exercise his right to the correction of his personal data. In addition Happy Loans, should also state the time period within which the correction will be effected.

The right to erasure is also known as the right to be forgotten. It allows individuals to request the deletion or removal of their personal data by DCPs. It gives data subjects the right to request for the deletion or removal of personal data where there is no compelling reasons for its continued processing. This right enables individuals to have control over their own personal data especially in situations where the data is no longer necessary for the purpose for which it was originally collected or instances where the individual withdraws their consent.

Example 1

In addition to discovering that Happy Loans charges exorbitant interest rates on its loans as above, Romeo also discovered that Happy Loans captured his personal information and bio data wrongly and that Happy Loans had gone ahead and created a Whatsapp group containing persons whose contacts were extracted unlawfully by Happy Loans from his contact list. Romeo got furious and did not want to continue being a customer to Happy loans any more.He immediately paid back the outstanding loan amount and withdrew his consent for processing of his personal data. He went further and requested Happy Loans to 'forget' him totally and erase his personal data and the data that Happy Loans had gained access to unlawfully without his knowledge and consent.

As regards to this request of erasure by Romeo, Happy Loans should abide by it and fully erase Romeo's personal data and all the information that was unlawfully taken from him.Further, Happy Loans should implement mechanisms to ensure that the time limits established for the erasure of Romeo's personal data have been followed.

It is also important to note that the right to rectification and erasure not only relates to the personal data in the possession of the data controller or data processor but also to the third parties to whom the data controllers might have shared the personal data with them for processing purposes.

However, it is important to acknowledge that certain legal obligations may prevent full compliance with the request. For instance, if certain data is required for the purposes of evidence or to comply with other legal obligations, the data controller may restrict its processing instead of erasing it, and inform Romeo within a reasonable time. This ensures that data protection rights are balanced with other legal requirements that the DCPs must adhere to.

Example 2

In example 1 above, had Happy Loans as a data controller contracted/ outsourced anotherthird party, Kiongozi Storage Agencies, and shared Romeo's personal data and information forpurposes of storage of the data, upon Romeo lodging his request to Happy Loans to erase his data completely, the same request applies automatically to the third party, Kiongozi Storage Agencies and Happy Loans should ensure that the third party, Kiongozi Storage Agencies,has also erased Romeo's data.

The request for erasure by Romeo must be responded and complied to **within fourteen (14) days** of the receiving the request.

DCPs must respond to such requests within 14 days, at no cost to the data subject. In exercising this right, DCPs should request the data subject to provide documents or evidence supporting the request for rectification and erasure. Where a DCP refuses to comply with the request, it must provide a justification for its decision and inform the data subject of their right to complain to a supervisory authority if not satisfied. It is important for individuals to exercise their right to rectification or erasure to ensure that their personal data is accurate and up-to-date, as inaccurate data can have serious consequences for individuals,such as being denied credit or other services.

THE RIGHT TO DELETION OF FALSE OR MISLEADING DATA.

A data subject has the right to approach a data controller or data processor with a request to promptly rectify any personal data that is inaccurate, outdated, incomplete, or misleading. Additionally, they can request the erasure or destruction of personal data that the data controller or processor is no longer authorized to retain due to its irrelevance, excessiveness, or if it was obtained unlawfully.

If the data controller has previously shared the personal data with a third party for processing, they are obligated to inform such third parties about the data subject's request for rectification or erasure. This ensures that third parties also comply with the data subject's wishes.

However, there are exceptions. If the personal data in question is required for evidential purposes, the data controller or processor is not required to erase or rectify it. Instead, they should limit its processing and promptly inform the data subject of this action.

The Act and Regulations place conditions under which a data subject can request the erasure of their personal data. These conditions include scenarios where the data is no longer necessary for its original purpose, the data subject withdraws their consent, the data subject objects to the processing and there is no legitimate overriding interest to continue, and several other conditions. However, the right to erasure is not absolute. It does not apply if the processing is necessary for reasons such as freedom of expression, compliance with a legal obligation, tasks carried out in the public interest, archiving for public interest, or the initiating or defending a legal claim.

An essential point to consider is the potential impact of erasing data without any trace or notice. Such an action could have implications, especially for DCPs. For instance, if a borrower's data influenced previous decisions made by the data controller, erasing it might misrepresent the borrower's situation. It's crucial to weigh the benefits of data erasure against the potential risks and implications it might have on past decisions and records.

Example

Romeo has found out that his personal information as captured by Happy Loans in its digital credit platfOrm is false and misleading and does not accurately reflect the person that he is. Having made such a discovery, Romeo became furious and immediately writes to Happy Loans requesting them to delete in its entirety the false and misleading information from its digital credit platform.

Here, Romeo has the right to request that Happy Loans totally delete the false and misleading data in its entirety from its platform.

Further, in relation to this right Happy Loans needs to establish and have clear internal procedures for the deletion and destruction of the data. Upon deletion, Happy Loans should ensure that it is not possible to recover the deleted data.
It is also important to note that this right can be exercised by Romeo at any point of processingof his data.

THE RIGHT TO RESTRICT PROCESSING OF DATA

The DCPs shall at the request of the data subject restrict the processing of personal data under the circumstances laid down under section 34 of the Data Protection Act. These are;

(a) 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;

(b) personal data is no longer required for the purpose of the processing, unless the data controller or data processor requires the personal data for the establishment, exercise or defence of a legal claim;

(c) processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(d) 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

Example

Romeo had taken up a loan with Happy Loans in January 2021.He then completed paying the loan in March 2022 and owed no outstanding dues to Happy Loans. He thereafter deleted the application. However, he continued to receive messages regarding the repayment contrary to Happy Loans' Privacy Policy which stated that upon repayment of a loan, personal data would no longer be processed after the lapse of 30 days upon loan repayment.

In this instance, Romeo has found out that his personal information as captured by Happy Loans in its digital credit platform is no longer required for the purpose of the processing. Therefore, Romeo has the right to restrict Happy Loans from further processing of this personal data unless Happy Loans requires the personal data for the establishment ,exercise or defence of a legal claim.

Example

DCP should provide for the avenue and means of how Romeo can restrict the processingof his data by DCP.

THE RIGHT TO DATA PORTABILITY

The right to data portability allows for the customers to move or port their personal data from one DCP to another, taking into account the compatibility of the systems and technologies in use. Entities are allowed to charge an amount, for exercising this right. However, the amount should not be so exorbitant as to prohibit the exercising of the right.

Example

Romeo has recently discovered another Digital Credit Provider by the name Kadogo Cash that offers digital credit facilities at a very low interest rate of 0.5% per annum. Since his discovery, Romeo has been contemplating of making a switch from Happy Loans to Kadogo Cash as he feels that the loan interest rates of 20% per month being charged by Happy Loans is very exorbitant.

On that note, Romeo has written to Happy Loans wanting them to give him his credit history with them and take it to Kadogo Cash for him to be able to enjoy higher loan limit amounts from Kadogo Cash.
In this case, Happy Loans should avail to Romeo all his credit history with them so that he can move with it and or take it to Kadogo cash. Happy Loans should provide the required information within the stipulated periods of 30 days.

OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS

Processing of personal data refers to any operation or set of operations that are performed on personal data, such as collecting, storing, using, sharing, or deleting it.

During the life cycle of personal data, entities processing that data are expected to comply with the provisions of the Data Protection Act, Data Protection Regulations, 2021 and any other legislation that the DCP is subject to.

DUTY TO NOTIFY

One of the key principles of data protection is transparency. The personal data processed by an entity shall be processed fairly and in a transparent manner. Therefore, at the time of collection,entities must comply with the obligations under Section 29 of the Act.

This provision requires that data controllers and data processors notify data subjects of their rights specified in the Act; inform them that personal data is being collected, state the purpose of the collection; disclosing any third parties who may receive the data and the safeguards adopted; provide the contacts of the data controller or data processor and disclose whether any other entity may receive the data; describe the technical and organisational security measures taken to ensure data confidentiality and integrity; state if the data is being collected pursuant to any law and if it is voluntary or mandatory; and outline the consequences if data subjects fail to provide all or part of the requested data.

Example

In addition to Happy Loans informing and notifying Romeo of his rights as can be seen in the above examples under part 7 of this guidance note, Romeo should also be informed that his personal data is being collected and the purposes of the collection. Happy Loans should also inform Romeo about the third parties who may receive the data e.g. Kiongozi Storage Agencies as can be seen from the last example under part 7 above, and the safeguards adopted by the third parties, Kiongozi Storage agencies in this case.

Further, Happy loans should provide the contacts of the data controller or data processor and disclose whether any other entity may receive the data. Happy loans should also provide a detailed description of the technical and organisational securitymeasures used to ensure confidentiality and integrity for example, the use of encryption and pseudonymisation, passwords, access rights, information security policies, business continuity plan, risk assessments, reviews and audits, etc.

Happy loans should also inform Romeo about the legal provisions relied upon b it to collect the data from him and the consequences of the failure to provide the information or refusal to provide the requested data.

This duty to notify can also be captured and encapsulated in a **Data Protection Policy**.

The Data Protection Policy acts as a notice to individuals whose data is to be collected or otherwise processed. This policy must be brought to the attention of all individuals prior to the collection of their personal data or as soon as possible soon after where information is not collected directly. The data protection policy should also be provided to individuals upon request.

TIPS FOR DRAFTING A DATA PRIVACY POLICY FOR DCPS.

When drafting a privacy policy, there are several practical tips and considerations that should be taken into account to ensure it effectively communicates to data subjects how their personal data will be processed, these include:

1. The policy should be written in clear and plain language that is easy to understand.Technical or legal jargon should be avoided as much as possible to ensure that data subjects can easily comprehend what the policy says. The entities should also take into account the likelihood of disabilities of the customers and factor that when preparing the policy.
2. The policy should be transparent and comprehensive, covering all the relevant information that data subjects need to know about the processing of their personal data. This includes information about the rights of data subjects under the Data Protection Act, the fact that personal data is being collected, the purpose for which the personal data is being collected, the third parties to whom the data may be transferred, and any safeguards in place to protect the data.
3. The policy should be accessible to data subjects. This can be achieved by making it available on the data controller's or data processor's platform set up to access the digital credit facility or by providing a copy upon request.
4. The policy should be reviewed and updated regularly to reflect any changes in data processing practices or in relevant laws and regulations.
5. The policy should include:
    - Contact details
    - Information collected
    - How information has been collected, what legal basis/bases is/are relied upon
    - How information is stored
    - Data subjects' rights
    - Avenues to complain, etc.
6. An indication of how the DCP will comply with its regulatory obligations under data protection and what actions are reasonable and appropriate (or reasonably practicable) for your organisation to take to correctly apply the data protection principles to its activities.
7. A clear indication of how the organisation will implement technical and organisational measures within to ensure compliance.

To make privacy policies easy for data subjects to understand, it is important to use plain language and avoid technical jargon. Visual aids such as infographics and diagrams can also be used to help convey complex information. In addition, using a question and answer format or breaking down the policy into shorter sections with clear headings can make it more digestible for data subjects. Providing examples of how personal data may be used in practice can also help data subjects to understand the policy and the implications of sharing their personal information.

EXAMPLE OF HOW THE DUTY TO NOTIFY CAN BE EFFECTED WHERE THE PERSONAL DATA IS COLLECTED INDIRECTLY.

In the event Happy Loans collects data about its customers' usage patterns and location information through their mobile devices. In such a case, Happy Loans could fulfil its duty to notify by including clear language in its privacy policy about the types of data being collected and the purposes for which it is being used.

Happy Loans could also provide notice through a pop-up or banner message on its mobile app or website through a cookie notification that explains the data collection and provides a link to the full privacy policy. Additionally, Happy Loans could offer a simple opt-out mechanism for customers who do not wish to have their data collected.

N/B:

The data protection policy is an external facing document and is not to be confused with any internal policies that an entity develops to ensure internal practices align with the Data Protection Act. The common practice of demonstrating compliance with the laws and regulations among controllers and processors is through privacy policies and notices on websites. The information in a data privacy policy must be provided in simple and clear plain language, appropriate language for the target audience and be provided free of charge. The data privacy policy must be kept up to date to meet any changes in your approach to processing data.

Example

A data privacy policy for a digital lending platform may clearly state that the platform collects certain phone information from borrowers solely for credit-scoring purposes, ensuring transparency and lawful data processing. However, the policy explicitly prohibits the lender from accessing borrowers' phone records to gather contact information of third parties for debt collection purposes. This restriction emphasizes the importance of respecting borrowers' privacy rights and ensures that data processing aligns with the principles of the Data Protection Act.

Example

The Section of lawful purpose for processing personal data can contain clauses including aprovision that contains the following;

- "Your information may be used and analysed by us for the following reasons:
- Processing the services you've enrolled in through our digital platform
- Billing you for accessing our services
- Debt recovery
- Conducting credit checks and scoring
- Contacting you with offers or promotions unless you choose not to receive them
- To comply with any legal, governmental, or regulatory requirements or for use by ourattorneys during any legal processes
- Prevention of Fraud and other crimes
- Research, statistics, surveys, and other academic or commercial endeavours
- Addressing any questions you may have

DATA COLLECTION (BOTH DIRECT AND INDIRECT)

DIRECT COLLECTION

Where personal data is collected directly from a data subject, a data controller needs to inform the data subject, in so far as practicable, of all relevant aspects of data processing defined under Section 29 of the DPA. In addition, a data controller needs to explain the legal basis of data collection, e.g. compliance with a legal obligation, performance of a contract, or legitimate interests.

Example

At all material times whenever Happy Loans wants to collect data from Romeo, a digital borrower, Happy Loans needs to inform Romeo in so far as practicable of all the relevant aspects of data processing as defined under section 29 of the DPA.

N/B:-

DCPs must be transparent about the data they collect from applications and how it is used. The information should also be collected for legal or legitimate purposes, which in the case of digital lending may be credit rating and maintaining business records. Moreover, digital lenders should maintain reliable data about borrowers; this includes immediately updating their payment histories on the credit- sharing information system.

INDIRECT COLLECTION

Section 28 of the DPA provides for the indirect collection of personal data, such as in cases data is contained in a public record or, the data subject has deliberately made the data public or, the data subject has consented to the collection from another source or, the data subject has an incapacity, the guardian appointed has consented to the collection from another source, or, the collection from another source would not prejudice the interests of the data subject. Also, data may be collected indirectly from another source if necessary for the protection of the interests of the data subject or another person.

Example

Happy Loans wants to create a very reliable credit profile for Romeo. The management of Happy Loans has discovered that Romeo only availed his name, phone number and place of residence where he stays. Romeo did not reveal his age which is very important in assessingthe credit repayment risks.

Happy loans can get the information relating to age from public records by searching through places such as the births and deaths records which are often maintained by governments to ascertain the number of births and deaths in the country. Such records typically contain information about when and where one was born.

From there, Happy Loans may be able to obtain further personal data about Romeo i.e. Romeo's age. After getting the information relating to age for Romeo, Happy Loans can go ahead and create the intended credit profile that it was to create.

N/B

While personal data may be publicly available through public records, it's still important to respect people's privacy and use this information responsibly and ethically.

DATA STORAGE

The principle of storage limitation is a fundamental principle in data protection. It provides that personal data should only be kept for as long as it is necessary for the purpose for which it was collected. Once the purpose has been fulfilled, the data should be deleted, anonymized or pseudonymised to ensure that it is not kept for longer than is necessary at the expiry of the retention period.

There are several reasons why the storage limitation principle is important in data protection. Firstly, it helps to ensure that personal data is accurate and up-to-date, as outdated data can be misleading or harmful. Secondly, it helps to prevent the misuse of personal data, as data that is no longer needed is less likely to be accidentally or intentionally misused. Finally, it helps to protect individuals' privacy rights, as personal data that is no longer needed is less likely to be accessed or disclosed without the individual's consent.

Organisations that collect and process personal data are responsible for ensuring that they

comply with the storage limitation principle. As provided for under the Data Protection (General) Regulations, 2021 data controllers and data processors are expected to put in place personal data retention schedules, with appropriate time limits for periodic review.

The retention schedules should outline the purpose for retention, the retention period, provisions on period of audits of the personal data retained as well as actions to be taken after the audit.

In carrying out the audit contemplated above, data controllers and data processors are expected to assess personal data to determine if it remains relevant and necessary for the original purpose of collection, ensure that the personal data being retained is up-to-date, specify the purpose of retention, ensure that the security measures are adequate and identify the best cause of action where theretention period has lapsed.

Policies and procedures in place for the retention and deletion of personal data must be regularly reviewed and updated to ensure that they remain relevant and effective.

Example 1

In the above example where Romeo has signed up to use the services of Kadogo Cash but he ends up not to take the credit facility from Kadogo Cash, Kadogo Cash has to notify Romeo how long his information will be held and the purpose of such retention, noting that the period of retention would be shorter compared to a customer who takes up the credit facility.

Kadogo Cash must also put in place a policy that allows for the review of all the customers information they have for both active and inactive customers.

Example 2

In the event after signing up with Kadogo Cash Romeo goes ahead and takes up the credit facility and completes repayment within the stipulated timeframes,Kadogo Cash has to notify Romeo how long his information will be held and the purpose of such retention.

One of the justifications for the retention may be compliance with the reporting requirements under the CBK digital credit providers regulations.

DATA SECURITY

In addition to cybersecurity policies, data security measures also include specific organisational and technical measures, such as access and availability control, passwords, physical security, rapid recoverability, encryption, pseudonymization, anonymization, data protection impact assessments, privacy by design and default, training programs and other interventions, which are determined by the type and volume of data processed, the technology being used, and the risks to data subjects. DCPs should also ensure that their employees are continuously trained

and that there are appropriate physical safeguards adopted.

Example

DCPs can enhance security by not only limiting access rights but also regulating user permissions in that, all valid users can access the system but can only access the data and system modules that are useful for their role and no other. i.e. A customer service agent may be given permissions to access a borrower's contact details but not necessarily their credit summary/history.

NOTIFICATION AND COMMUNICATION OF BREACHES

DCPs have to report personal data breaches to the Office without delay within 72 hours of becoming aware of the breach. Where there has been unauthorized access, firms within the digital credit sector are required to communicate to the affected data subjects in writing within a reasonable period, unless the identity of the data subject cannot be established.

To fulfil these and other obligations under Section 43 of DPA, DCPs should have robust breach detection, investigation and internal reporting procedures.

CONTENTS OF A DATA BREACH REPORT

In reporting a data breach to the Office, DCPs need to provide the following:

1. The date on which and the circumstances in which the data controller or data processor first became aware that the data breach had occurred;
2. a chronological account of the steps taken by the data controller or data processor after the data controller or data processor became aware that the data breach had occurred, including the data controller or data processor's assessment that the data breach is a notifiable data breach;
3. details on how the notifiable data breach occurred, where applicable;
4. The number of data subjects or other persons affected by the notifiable data breach;
5. The personal data or classes of personal data affected by the notifiable data breach;
6. The potential harm to the affected data subjects as a result of the notifiable data breach;
7. Information on any action by the data controller or data processor, whether taken before or to be taken after the data controller or data processor notifies the Data Commissionerof the occurrence of the notifiable data breach to—
    i. eliminate or mitigate any potential harm to any affected data subject or otherperson as a result of the notifiable data breach; or
    ii. address or remedy any failure or shortcoming that the data controller or data processor believes to have caused, or enabled or facilitated the occurrence of,the notifiable data breach; the affected individuals or the public that the notifiable data breach has occurred and how an affected data subject may eliminate or mitigate any potential harm as a result of the notifiable data breach; and

iii. contact information of an authorised representative of the data controller or data processor.

EXAMPLE:-

Dante has just been recruited as a Data Protection Officer by Happy Loans. On day one, when he reported for duty he kicked off on a high note. The day in which he reported for work is when a data breach occurred in Happy Loans Company and as a Data Protection Officer he was tasked with the responsibility of advising the Management of Happy Loans how they will handle the situation in accordance with the Data Protection Act, 2019. He was tasked to do an internal memo/ advisory to the management to this effect.

The contents of the internal memo/ advisory to the Happy Loans management should stipulate that the data breach needs to be notified to the Office of the Data Protection Commissioner (ODPC) within 72 hours of becoming aware of the breach. The notification should be made through the ODPC website.

In the event Happy Loans Company had contracted another third party as a data processor and the data processor is the one who becomes aware of the breach, the data processor should notify Happy Loans Company as the data controller as soon as possible but not later than 48 hours of becoming aware of such breach.

Happy Loans Company should also communicate the breach to the data subjects in writing immediately, unless the identity of the data subject cannot be established. This communication to the data subject shall not be required where the data controller or data processor has implemented appropriate security safeguards e.g. encryption of the affected data.

Happy Loans Company must record the following information in relation to the personal data breach:-

- The facts relating to the breach
- Its effects; and
- The remedial action taken.

The breach notification can be filed with the Office in a number of ways, including through a breach notification form accessible through www.odpc.go.ke, by email or a physical delivery to the Office.

DATA PROTECTION OFFICER

A data controller or data processor may designate or appoint a data protection officer in accordance with section 24(1) of the Data Protection Act. The DPO plays a crucial role in ensuring compliance with data protection regulations within the organization. Their responsibilities include overseeing data protection practices, providing advice and guidance on data processing activities, monitoring compliance with the Act, handling data subject rights requests, and acting as a point of contact for data protection authorities and individuals seeking information about the organization's data processing activities. The designation of a DPO demonstrates an entity's commitment to safeguarding personal data and upholding data protection principles.

- A group of entities may appoint a single data protection officer, provided that such officer isaccessible by each entity.

- Where a data controller or a data processor is a public body, a single data protection officer may be designated for several such public bodies, taking into account their organisational structures. 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 relevantacademic 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 officeron the website.
- A Data Controller or a Data Processor who appoints a data protection Officer needs to notify the Office of such appointments.

DUTIES OF A DATA PROTECTION OFFICER

- Advising the data controller or data processor and their employees on data processingrequirements provided under this Act or any other written law;
- Ensuring on behalf of the data controller or data processor that this Act is complied with;
- Facilitating capacity building of staff involved in data processing operations;
- Providing advice on data protection impact assessment; and
- Cooperating with the Data Commissioner and any other authority on matters relating to dataprotection.

EXAMPLE:-

Dante has recently been employed by Happy Loans Company as a Data Protection Officer. When he was interviewing for this position the Happy Loans Company recruitment panel asked him what his roles and duties would be in the event he is successful in getting this position to be the Data Protection Officer for Happy Loans.

The expected answers by the Happy Loans Recruitment panel were:-

1. Ensuring compliance with data protection laws: The DPO is responsible for ensuring that the company's data processing activities comply with relevant data protection laws, such as the Data Protection Act, 2019.
2. Advising on data protection issues: The DPO should be available to provide advice and guidance on data protection issues to the company's employees, customers, and other stakeholders.

1. Conducting Data Protection Impact Assessments (DPIAs): The DPO should lead the company's efforts to identify and mitigate risks to data subjects' privacy rights through conducting DPIAs.

2. Monitoring data protection compliance: The DPO should regularly monitor the company'scompliance with data protection laws and regulations.
3. Responding to data subject requests: The DPO should be responsible for handling data subject requests related to their personal data, such as access requests or erasure requests.
4. Coordinating with data processors: If the company uses third-party data processors to handle personal data, the DPO should ensure that they comply with data protection laws and regulations.
5. Training staff: The DPO should ensure that all employees who handle personal data are trained on data protection laws, regulations, and company policies.
6. Investigating data breaches: In the event of a data breach, the DPO should lead the company's response efforts, including conducting investigations and notifying relevant authorities and data subjects.
7. Maintaining records: The DPO should maintain records of the company's data processing activities and compliance efforts.

Overall, the DPO plays a crucial role in ensuring that the company processes personal data in a lawful and ethical manner, while also protecting the privacy rights of data subjects.

DATA SHARING

Sharing personal data can be advantageous in many ways, but it is also important for organisations to be aware of the risk associated with sharing personal data. The legal framework recognises that personal data can be shared upon the request by another data controller, data processors, third party or a data subject.

There may be instances where DCP may be required to share the personal information they hold or need to share for purposes of business continuity or for compliance with a legal obligation.

To ensure lawful sharing of information with data processors and third parties, digital credit providers (DCPs) must establish secure and reliable data-sharing mechanisms. They need to implement strong data protection measures to safeguard the data they access, including mobile phone records, social media, and financial statements. Compliance with DPA and Regulations is essential to maintain accurate and up-to-date data within formal data-sharing channels like credit bureaus. By ensuring data accuracy and security, DCPs can effectively segment borrowers and offer personalized products while meeting their obligations under data protection laws.

For digital credit and other financial services where sharing of personal data is adopted, there should be a more open and consumer-led data-sharing environment, such as data portability standards that allow consumers to easily access and share their financial histories across providers. Such a system would not only improve consumers' ability to share or restrict the sharing of their data, but would also empower them to ensure the accuracy of their data.

Example

A Digital Credit Provider A may need to share information with another Digital Credit ProviderB for purposes of verification of the identity of customers seeking a digital credit facility. In such an instance, the DCP B will be required to enter into a data sharing agreement with theDCP A requesting or requiring the personal data.

Prior to engaging in the sharing of personal data, the DCP B is expected to determine the purpose and means of sharing between the sharing entities. This should be done within the framework of an agreement. The Agreement should outline provisions on: the purpose for which the personal data is required, the duration for which personal data shall be retained and the proof of safeguards put in place to secure the personal data from unlawful disclosure.

DATA TRANSFER

A data controller or data processor transferring data shall ascertain that the transfer is done in accordance with one or more of the following:

i. Appropriate data protection safeguards;
ii. Transfer as a necessity; or
iii. Consent of the data subject

APPROPRIATE SAFEGUARDS

A transfer of personal data to a third country or a relevant international organisation is based on the existence of appropriate safeguards where:

i. Data protection legislation that essentially equivalent to DPA is binding on the intended recipient;

ii. On assessment of transfers of that type of personal data to the third country or relevant international organisation, the data controller concludes that appropriate safeguards exist to protect the data.

A data controller has the obligation to:

1. Document the transfer;

2. Provide the documentation to the Data Commissioner on request. The documentation must include:

    i. the date and time of the transfer;
    ii. the name of the recipient;
    iii. the justification for the transfer; and
    iv. A description of the personal data transferred.

TRANSFER AS A NECESSITY

Personal data may be transferred to a third country or territory on the basis of necessity if such a transfer is necessary for any of the purpose outlined below:

a) Performance of a contract or contractual obligations
b) Conclusion of performance of a contract in the data subjects interest
c) Public interest
d) Establishment, exercise or defence of a legal claim
e) Data Subjects' vital interest
f) Compelling legitimate interest

Prior to making a transfer on the basis of necessity, a transferring entity shall ascertain that—

i. the transfer is strictly necessary in the specific cases outlined above.
ii. there are no fundamental rights and freedoms of the data subject concerned that overridethe public interest necessitating the transfer.

CONSENT OF THE DATA SUBJECT

In accordance with the Act, in the absence of an adequacy decision, appropriate safeguards or prerequisites for transfer as a necessity, a transfer or a set of transfers of personal data to a third country shall take place only on the condition that the data subject

i. has explicitly consented to the proposed transfer; and
ii. has been informed of the possible risks of such transfer.

A data controller or processor must seek consent from a data subject for the transfer of sensitive personal data, in accordance with section 49 of the Act.

AGREEMENTS

A transferring entity may enter into a written agreement with the recipient of personal data, which shall contain provisions relating to—

a) unlimited access by the transferring entity to ascertain the existence of a robust information system of the recipient for storing the personal data; and
b) the countries and territories to which the personal data may be transferred under the contract.

Example

If a digital lender employs a cloud-based data storage service as a repository to archive data; they can consider employing Transport Layer Security (TLS) to encrypt data whilst in transit so that it cannot be intercepted. The digital lender should also be aware that TLS will only offer adequate security while the data is in transit. The data would typically be in a decrypted state after it was delivered to the cloud service provider. The lender should therefore encrypt each file on its system before uploading.

REGISTRATION

Institutions in the digital credit sector must register as a data controller or data processor. To note, whilst the Act foresees some exemptions to registration, DCPs are subject to mandatory registration regardless of their size and/or their annual turnover/ revenue.

The Office has published a Guidance Note on Registration of Data Controllers and Data Processors which is accessible through www.odpc.go.ke. The Guidance Note includes a step by step guide on how to complete the registration process and the information required during the registration process is available here

PRIVACY BY DEFAULT OR DESIGN

The Data Protection Act, in section 41, outlines the requirement for data controllers and data processors to implement appropriate technical and organisational measures to ensure effective implementation of data protection principles and necessary safeguards in data processing. Additionally, the Act requires that only necessary personal data is processed, taking into account the amount of data collected, the extent of its processing, storage period, accessibility, and cost of processing.

Data protection by design is an approach that ensures data controllers and data processors consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle. Data protection by default requires data controllers and processors to ensure that only data that is necessary to achieve your specific purpose is processed. Data protection by default requires entities to ensure that data protection issues have already been considered and protection methods incorporated into existing systems and practices.This could be achieved by data controllers and processors specifying the personal data required before the processing starts, appropriately informing individuals and only processing the personaldata needed for the specific purpose. Applying appropriate security measures to such data, and its processing environments both at rest and in transit, is vital to ensure the personal data is protected to the highest standards. Security measures should take into account the current state of the art data-security methods and techniques in the field of data processing.

Entities in the digital credit sector should take appropriate security measures to ensure against accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data. These measures include: training in privacy and security; access controls; confidentiality agreements; and physical controls.

In the digital lending sector, appropriate measures could include implementing a robust data protection policy, encrypting data transmission channels, and implementing access controls to protect customers' financial information. For example, a DCP may implement two-factor authentication for customers' accounts, data encryption, password protection for customer accounts and data access controls to ensure only necessary personal data is processed and stored securely.

Taking into account the nature and volume of the data processed and the risks for data subjects, some additional physical and organisational measures that should be adopted, such as:

- physical security of paper files;
- shredding all confidential waste;
- Keeping devices under lock and key when not in use;
- not leaving papers and devices lying around;
- A written information security policy outlining the responsibilities of all staff members inprotecting personal data
- Regular training for all staff members on data protection best practices and the importance of maintaining the confidentiality of personal data
- Regular internal and external audits to assess the effectiveness of technical andorganizational safeguards

Entities should ensure that they are continuously raising awareness on data protection amongst staff and their stakeholders. This should also include raising awareness internally of security measures that their organisation is implementing and the proper procedures for carrying out tasks related to personal data.

ENGAGEMENT OF DATA PROCESSORS

Many entities within the digital credit sector work with vendors/ service providers (data processors) providing different cloud-based and data management solutions, debt collection services among others. DCPs should consider the vendors they engage with and ensure that they opt only for a data processor who provides sufficient guarantees that their data processing will meet the requirements under the Act and protect data subjects' rights. In particular, in instances where data is processed by vendors or service providers, entities in the digital credit sector must remain aware of their ongoing responsibilities as data controllers. Controllers must demonstrate due diligence to establish the vendor's/ service provider's ability to protect personal data confidentiality.

To assist with this, the Act sets out that where an entity engages a vendor or service provider (processor) to process information on its behalf, there must be a written contract stipulating that the processor acts only on the controller's instructions and is bound by the obligations of the controller. Further, both parties should take all reasonable steps to ensure that any person employed by or acting under the authority of the data controller or data processor complies withthe relevant security measures.

In the digital credit sector, data processors may be engaged to handle sensitive personal data such as financial transactions and customer profiles, including spending preferences. The contract between the controller and processor should outline the nature of that data processing, the security measures to be implemented, and the obligation of the processor to assist the controller in meeting their obligations under the Data Protection Act. The contract should also include provisions for liability in case of failure to meet obligations, and auditing and inspection to ensure compliance with data protection regulations.

DATA PROTECTION IMPACT ASSESSMENT

The carrying out of a DPIA is only mandatory where processing is "likely to result in a high risk to the rights and freedoms of data subjects". In cases where it is not clear whether a DPIA is required, it is recommended that a DPIA is carried out nonetheless as a DPIA is a useful tool to help data controllers and/or data processors comply with data protection law. In addition to theaforesaid, the Act requires that all data controllers and processers implement appropriate technical and organisational measures and integrate appropriate safeguards to ensure the adequate protection of personal data of data subjects.

Note

The Office has published a Guidance Note on Data Protection Impact Assessments on www.odpc.go.ke. The Guidance Note includes the form which a Data Protection Impact Assessment should be submitted and guidance on when it should be submitted.

APPENDIX

	Question	YES	No	Comments/ Remedial Action
	We respect the right to privacy as a fundamental human right as provided byArticle 31(c) and (d) of the Constitution.			
	We have identified an appropriate legal basisfor our processing under Section 30 of the Data Protection Act (DPA).			
	If we are processing sensitive data, we have identified permitted grounds under section 44of the DPA			
	We grant the highest degree of autonomypossible with respect to control over theirpersonal data.			
	We restrict processing where the legal basis or legitimate interests ceases to apply.			
	We do not do anything generally unlawful with the personal data or inconsistent purposefor processing.			
	If we are subject to mandatory registration, we have submitted to the Office of Data Protection Commissioner (ODPC) accurate and up-to-date information concerning our processing activities.			
	We have considered how the processing mayaffect the individuals concerned and can justify any adverse impact.			
	We only handle data about individuals in waysthey would reasonably expect, or we can clearly explain why any unexpected processing is justified			
	We do not allow any discrimination or exploitation of the needs or vulnerabilities of adata subject.			

	We do not deceive or mislead people whenwe collect their personal data.			
	We have clearly identified our purpose orpurposes for processing and have clearlydocumented those purposes.			
	We include details of our purposes in ourprivacy notices.			
	We regularly review whether the processing is necessary for the purposes for which the datawas collected and test the design against purpose limitation.			
	If we plan to use personal data for a new purpose, we check that this is compatible withour original purpose, or we obtain specific consent for the new purpose.			
	We use technical measures to limit the possibility of repurposing personal data.			
	We only collect personal data which is adequate, relevant, and limited to what isnecessary for our specified purposes.			
	We can demonstrate the relevance of the datato the processing in question.			
	We periodically review the data we hold, and delete anything we don't need.			
	We avoid the creation of more copies or entrypoints for data collection than is necessary.			
	We ensure that it is not possible to re-identify anonymised data or recover deleted data andtest whether this is possible.			
	We ensure the accuracy of any personal datawe			

	process and the reliability of our sources.			
	We have appropriate processes in place to check and verify the accuracy of the data we collect, and we record the source of that data.			
	We carry out tests for accuracy at criticalsteps.			
	We use technological and organisational design features to decrease inaccuracy and mitigate the effect of an accumulated error in the processing chain.			
	We have a process in place to identify when we need to keep the data updated to fulfil our purpose properly, and we update it as necessary.			
	If we need to keep a record of a mistake, weclearly identify it as a mistake.			
	We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personaldata.			
	As a matter of good practice, we keep a noteof any challenges to the accuracy of the personal data.			
	We know what personal data we hold andwhy we need it.			
	We carefully consider and can justify how longwe keep personal data.			
	We have a policy with standard retention periods where possible.			
	We regularly review our records with a view of identifying personal data that no longer requires to be retained and delete or anonymise such data.			

	We have appropriate processes in place tocomply with individuals' requests for rectification and/or erasure of false or misleading data about them.			
	We clearly identify any personal data that weneed to keep for public interest archiving, scientific or historical research, or statistical purposes.			
	We do not transfer data outside Kenya unlessthere is proof of adequate data protection safeguards or valid consent from the data subject.			
	We checked and fulfilled all conditions setunder part VI of the DPA and Regulations2021.			
	We have clearly identified our purpose orpurposes for processing.			
	We have documented those purposes.			
	We include details of our purposes in ourprivacy notices.			
	If one of the purposes is direct marketing, wemake sure that the data subject is notified that direct marketing is one of the purposes for which personal data is collected or consented to the use of this/her data for the purpose of direct marketing and in any case, is provided with simplified opt-out mechanism.			
	We regularly review whether the processing is necessary for the purposes for which the datawas collected and test the design against purpose limitation.			
	If we plan to use personal data for a new purpose, we check that this is compatible withour original purpose, or we obtain specific consent for the new purpose.			
	We use technical measures to limit the possibility of repurposing personal data.			

	Question	Yes	No	Comments/ Remedial Action
Processing personal data based on consent	Have you reviewed your organisation's mechanisms for collecting consent to ensure that it is freely given, specific, informed and freely given, specific, informed and that it is a clear indication that an individual has chosen to agree to the processing of their data by way of a statement or a clear affirmative action?			
	Are procedures in place to demonstrate that an individual has consented to their data being processed?			
	Are procedures in place to allow an individual to withdraw their consentto the processing of their personal data?			
Processing children's personal data	Are procedures in place to verify the age of a child. Have you obtained consent from a parent/ legal guardian?			
Processing personal data based on legitimate interests	If legitimate interest is a legal basison which personal data is processed,has an appropriate analysis been carried out to ensure that the use ofthis legal basis is appropriate? (That analysis must demonstrate that 1) there is a valid legitimate interest, 2)the data processing is strictly necessary in pursuit of the legitimateinterest, and 3) the processing is notprejudicial to or overridden by the rights of the individual)			

DATA SUBJECTS RIGHTS

	Question	Yes	No	Comments/ Remedial Action
Access to personal data	Is there a documented policy/procedure for handling Data Subject Access Requests?			
	Is your organisation able to respond to Data Subject Access requests within 14 days?			
Data portability	Are procedures in place to provide individuals with their personal data in a structured format, including a machine readable format?			
Deletion and rectification	Are there controls and procedures in place to allow personal data to be deleted or rectified (where applicable)?			
Right to restriction of processing	Are there controls and procedures in place to halt the processing of personal data where an individual has on valid grounds sought the restriction of processing?			
Right to object to processing	Are individuals told about their right to object to certain types of processing such as direct marketing?			
	Are there controls and procedures in place to halt the processing of personal data where an individual has objected to the processing?			

Profiling and automated processing	If automated decision making, which has a legal or significant similar affect for an individual, is based on consent, has explicit consent been collected?			
	Where an automated decision is made which is necessary for entering into, or performance of, a contract, or based on the explicit consent of an individual, are procedures in place to facilitate an individual's right to obtain human intervention and to contest the decision?			
Restrictions to data rights	Have the circumstances been documented in which an individual's data protection rights may be lawfully restricted?			

ACCURACY AND RETENTION

	Question	Yes	No	Comments/ Remedial Action
Purpose Limitation	Are personal data only usedfor the purposes for which they were originally collected?			
Data minimisation	Are the personal data collected limited to what isnecessary for the purposes for which they are processed?			
Accuracy	Are procedures in place to ensure personal data are kept up to date and accurate and where a correction is required, the			
	necessary changes are made without delay?			
Retention	Are retention policies and procedures in place to ensure data are held for no longer than is necessary for the purposes for which they were collected?			
	Do you have procedures inplace to ensure data are destroyed securely, in accordance with your retention policies?			

TRANSPARENCY REQUIREMENTS

	Question	Yes	No	Comments/ Remedial Action
Transparency to data subjects	Are individuals fully informed of how you use their data in a concise, transparent, intelligible and easily accessible form, using clear and plain language?			
	Where personal data are collected directly from the individuals, are procedures in place to ensure you have complied with your duty to notify?			
	Are procedures in place to ensure personal data are kept up to date and accurate and where a correction is required, the			
	necessary changes are made without delay?			
	If personal data are not collected from the subject but from a third party (e.g. shared due to legal obligation) are procedures in place to provide a data protection policy to the individuals?			
	When engaging with individuals, such as when providing a service or CCTV monitoring, are proceduresin place to proactively inform individuals of their data protection rights?			

	s information on how the organisation facilitates individuals exercising their data protection rights published in an easily accessible and readable format?			

OTHER DATA CONTROLLER OBLIGATIONS

	Question	Yes	No	Comments/ Remedial Action
Data Processor Agreements	Have agreements with data processors (such as suppliers and other third parties) processing personal data on yourbehalf been reviewed to ensure			
	all appropriate data protection requirements are included?			
Data Protection Impact Assessments (DPIAs)	If your data processing is considered high risk, do you have a process for identifying the need for, and conducting of,DPIAs? Are these procedures documented?			

DATA SECURITY

	Question	Yes	No	Comments/ Remedial Action
Appropriate technical and organisational security measures	Have you assessed the risks involved in processing personal data and put measures in place to mitigate against them?			

Documented Security Program	Is there a documented process for resolving security related complaints and issues that specifies the technical, administrative and physical safeguards for personal data?			
	Is there a designated individual who is responsible for preventing and investigating security breaches?			
	Are industry standard encryption technologies employed for transferring, storing, and receiving individuals' sensitive personal information?			
	Are personal data systematically destroyed, erased, or anonymised when they are no longer legally required to be retained.			
	Can access to personal data be restored in a timely manner in the event of a physical or technical incident?			

DATA BREACHES

	Question	Yes	No	Comments/ Remedial Action
Data Breach Response Obligations	Does the organisation have a documented privacy and security incident response plan?			
	Are there procedures in place to notify the Office of the Data Protection Commissioner of a data breach?			
	Are there procedures in place to notify data subjects of a data breach?			
	Are plans and proceduresregularly reviewed?			
	Are all data breaches fully documented?			
	Are there cooperation procedures in place between data controllers, data processors and other partners to deal with data breaches?			