OFFICE OF THE DATA PROTECTION COMMISSIONER

Guidance Note on

Emerging Technologies

July 2026

CONTENTS

DEFINITION OF TERMS

"Act" means the Data Protection Act, Cap. 411C.

"Anonymisation" means the irreversible removal of personal identifiers from personal data such that the data subject is no longer identifiable, directly or indirectly.

"Augmented Reality (AR)" means technology that overlays digital information, including images, sounds, or text, onto a user's real-world environment in real time, typically through a device screen or wearable device.

"Autonomous Vehicle (AV)" means a vehicle capable of sensing its environment and operating without human input, relying on sensors, cameras, radar, and artificial intelligence-based processing systems.

"Biometric Data" means personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person which allows or confirms unique identification, including facial images, fingerprints, iris scans, voice patterns, or gait analysis.

"Blockchain" means a distributed ledger technology in which data is recorded in linked, cryptographically secured blocks across a decentralised network of nodes, such that once recorded the data is designed to be immutable.

"Cloud Computing" means the on-demand availability of computing resources, including servers, storage, databases, networking, software, and analytics, over the internet, typically provided by a third-party cloud service provider.

"Connected Vehicle" means a vehicle equipped with internet connectivity and sensors enabling it to communicate with other vehicles, infrastructure, networks, and services, generating and transmitting data about its operation, location, and occupants.

"Data Commissioner" means the person appointed pursuant to Section 6 of the Act.

"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 Localisation" means the requirement that personal data collected within a country be stored and processed within that country's borders or be subject to specific restrictions on cross-border transfer.

"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 Protection Impact Assessment (DPIA)" means a process designed to identify and mitigate data protection risks arising from a processing activity, required under Section 31 of the Act.

"Data Protection Officer (DPO)" means the officer designated pursuant to Section 24 of the Act to advise on and monitor compliance with data protection obligations.

"Data Subject" means an identified or identifiable natural person who is the subject of personal data.

"Distributed Ledger Technology (DLT)" means technology that enables the storage and sharing of data across a decentralised network of participants without a central administrator, of which blockchain is a prominent example.

"Emerging Technology" means a technology that is new or rapidly developing and whose data protection implications are not yet fully addressed in established regulatory guidance, including the Internet of Things, cloud computing, blockchain, biometric recognition systems, immersive technologies, and connected or autonomous vehicles.

"Extended Reality (XR)" means the spectrum of immersive technologies encompassing virtual reality, augmented reality, and mixed reality.

"Federated Cloud" means a cloud computing arrangement in which multiple cloud service providers interconnect their infrastructure, allowing data and workloads to move between cloud environments.

"Internet of Things (IoT)" means the network of physical objects, including devices, vehicles, appliances, and other items, embedded with sensors, software, and connectivity enabling them to collect and exchange data with other systems and devices over the internet.

"Mixed Reality (MR)" means technology that merges the physical and digital worlds, allowing digital objects to interact with the real-world environment in real time.

"Office" means the Office of the Data Protection Commissioner established under Section 5 of the Act.
"Personal Data" means any information relating to an identified or identifiable natural person.

"Privacy by Design and by Default" means the integration of data protection safeguards into the design and default settings of technologies and systems from the outset.

"Processing" means any operation or set of operations performed on personal data, whether or not by automated means, including collection, recording, organisation, storage, adaptation, retrieval, use, disclosure, combination, restriction, erasure, or destruction.

"Pseudonymisation" means the processing of personal data in such a manner that it can no longer be attributed to a specific data subject without additional information kept separately and protected through appropriate technical and organisational measures.

"Regulations" means the regulations made under Section 71 of the Act and related subsidiary legislation.

"Sensitive Personal Data" means data revealing a natural person's race, health status, ethnic or social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details, sex, or sexual orientation.

"Smart Contract" means a self-executing program stored on a blockchain that automatically carries out the terms of an agreement when predetermined conditions are met.

"Virtual Reality (VR)" means technology that immerses users in a fully simulated digital environment, typically experienced through a headset, which may collect physiological, behavioural, and spatial data.

"Wearable Device" means a sensor-enabled device worn on the body that collects and transmits data about the wearer's physiological state, location, activity, or environment.

1. OFFICE

The Office of the Data Protection Commissioner (Office) is a government agency established to protect the privacy and security of personal data in our increasingly digital world. It is responsible for enforcing data protection laws and policies to safeguard the privacy, dignity, and fundamental rights of individuals. The Office is mandated to oversee the implementation and enforcement of the Data Protection Act, 2019, which regulates the processing of personal data of persons located in Kenya by both private and public sector organisations.

The Office plays a vital role in ensuring that individuals have control over their personal data and that organisations respect their 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 is responsible for raising public awareness about data protection issues and educating individuals and organisations on how to protect personal data. With the growing importance of data protection in our digital age, the Office is a critical institution in maintaining trust and confidence in our data-driven society.

The Office is uniquely positioned to facilitate both the government and private sector entities in achieving Government's strategic goals under the "Bottom-Up Economic Transformation Agenda" 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 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.

2. INTRODUCTION

2.1. Background

Emerging technologies are transforming how personal data is collected, used, shared, and stored in Kenya and globally, and in doing so they are directly affecting the protection of personal data. They enable continuous and often invisible collection of personal data, large-scale aggregation and analysis that can reveal sensitive information, complex multi-party processing chains, and extensive cross-border data flows, each of which affects the privacy of data subjects.

The Internet of Things (IoT), for example, connects millions of devices, from smart metres and agricultural sensors to wearable health monitors and connected vehicles, each generating continuous streams of personal data. Cloud computing has become the dominant infrastructure model for data storage and processing, enabling scalable but complex multi-jurisdictional data flows. Blockchain and distributed ledger technologies are being adopted in financial services, land administration, supply chain management, and digital identity, raising novel questions about the permanence and immutability of recorded personal data. Biometric recognition systems are deployed for identity verification, physical access control, and mass surveillance. Immersive technologies are creating new environments in which physiological, spatial, and behavioural data about users is collected in real time. Connected and autonomous vehicles generate granular data about location, movement, and occupant behaviour at scale.

Each of these technologies interacts with data protection law in ways that require specific guidance. While the Data Protection Act provides a technology-neutral framework of principles and obligations

that applies to all processing of personal data, the application of those principles and obligations to the specific characteristics of emerging technologies raises interpretive and practical questions that this Guidance Note addresses.

Kenya's National Digital Master Plan and the Bottom-Up Economic Transformation Agenda create conditions of rapid technology adoption across both public and private sectors. The data protection implications of this acceleration shall be addressed proactively and systematically.

2.2. Privacy Issues and Concerns

Emerging technologies raise the following cross-cutting privacy and data protection concerns, in addition to the technology-specific concerns addressed in later sections of this Guidance Note:

- **Ubiquitous and invisible data collection:** Many emerging technologies collect personal data continuously, automatically, and without the active engagement of data subjects, making informed consent and meaningful transparency structurally challenging.
- **Data aggregation and inference:** Personal data collected by emerging technologies individually innocuous can be combined to generate sensitive inferences about data subjects' health, behaviour, location, associations, and financial status.
- **Complexity of data controller and data processor relationships:** Emerging technology ecosystems frequently involve multiple parties device manufacturers, platform operators, application developers, cloud providers, and analytics services each processing personal data in the same chain, creating uncertainty about the allocation of data protection responsibilities.
- **Cross-border data flows:** Emerging technology infrastructure is predominantly global. Data collected by a device in Nairobi may be stored in servers in Europe, analysed by a platform in the United States, and monetised by a service provider in Asia, often without the data subject's awareness.
- **Security vulnerabilities:** Emerging technologies, particularly IoT devices, frequently have limited computational capacity for security controls, are rarely updated, and are often deployed in environments without adequate cybersecurity governance, creating significant breach risk.
- **Immutability and erasure:** Technologies such as blockchain are designed to be tamper-resistant and immutable, creating fundamental tension with the data subject's right to erasure under the Act.
- **Novel categories of data:** Emerging technologies generate new categories of data such as biometric data, geolocation trails, behavioural patterns, and physiological signals that may constitute sensitive personal data requiring heightened protections.
- **Children's personal data:** Emerging technologies, including connected toys, gaming and immersive platforms, and educational technologies, are widely used by and collect personal data about children, requiring heightened protections under Section 33 of the Act.

2.3. Scope and Purpose of Guidance Note

The purpose of this Guidance Note is to provide data controllers, data processors, technology developers, and deployers with an understanding of their obligations under the Data Protection Act and the attendant Regulations when developing, deploying, or operating systems using emerging technologies that process personal data of persons located in Kenya.

This Guidance Note applies to all entities, whether public or private, that deploy or operate the following categories of emerging technology in a manner that involves processing of personal data:

- Internet of Things systems;
- cloud computing services;
- blockchain and distributed ledger technologies;
- biometric recognition systems;
- immersive and extended reality technologies;
- connected and autonomous vehicles; and
- unmanned aircraft systems (UAS)/drones.

The list is illustrative and not exhaustive; the Office may issue updated or supplementary guidance as further emerging technologies attain sufficient deployment in Kenya to warrant specific treatment.

This Guidance Note should be regarded as a minimum standard. Entities operating in regulated sectors shall additionally comply with applicable sector-specific data protection guidance and sector regulator requirements.

3. LEGISLATIVE FRAMEWORK

The deployment of emerging technologies in Kenya is governed by the following legislative and regulatory framework, including but not limited to:

i) The Constitution of Kenya, 2010

Article 31 guarantees the right to privacy, including in respect of information relating to a person's family or private affairs. Article 43 recognises social and economic rights that emerging technologies used in public service delivery shall not undermine. Article 27 prohibits discrimination, which is relevant to the use of biometric and profiling technologies. Article 35 guarantees the right of access to information held by the state, which intersects with blockchain-based government data systems.

ii) The Data Protection Act

The Act applies in full to all processing of personal data by or through emerging technologies. Every emerging technology deployment shall comply with the Act in its entirety, including the data protection principles, the requirements for lawful processing, the rights of data subjects, the obligations of data controllers and data processors, the restrictions on the cross-border transfer of personal data, and the enforcement provisions of the Act.

iii) The Data Protection (General) Regulations, 2021

These Regulations give detailed effect to the Act's principles and obligations, including the content requirements for privacy notices, the conditions for obtaining valid consent, the mandatory content of agreements between data controllers and data processors, and the framework for data protection impact assessments. All these provisions apply to emerging technology deployments.

iv) The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021

These Regulations set out the requirements and procedure for the registration of data controllers and data processors, which apply to entities that develop, deploy, or operate emerging technology systems processing personal data.

v) The Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021

These Regulations set out the procedure for lodging, admitting, and determining complaints and the enforcement mechanisms available to the Office, all of which apply to complaints arising from emerging technology deployments.

vi) Sector-specific laws and international best practices

Emerging technology deployments are further governed by applicable sector-specific laws and regulations, including, among others, the Civil Aviation Act, Cap 394 and the Civil Aviation (Unmanned Aircraft Systems) Regulations, 2020 in respect of drones; the Computer Misuse and Cybercrimes Act, 2018; and the Kenya Information and Communications Act, Cap 411A. Entities should also have regard to international best practices and comparative technology governance frameworks.

4. APPLICATION OF DATA PROTECTION PRINCIPLES TO EMERGING TECHNOLOGIES

All processing of personal data by or through emerging technologies shall comply with the data protection principles under Section 25 of the Act. This section addresses the specific application of each principle to the emerging technology context.

4.1. Lawfulness, Fairness, and Transparency

Emerging technologies often collect personal data automatically, continuously, and from data subjects who may not be aware that collection is occurring. The transparency principle requires that entities deploying such technologies provide clear, accessible, and intelligible disclosure of the data collection and processing activities at the point of deployment.

Where physical devices are involved, privacy notices shall be accessible through accompanying applications, websites, or physical signage, as appropriate to the deployment context.

Fairness requires that personal data collected through emerging technologies is not used in ways that would be unexpectedly harmful or disadvantageous to data subjects.

Entities shall assess whether the use cases for emerging technology data collection are within the reasonable expectations of data subjects at the time of deployment.

Example

Bahari Smart City deploys environmental sensors and smart lighting across a residential area of a County. Some sensors incidentally collect data about pedestrian movements. The City authority shall:

- identify a lawful basis for any personal data processing;
- publish accessible privacy notices including on signage at entry points to the smart area disclosing what data is collected, for what purpose, and for how long; and
- ensure the processing is proportionate and within the reasonable expectations of residents.

4.2. Purpose Limitation

Data collected by emerging technologies for one purpose, for example, smart metre energy consumption monitoring shall not be repurposed for a different, incompatible use, such as insurance risk scoring, credit risk scoring, or marketing, without a fresh legal basis.

The ease with which data from emerging technologies can be aggregated and analysed makes purpose creep a significant risk.

Entities shall define and document the specific purpose of each data collection activity at the point of system design.

4.3. Data Minimisation

Many emerging technologies can collect far more data than is necessary for their stated purpose. IoT devices may collect high-frequency sensor readings when periodic readings would suffice. Connected vehicles may store detailed journey logs when only aggregate movement data is required. Biometric systems may capture and retain full biometric templates when only one-to-one matching is needed at the point of authentication.

Entities shall implement data minimisation at the system design stage: collecting only the data that is adequate, relevant, and limited to what is necessary for the specific, documented purpose.

4.4. Accuracy

Emerging technologies can generate, store, and transmit inaccurate data at scale. Sensor drift, calibration errors, and connectivity failures can produce inaccurate readings. Biometric recognition systems can produce false positives or false negatives.

Entities shall implement quality controls to detect and correct inaccurate data and shall provide mechanisms for data subjects to request rectification of inaccurate personal data.

4.5. Storage Limitation

The high data volumes generated by emerging technologies create pressure to retain data indefinitely on the assumption that it may prove useful in the future. This is inconsistent with the storage limitation principle.

Entities shall establish and enforce data retention policies that specify the maximum period for which personal data generated by each emerging technology will be retained, the criteria used to determine that period, and the processes for deletion or anonymisation of data that has reached the end of its retention period.

4.6. Integrity and Confidentiality

Emerging technologies, particularly IoT devices, are frequently vulnerable to cybersecurity attack. Many devices have limited computational resources for security controls, are shipped with default or weak credentials, receive infrequent security updates, and are deployed in environments with poor network security.

Entities shall implement appropriate technical and organisational security measures calibrated to the risk profile of the emerging technology deployment, including:

- device authentication and access control;
- encryption of data in transit and at rest;
- network segmentation;

- regular security patching and firmware update management; and
- intrusion detection and incident response capabilities.

4.7. Accountability

Entities deploying emerging technologies bear accountability for data protection compliance throughout the technology lifecycle. In multi-party technology ecosystems such as IoT platforms, cloud environments, and blockchain networks entities shall clearly document and contractually establish the allocation of data protection responsibilities among all parties in the processing chain.

Accountability in the emerging technology context requires the following, but not limited to:

- DPIA before deployment;
- DPO engagement where required;
- records of processing activities that document each emerging technology deployment; and
- ongoing compliance monitoring.

5. INTERNET OF THINGS (IoT)

The Internet of Things encompasses a vast and growing ecosystem of connected devices that collect, transmit, and process data in real time.

IoT deployments span consumer products (smart home devices, wearables, connected appliances), industrial systems (agricultural sensors, smart metres, manufacturing monitors), healthcare (remote patient monitoring devices, connected medical equipment), public infrastructure (traffic sensors, smart lighting, environmental monitors), and financial services (point-of-sale devices, ATMs, connected payment terminals).

Many IoT systems process personal data continuously, automatically, and without active data subject engagement.

5.1. Data Protection Concerns in IoT

- **Continuous and ambient data collection:** IoT devices collect data around the clock, often in intimate settings such as the home, the workplace, or the body, where data subjects have a heightened expectation of privacy.

Example

Shamba Smart, an agri-tech company, deploys soil sensors, weather stations, and drone imagery systems across smallholder farms in the Rift Valley. These systems collect location data, farm productivity data, and, through drone imagery, may incidentally capture images of farm workers and residents.

Shamba Smart shall:

- identify the lawful basis for processing farmer and worker personal data (likely a combination of contract with participating farmers and, for incidental worker data, legitimate interests subject to a Legitimate Interests Assessment);
- provide a privacy notice to farmers and affected workers;
- conduct a DPIA;
- implement data minimisation, for example, by blurring identifiable persons in drone imagery; and

- secure data transmission from sensors to the platform using encryption.

Entities that manufacture IoT devices for the Kenyan market, or that supply IoT device management platforms used by Kenyan deployers, should note that the Act applies to the processing of personal data of persons located in Kenya regardless of where the manufacturer or platform operator is established.

6. CLOUD COMPUTING

Cloud computing has become the dominant infrastructure model for data storage and processing in Kenya. Government agencies, financial institutions, healthcare providers, educational institutions, and businesses of all sizes rely on cloud services to store, process, and transmit personal data.

Cloud service models, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) involve varying degrees of shared responsibility for data protection between the cloud customer (typically acting as data controller) and the cloud service provider (typically acting as data processor).

6.1. Data Protection Concerns in Cloud Computing

- **Shared responsibility uncertainty:** Cloud customers frequently misunderstand the boundary between their data protection responsibilities and those of the cloud provider. The cloud provider's security of the underlying infrastructure does not relieve the customer of responsibility for the security and lawful processing of personal data stored in the cloud.
- **Limited visibility and control:** Entities may have limited visibility into how personal data is processed, accessed, or secured within cloud environments, making it difficult to ensure compliance with data protection obligations.
- **Foreign government access risks:** Personal data stored in foreign cloud infrastructure may be subject to disclosure or access requests under the laws of other jurisdictions, potentially affecting the privacy and confidentiality of data subjects.
- **Sub-processor chains**: Cloud providers frequently engage sub-processors, including content delivery networks, database providers, and monitoring services that may also process personal data. Cloud customers shall ensure they have visibility and contractual control over sub-processor engagement.
- **Data portability and vendor lock-in**: The ability of data subjects to exercise their right to data portability may be compromised if personal data is stored in proprietary cloud formats that cannot be exported.
- **Data retention and deletion:** Cloud environments can make it difficult to ensure that all copies of personal data including backups, snapshots, and replicated data are deleted upon expiry of the retention period or upon a valid erasure request.

Example

Afya Digital, a private hospital chain, migrates its patient records management system to a cloud-based SaaS platform operated by an international provider whose servers are located in the European Union and the United States.

Afya Digital shall:

- enter into a data processing agreement with the SaaS provider;
- assess the adequacy of data protection in the EU (likely adequate) and the US (requires additional safeguards);
- implement contractual safeguards for US transfers;
- conduct a DPIA given the sensitivity of health data and the scale of processing;
- ensure the DPO is involved in the migration decision; and
- verify that the SaaS provider's sub-processor list does not include any processor in a jurisdiction lacking adequate data protection without appropriate safeguards.

The Office notes that data localisation considerations may arise in specific contexts, including for data relating to the strategic interests of the state. Entities processing personal data in connection with critical national infrastructure, national security, or strategic government functions should assess whether applicable law or policy imposes data localisation requirements that may constrain cloud deployment options.

Data controllers and data processors that adopt or utilise cloud computing services should also ensure that their cloud environments and service providers comply not only with the requirements of the Data Protection Act and its attendant regulations, but also with the Kenya Cloud Policy. Compliance with the Kenya Cloud Policy promotes secure, resilient, and accountable cloud adoption by requiring appropriate governance, data classification, cybersecurity safeguards, data residency and sovereignty considerations, contractual protections, vendor due diligence, and ongoing risk management. Adherence to both frameworks enables organisations to protect personal data while supporting Kenya's digital transformation agenda through responsible and trusted cloud computing.

7. BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGIES

Blockchain and distributed ledger technologies (DLT) are being adopted across a range of sectors, including financial services (digital currency, payment systems, trade finance, and microfinance), land administration (digital land registries), supply chain management, digital identity verification, and public procurement.

DLT's defining characteristics, decentralisation, transparency, and immutability create fundamental tension with several data protection principles and data subject rights under the Act, particularly the right to erasure, the right to rectification, and the principle of storage limitation.

7.1. Data Protection Concerns in Blockchain and DLT

- **Immutability and the right to erasure:** Blockchain is architecturally designed to prevent the alteration or deletion of recorded data. This is in direct tension with the data subject's right to erasure under the Act, which requires the deletion of personal data when the conditions for erasure are met. Where personal data is recorded on a blockchain, whether in transactions, smart contracts, or associated metadata, technical erasure may be impossible.
- **Pseudonymity and re-identification:** Blockchain addresses and transaction identifiers are pseudonymous rather than anonymous: they can be linked to real-world identities through transaction analysis, exchange records, or linkage with off-chain data. Personal data on a public blockchain shall be treated as personal data for the purposes of the Act.

- **Distributed data controllership:** In a decentralised blockchain network, the determination of who is the data controller responsible for compliance with the Act is not straightforward. Multiple participants in the network may jointly determine the purposes and means of processing, giving rise to joint controller obligations.
- **Public blockchain transparency:** Personal data recorded on a public blockchain is visible to all network participants. This is inconsistent with the Act's requirement for confidentiality and purpose limitation and may result in inadvertent disclosure of personal data to parties with no lawful basis for access.

Case Study: Blockchain Land Registry, Data Protection Obligations

The government implements a blockchain-based land title registry to prevent fraudulent land transactions. Land ownership records include personal data such as names, national ID numbers, and plot details. The government shall:

- assess whether personal data should be stored on-chain or whether the blockchain should store only hashes of records with personal data held in a conventional database;
- identify a lawful basis for recording personal data on the blockchain (likely public task or legal obligation);
- conduct a DPIA addressing the immutability-erasure tension;
- implement access controls that limit on-chain data visibility to authorised parties (a permissioned rather than public blockchain architecture); and
- establish a process for addressing rectification requests where on-chain data is inaccurate.

7.2. Smart Contracts and Personal Data

Smart contracts that automatically process personal data, for example, to execute payment obligations triggered by verified identity or asset transfer conditions are subject to the Act's full data protection obligations. Entities deploying smart contracts that process personal data shall identify the lawful basis for processing, ensure transparency to data subjects about smart contract processing, and assess whether the automated execution of smart contracts constitutes automated decision-making under Section 35 of the Act.

8. BIOMETRIC RECOGNITION SYSTEMS

Biometric recognition systems are deployed across Kenya in identity registration and credentialing examples include

- Huduma Namba and the successor Maisha Namba;
- passport issuance;
- voter registration,
- in financial services (mobile-money customer onboarding, banking know-your-customer (KYSC),
- in social protection and health (former NHIF and now SHA enrolment as well as across the health insurance industry),
- in education (examination integrity, school attendance),
- in employment (time-and-attendance, secure-area access),

- in retail and hospitality (loss prevention, loyalty), and
- in policing and public-space surveillance.

Biometric recognition systems process biometric data , which is defined under the Act as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allows or confirms unique identification, it is also classified as sensitive personal data under Section 2 of the Act, attracting heightened protections.

This section provides additional guidance specific to biometric recognition. It applies in addition to the general obligations applicable to all emerging-technology deployments set out earlier in this Guidance Note.

8.1. Classification : Verification, Identification, and Surveillance

The data-protection risks of biometric processing depend critically on the type of matching being performed. Entities shall identify, before deployment, which of the three matching modes their system performs, and shall apply the corresponding safeguards. A system that combines modes (for example, performs 1:1 verification at the device but transmits templates to a 1:N database) shall be treated as performing the higher-risk mode.

8.2. Verification (one-to-one matching, 1:1)

Verification answers the question: "Is this person who they claim to be?" The data subject presents a claimed identity (a card, a number, a username) together with a fresh biometric sample, and the system compares that sample against a single stored reference template associated with that claimed identity. Examples include unlocking a mobile phone with a fingerprint, confirming a banking customer's identity at branch onboarding, and authenticating an employee at a building access point. Verification is the lowest-risk mode because the comparison is bounded (limited to one subject), the data subject is engaged (knows), and the system does not attempt to identify the person from a population.

8.3. Identification (one-to-many matching, 1:N)

Identification answers the question: "Who is this person, out of a known population of N enrolled persons?" A fresh biometric sample is compared against a database of stored templates to find a match. Examples include de-duplication checks during national-identity enrolment, attendance systems that identify staff without a card, and search of a forensic database. Identification is materially higher risk than verification because (i) it requires a centralised template database, (ii) false-match rates compound with database size, and (iii) the system can in principle identify any enrolled person without their active cooperation.

8.4. Surveillance / mass identification (N:N or open-set N:1)

Surveillance biometrics attempts to identify, recognise, or characterise individuals in an environment that they have not deliberately entered for the purpose of being identified for example, live facial recognition in public spaces, voice recognition in call queues, The matching may be open-set (the captured person may not be enrolled at all) and is typically unconsented. Surveillance biometrics is the highest-risk mode, raises the most concerns under the Act and the Constitution, and is treated as such in the obligations below.

8.5. Data Protection Concerns in Biometric Recognition Systems

- Sensitive and irreversible: Biometric data is sensitive personal data and a breach is irreversible — the data subject cannot reissue their face, fingerprint, iris, voice or gait.
- Function creep: Systems deployed for one purpose (for example, time and attendance) tend to acquire further uses (for example, performance monitoring or law-enforcement cooperation) without fresh lawful basis.
- Centralised template stores: Population-scale identification systems require centralised databases that become high-value targets and create the conditions for mass surveillance.
- Demographic accuracy disparities: False-match and false-non-match rates differ across skin tone, gender, age and other characteristics, with potential discriminatory consequences.
- Inferred sensitive data: Biometric features can be used to infer further sensitive personal data, including health conditions, age, ethnicity, gender identity, sexual orientation and emotional state. Such inferences are themselves sensitive personal data.
- Children and vulnerable groups: Biometric processing of children raises specific concerns under Section 33 of the Act, including the immaturity of features, the long horizon of the data, and the difficulty of meaningful consent.

Example

XYX Manufacturing wishes to replace its access cards with a fingerprint-based time and attendance system covering 1,200 employees at three sites. The vendor proposes a centralised database of fingerprint templates accessible by HR, security, and the vendor's offshore support team.

XYZ Manufacturing shall:

(a) recognise that fingerprint data is sensitive biometric personal data and that the employer-employee relationship is a context of significant power imbalance, so consent is unlikely to be freely given;

(b) identify whether a specific statutory basis exists (it does not, for routine attendance);

(c) re-scope the deployment to 1:1 verification at each access point with on-device or match-on-card matching, and a non-biometric fallback (a card, or supervisor sign-in) available without disadvantage;

(d) avoid creating a centralised template database: each employee's template is stored on a smartcard they carry and is matched locally at the device;

(e) conduct a DPIA addressing template protection, accuracy and equity across the workforce demographic (skin tone, age, manual-labour fingerprint wear), and the proportionality of biometric processing for the stated purpose;

(f) test the system's false-non-match rate on a representative sample of the workforce, document any disparity across demographic groups, and ensure the fallback is genuinely usable;

(g) execute a data processing agreement with the vendor that prohibits use of employee biometric data for vendor model training and prohibits offshore access to template data without specific authorisation;

(h) provide employees with a privacy notice in plain language in Kiswahili and English, including the route to opt for the fallback without detriment; and

(i) implement secure deletion of any template on an employee's exit, including from issued smartcards.

9. IMMERSIVE TECHNOLOGIES: VIRTUAL, AUGMENTED, AND EXTENDED REALITY

Virtual reality (VR), augmented reality (AR), mixed reality (MR), and the broader spectrum of extended reality (XR) technologies are creating new environments immersive, interactive, and experiential in which personal data is collected in fundamentally new ways.

XR technologies are emerging in education, healthcare training, tourism, gaming, retail, and enterprise training applications. The personal data generated by XR systems includes not only conventional identifiers but also novel categories: precise spatial positioning, eye movement tracking, body movement and gesture data, physiological responses (heart rate, galvanic skin response), and fine-grained behavioural data that can reveal highly sensitive information about a user's health, psychological state, and personal characteristics.

9.1. Data Protection Concerns in Immersive Technologies

- **Novel and highly sensitive data categories**: XR systems collect biometric-grade physiological and behavioural data that can be used to infer health conditions, emotional states, personality traits, and socioeconomic status, even where users are not aware of this inference potential.
- **Immersive environments and meaningful consent:** The immersive, engaging, and sometimes addictive nature of XR environments makes it difficult for users to maintain the detached awareness needed for meaningful informed consent to data collection.
- **Persistent and pervasive collection:** Wearable XR headsets and AR devices can collect continuous data about a user's physical environment, including the presence of other individuals who have not consented to data collection.

Example

EduVR, a Nairobi-based edtech company, deploys a VR platform for secondary school students that tracks students' gaze patterns, movement, and engagement levels during virtual lessons. The company shall:

- recognise that gaze tracking data constitutes biometric data (sensitive personal data);
- establish explicit consent from parents or guardians, given the students are minors as the lawful basis;
- conduct a DPIA;
- provide parents and students with a privacy notice in plain, age-appropriate language;
- implement data minimisation, collecting engagement metrics rather than raw biometric data where the educational purpose can be served; and
- prohibit any use of the biometric data for commercial profiling.

10. CONNECTED AND AUTONOMOUS VEHICLES

Connected vehicles are becoming increasingly prevalent, including passenger vehicles equipped with internet connectivity, GPS navigation, and telematics systems, as well as commercial fleet management systems, ride-sharing platforms, and, on a horizon basis, autonomous vehicle deployments. Connected vehicles generate large volumes of personal data: precise and continuous location data, journey histories, driving behaviour data (speed, acceleration, braking, cornering), in-cabin audio and video data, occupant identification data, and, in some systems, biometric data for driver monitoring and authentication.

10.1. Data Protection Concerns in Connected Vehicles

- **Location and movement data:** Continuous GPS tracking creates a granular record of an individual's movements, associations, and daily routines that can reveal sensitive information about health, religion, political activity, and personal relationships.
- **Multiple data subjects:** A connected vehicle may carry multiple occupants, each of whom is a data subject whose personal data including location and, where in-cabin systems are active, audio and video is being processed. Data collection obligations run to all occupants, not only the vehicle owner or registered driver.
- **Fleet management and employee monitoring:** Commercial fleet telematics systems that track driver behaviour and location are a form of employee monitoring, raising questions about proportionality, transparency, and the power imbalance between employer and employee.

Example

Safari Rides, a ride-sharing company, collects GPS location data, driver behaviour data, and passenger journey data through its platform. The company shall:

- provide a privacy notice to drivers and passengers at the point of registration and in the application;
- identify the lawful basis for each category of data (contract for journey data;
- legitimate interests, subject to LIA for driver behaviour monitoring);
- conduct a DPIA given the scale and sensitivity of location processing;
- implement data retention limits on journey history;
- assess cross-border transfer obligations if journey data is processed on servers outside Kenya; and
- ensure that driver monitoring data is not used for automated disciplinary decisions without a human review mechanism.

11. LAWFUL BASIS FOR PROCESSING PERSONAL DATA IN EMERGING TECHNOLOGY CONTEXTS

Every processing operation conducted through or in connection with an emerging technology shall have a valid lawful basis under Section 30 of the Act.

The lawful bases are: consent of the data subject; necessity for the performance of a contract to which the data subject is a party; compliance with a legal obligation to which the data controller is

subject; protection of the vital interests of the data subject or of another person; performance of a task carried out in the public interest or in the exercise of official authority; and the pursuit of the legitimate interests of the data controller or a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject.

The following table sets out guidance on the application of each lawful basis to emerging technology processing activities generally, with illustrative examples:

Lawful Basis	**Application to Emerging Technologies**	**Key Limitations**
Consent	Appropriate where data subjects have a genuine and free choice about the processing. Examples include consumer IoT devices; XR platforms; optional biometric authentication; and connected vehicle passenger data, among other comparable applications	Shall be freely given, specific, informed, unambiguous; not appropriate where there is significant power imbalance (e.g., employer-employee IoT monitoring) or where consent is a condition of a non-negotiable service
Contract	Appropriate where the processing is objectively necessary to perform a contract with the data subject. Examples include cloud services for contract management; fleet telematics for logistics performance; and IoT systems for supply chain monitoring, among other comparable applications	Extends only to processing objectively necessary for the contract; does not justify ancillary processing the entity finds convenient
Legal Obligation	Appropriate where a specific law requires the processing. Examples include anti-money laundering transaction monitoring; biometric voter registration under electoral law; and vehicle telematics data required by transport regulators, among other comparable applications	The legal obligation shall be specific and clearly impose the processing requirement; general legal obligations do not authorise all processing connected with compliance
Vital Interests	Appropriate where processing is necessary to protect life or health. Examples include emergency health IoT monitoring and disaster response location tracking, among other comparable applications	Reserve for genuine life-threatening situations where no other basis is available
Public Task / Official Authority	Appropriate where processing is necessary for a statutory public function.	Public entities shall identify the specific statutory task or authority; shall still

	Examples include smart city infrastructure; government registries; public sector deployments in health, education, and infrastructure; and national identity systems, among other comparable applications	comply with all other data protection principles
Legitimate Interests	Appropriate where a documented balancing of interests favours the processing. Examples include telematics for commercial logistics safety; security monitoring in enterprise environments; and fraud detection systems, among other comparable applications	Requires documented Legitimate Interests Assessment (LIA); unlikely to be adequate for high-risk processing involving sensitive data or systematic monitoring of individuals in personal contexts

12. RIGHTS OF DATA SUBJECTS IN EMERGING TECHNOLOGY CONTEXTS

The data subject rights provided by the Act apply with full force to personal data processed through emerging technologies. Entities shall implement technical and procedural mechanisms that enable data subjects to effectively exercise each right in the emerging technology context.

The rights of data subjects are not absolute and may be limited in accordance with the Act, including under the exemptions set out in the Act, and a request may be declined where it is manifestly unfounded or excessive.

Entities shall respond to data subject requests within the timelines prescribed under the Act and the Data Protection (General) Regulations, 2021. Where a request is declined, the entity shall notify the data subject of the refusal in writing, with reasons, within the prescribed period.

12.1. Right to Be Informed

The transparency obligation under Section 29 of the Act requires that data subjects are informed of emerging technology processing at the point of data collection. In practice, the often ambient and continuous nature of emerging technology data collection makes compliance with this obligation structurally challenging. Entities shall:

- for consumer IoT devices: provide privacy notices through device setup processes, companion applications, and product packaging;
- for public space IoT (smart city sensors, surveillance cameras): provide privacy notices through prominent on-site signage and publicly accessible online notices;
- for cloud-hosted services: provide clear privacy notices at the point of service subscription and through user interfaces;
- for blockchain-based services: provide privacy notices that specifically disclose the immutability of on-chain data and its implications for erasure and rectification rights; and
- for XR platforms: provide in-experience privacy notices that are accessible within the immersive environment.

12.2. Right of Access

Data subjects are entitled to access the personal data processed about them through emerging technologies. Entities shall implement technical mechanisms that enable data subjects to obtain a copy of their personal data in a commonly used, machine-readable format, including data generated by IoT devices, stored in cloud environments, and recorded on blockchain-based systems. For blockchain data, entities shall be able to supply data subjects with the personal data recorded on-chain in a readable format, even where the on-chain record cannot be altered.

12.3. Right to Rectification

Data subjects have the right to have inaccurate personal data rectified. For most emerging technologies, rectification of off-chain data is technically straightforward.

For blockchain-based systems, where on-chain data cannot be altered, entities shall implement compensating mechanisms: for example, recording a corrective entry on the blockchain that supersedes the inaccurate record, or maintaining an off-chain authoritative record that overrides the on-chain data.

12.4. Right to Erasure

The right to erasure presents the most significant challenge in the emerging technology context, particularly for blockchain systems. Where erasure conditions are met under the Act, entities shall:

- **for IoT and cloud systems**: implement automated deletion processes that erase personal data from all storage locations, including backups and replicated copies, upon expiry of the retention period or upon a valid erasure request;
- **for blockchain systems:** where technical erasure of on-chain data is not feasible, implement cryptographic deletion (destruction of encryption keys rendering the data functionally inaccessible) or record amendment (recording a superseding entry that voids the personal data content of the original record), and document the technical impossibility and compensating measure adopted; and
- **for XR systems:** implement mechanisms to delete behavioural and physiological session data upon user request, including deletion from any analytics or training datasets derived from the session data.

12.5. Right to Data Portability

Data subjects have the right to receive personal data they have provided to a controller in a structured, commonly used, machine-readable format. For IoT systems, this includes sensor data and usage logs generated by the device. For cloud-based services, entities shall ensure that personal data can be exported in an interoperable format and not locked into proprietary systems. The right to portability is particularly relevant to connected vehicle operators, who hold journey and behaviour data generated by the data subject's use of the vehicle.

12.6. Right Not to Be Subject to Automated Decision-Making

Where emerging technology systems produce decisions that significantly affect data subjects through automated means, including IoT-based insurance telematics scoring, biometric access control decisions, or AI-embedded decisions in XR or connected vehicle systems Section 35 of the Act applies. Entities shall implement human review mechanisms, provide explanations of automated decisions upon request, and enable data subjects to contest automated outcomes.

13. OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS

13.1. Registration

All entities that develop, deploy, or operate emerging technology systems that process personal data of persons located in Kenya shall register with the Office as data controllers or data processors in accordance with the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021. Entities procuring emerging technology systems from third-party vendors shall assess whether the vendor is acting as a data processor and ensure the vendor is registered and subject to a compliant data processing agreement.

13.2. Privacy by Design and Default

Privacy by design and default requires that data protection safeguards are embedded into emerging technology systems from the design stage. In the emerging technology context, examples of privacy by design and default include, among others:

- selecting the least privacy-invasive technology architecture capable of achieving the stated purpose (for example, edge computing in IoT systems to minimise data transmission; off-chain storage in blockchain systems; permissioned rather than public blockchains; privacy-preserving computation in XR platforms);
- configuring emerging technology systems to default to the most privacy-protective settings available without requiring user action;
- implementing automatic data deletion at the expiry of defined retention periods;
- building data subject rights interfaces into emerging technology platforms as core system features; and
- including data protection requirements in technology procurement specifications and vendor contracts; and
- implementing age verification, parental consent, and age-appropriate, privacy-protective default settings where an emerging technology system is likely to process children's personal data, for example a connected toy or an educational XR platform.

13.3. Data Protection Impact Assessment

A DPIA is required before deploying any emerging technology system that is likely to result in high risk to the rights and freedoms of data subjects. Processing of personal data using new technologies is considered high-risk processing. Accordingly, all emerging technology deployments that involve the processing of personal data are subject to a DPIA. Such deployments include:

- IoT systems involving large-scale processing of personal data, systematic monitoring of individuals, or processing of children's data;
- cloud migrations involving sensitive personal data or large volumes of personal data;
- any blockchain system recording personal data;
- all biometric recognition system deployments;
- XR systems collecting physiological, biometric, or behavioural data;
- connected vehicle systems involving systematic location tracking of individuals; and
- smart city or public space surveillance deployments.

The Office has published a Guidance Note on Data Protection Impact Assessments accessible at www.odpc.go.ke. Entities shall consult that Guidance Note when conducting DPIAs for emerging technology systems.

13.4. Data Protection Officer

Entities whose core activities involve large-scale systematic monitoring of data subjects through emerging technology systems, including IoT monitoring platforms, biometric recognition systems, connected vehicle fleet operators, and smart city infrastructure operators or large-scale processing of sensitive personal data through such systems, shall designate a DPO under Section 24 of the Act. The DPO shall be involved in all DPIA processes, technology procurement decisions, and data subject rights responses relating to emerging technology systems.

13.5. Data Sharing and Processor Agreements

Emerging technology ecosystems involve complex webs of data sharing between manufacturers, platform operators, application developers, cloud providers, analytics services, and third-party partners. Entities shall:

- map all data flows in the emerging technology ecosystem, identifying each party that processes personal data and their role as controller, joint controller, or processor;
- enter into compliant data processing agreements with all data processors in the ecosystem; and
- implement data sharing agreements with any party that receives personal data as a controller in its own right, ensuring the sharing has a documented lawful basis.

13.6. Breach Notification

Entities shall implement breach detection, containment, and notification procedures specific to their emerging technology systems. The Office shall be notified of any personal data breach likely to result in risk to data subjects within 72 hours of the entity becoming aware. Affected data subjects shall be notified without undue delay where the breach is likely to result in high risk to their rights and freedoms. Given the scale and sensitivity of data processed by many emerging technology systems, breach notification procedures shall be tested regularly and integrated into the entity's broader incident response capability.

13.7. General Obligations for Emerging Technology Deployments

The following obligations apply to every entity involved in the development, deployment, or operation of an emerging technology system that processes personal data, whether as a data controller, data processor, developer, manufacturer, platform operator, or vendor. Such entities shall:

- identify and document the lawful basis for each category of personal data processed by the emerging technology system before deployment;
- provide clear, accessible, plain-language privacy notices at the point of data collection, in a form appropriate to the technology context, disclosing the categories of data collected, the processing purposes, the parties with whom data is shared, the retention period, and data subject rights;
- implement data minimisation at the system design stage, collecting data at the minimum frequency and granularity necessary for the stated purpose and implementing automatic deletion or anonymisation of data that has exceeded its retention period;

- conduct a DPIA before deploying any emerging technology system that involves the processing of personal data;
- implement security-by-design, including encryption of data in transit and at rest, access authentication and controls, regular security patching and update management, and breach detection, containment, and notification procedures;
- execute compliant data processing agreements with all third-party vendors, platform operators, and service providers acting as data processors, and data sharing agreements with any party that receives personal data as a data controller in its own right; and
- assess and document the lawful basis for any cross-border transfer of personal data and implement appropriate safeguards under Part VI of the Act.

13.8. Technology-Specific Obligations

In addition to the general obligations set out above, the following technology-specific obligations apply.

Internet of Things (IoT)

Entities that deploy IoT systems processing personal data shall:

- implement security-by-design in IoT deployments, including: unique per-device authentication credentials; encrypted data transmission; regular security update and patch management; network segmentation of IoT devices from core systems; and mechanisms for secure decommissioning of devices;
- AI-enabled IoT processing: Where IoT systems incorporate AI , entities shall comply with the applicable requirements under the Artificial Intelligence Guidance Note.

Cloud Computing

Entities that use cloud computing services to store or process personal data shall:

- enter into a written data processing agreement with the cloud service provider before any personal data is stored or processed in the cloud, containing the mandatory provisions required under the General Regulations, including restrictions on processing personal data only on the customer's instructions and requirements to assist the customer in responding to data subject rights requests;
- conduct due diligence on the cloud service provider's data protection and security practices, including:
  - the jurisdictions in which data may be stored or processed;
  - security certifications and audit reports;
  - incident response and breach notification procedures; and
  - sub-processor lists and authorisation mechanisms;
- maintain a clear record of what personal data is stored in which cloud environment, and implement data retention and deletion controls that ensure personal data is deleted or anonymised at the end of its retention period, including from backups and replicated copies; and
- classify personal data before cloud migration, applying heightened controls to sensitive personal data, including encryption with customer-managed keys.

Blockchain and Distributed Ledger Technologies

Entities deploying or using blockchain or DLT systems that process personal data shall:

- assess, at the system design stage, whether personal data needs to be stored on the blockchain itself, or whether the blockchain can be used to store only cryptographic references (hashes) to personal data held in off-chain storage systems that are subject to full data protection controls and can be erased;
- where personal data shall be recorded on-chain, identify the specific lawful basis for that processing and document it, taking particular account of the immutability constraint which limits the ability to honour erasure and rectification rights;
- implement technical measures to protect personal data recorded on blockchain, including encryption of personal data before recording and the use of private or permissioned blockchain architectures rather than public blockchains where feasible;
- document the allocation of data controller and data processor responsibilities among participants in the blockchain network, including in any consortium or governance agreement;
- conduct a DPIA before deploying any blockchain system that records personal data, specifically assessing the tension between immutability and data subject rights and identifying technical mitigations;
- where erasure of on-chain personal data is technically impossible, implement compensating measures: rendering the data functionally inaccessible (for example, by destroying the encryption key), and documenting the impossibility of technical erasure and the compensating measure adopted; and
- assess and document the cross-border transfer implications of all nodes in the blockchain network that process personal data.

Biometric Recognition Systems

The Office has issued the Guidance Note on Biometric Data to provide practical guidance to data controllers and data processors on the lawful processing of biometric data under the Data Protection Act (accessible at www.odpc.go.ke). The Guidance Note recognises biometric data as sensitive personal data and emphasises that its processing presents heightened risks to the rights and freedoms of data subjects, particularly the right to privacy. It provides guidance on the lawful collection, use, storage, sharing, retention, security, and disposal of biometric data, and promotes the application of data protection by design and by default throughout the lifecycle of biometric systems. Data handlers processing biometric data should comply with the Guidance Note in addition to the requirements of the Act and the Regulations.

In particular, entities deploying biometric recognition systems should ensure that biometric processing is supported by an appropriate lawful basis, undertake a Data Protection Impact Assessment (DPIA) before deployment where required, implement robust technical and organisational safeguards to protect biometric templates, conduct regular testing to ensure the accuracy and fairness of biometric systems, provide clear and accessible privacy notices, implement appropriate retention and deletion controls, and establish effective governance over third-party biometric service providers and cross-border data transfers. Where biometric technologies are deployed for surveillance or in publicly accessible spaces, data handlers should ensure that such deployments satisfy the requirements of the Data Protection Act are demonstrably necessary and

proportionate, and comply with the specific safeguards contained in the ODPC's Guidance Note on Biometric Data.

Immersive Technologies (XR)

Entities deploying XR systems that process personal data shall:

- identify the lawful basis for each category of personal data collected in the XR environment, recognising that physiological and biometric data collected by XR systems constitutes sensitive personal data requiring a specific legal basis;
- provide privacy notices in accessible, in-experience formats that are meaningful to users in the XR context, including disclosure of all categories of data collected, the processing purposes, and data subject rights;
- implement data minimisation: collecting only the data required for the specific XR application purpose, disabling unnecessary sensors where technically feasible, and anonymising data as early as possible in the processing pipeline;
- implement heightened protections for XR data relating to children, including age verification, parental consent, and prohibition of commercial profiling of children in XR environments;
- implement technical measures to prevent the inadvertent collection of personal data from third parties in the user's physical environment, including through camera or audio capture; and
- provide users with accessible mechanisms to review, correct, and delete personal data collected during XR sessions.

Connected and Autonomous Vehicles

Entities that operate connected vehicle systems processing personal data including vehicle manufacturers, fleet operators, ride-sharing platforms, and telematics service providers shall:

- identify the lawful basis for each category of personal data collected by the connected vehicle system. Location tracking of fleet vehicles for operational purposes may be based on legitimate interests or contract; continuous monitoring of employee driving behaviour for performance management purposes requires careful assessment of proportionality and, typically, explicit disclosure to employees;
- provide clear privacy notices to all vehicle occupants, not only the registered vehicle owner disclosing what data is collected, for what purposes, and with whom it is shared;
- implement data minimisation: collecting location data at the minimum frequency required for the operational purpose; not retaining detailed journey logs beyond the period necessary; anonymising aggregated location data for analytics purposes;
- implement strict access controls on connected vehicle data, limiting access to the data to parties with a specific and documented operational need, and prohibiting onward sharing of personal data without a lawful basis;
- implement cybersecurity measures appropriate to the safety-critical nature of connected vehicle systems, including encryption of data transmission, access authentication, and intrusion detection.

14. ENFORCEMENT AND COMPLAINTS

The Office is mandated to oversee the implementation and enforcement of the Act. The Office is empowered to receive and investigate complaints, conduct inspections and audits of data controllers and data processors, issue enforcement and penalty notices, impose administrative fines, and make referrals for criminal prosecution where applicable. These enforcement powers apply in full to entities that process personal data through emerging technology systems.

Data subjects who believe that an entity has violated their data protection rights in connection with an emerging technology deployment may lodge a complaint with the Office. Complaints may relate to, among other matters:

- failure to provide a privacy notice at the point of IoT data collection or through an XR platform;
- use of biometric data without explicit consent or specific statutory authority;
- failure to conduct a DPIA before deploying a high-risk emerging technology system;
- unlawful transfer of personal data to offshore cloud infrastructure or technology platform operators;
- failure to give effect to a data subject's erasure request, including in relation to blockchain-recorded data;
- failure to implement adequate security measures, resulting in a data breach through an IoT, cloud, or connected vehicle system;
- use of emerging technology data for a purpose incompatible with the original collection purpose; or
- processing of children's personal data through emerging technologies without parental consent or adequate safeguards.

Entities found to have violated the Act in connection with emerging technology processing are liable to enforcement action, including administrative fines and civil remedies, in accordance with the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021.

The Office encourages entities to engage proactively with the Office on emerging technology data protection questions and to participate in ODPC-facilitated stakeholder engagement on technology governance. The Office may consider cooperation and proactive engagement among relevant factors during enforcement processes.

To lodge a complaint or seek further guidance, contact the Office at:

Office of the Data Protection Commissioner

Britam Towers, 12th Floor, Hospital Road, Upperhill, Nairobi

P.O. Box 30920-00100, Nairobi, Kenya

Email: complaint@odpc.go.ke (for lodging complaints) | info@odpc.go.ke / enquiries@odpc.go.ke (for enquiries and further guidance)

Telephone: 0207801800 | 0796954269 / 0752896867

Website: www.odpc.go.ke

ANNEX 1: COMPLIANCE CHECKLIST FOR EMERGING TECHNOLOGY DEPLOYMENTS

The following checklist assists entities in self-assessing data protection compliance for emerging technology deployments. It does not substitute for a full DPIA or legal review.

Compliance Requirement	**Action Required**
Registration	Register with the ODPC as a data controller or processor before deploying any emerging technology system that processes personal data of persons in Kenya.
Privacy Notice	Provide accessible, plain-language privacy notices at the point of emerging technology data collection, disclosing: categories of data collected; processing purposes; sharing arrangements; retention periods; and data subject rights.
Lawful Basis	Identify and document a lawful basis under Section 30 of the Act for each processing activity conducted through the emerging technology system before deployment.
Sensitive Personal Data	Identify whether the system processes sensitive personal data (including biometric, health, or location data). If so, ensure explicit consent or specific legal authority and implement heightened safeguards.
Children's Data	Assess whether the emerging technology system may be used by or process data about children. If so, implement age verification, parental consent, and age-appropriate design measures.
DPIA	Conduct a mandatory DPIA before deploying any high-risk emerging technology system. Document the assessment, record residual risks, and retain the DPIA for regulatory inspection.
DPO	Designate a DPO where the deployment involves large-scale systematic monitoring or large-scale processing of sensitive personal data.
Privacy by Design	Embed privacy by design at the system architecture stage. Select least privacy-invasive architecture; configure privacy-protective defaults; build in data subject rights interfaces.
Data Minimisation	Collect only the minimum personal data necessary. Review sensor frequency, granularity, and retention periods. Prefer anonymised or aggregated data for analytics purposes.
Security	Implement security-by-design: encrypted data transmission and storage; access authentication; patch management; intrusion detection; incident response procedures.
Data Processor Agreements	Execute compliant data processing agreements with all third-party technology vendors, platform operators, and cloud providers before any personal data is shared.

Cross-Border Transfers	Map all cross-border data flows. Identify the lawful transfer basis for each. Implement contractual or other safeguards where adequacy of the destination jurisdiction is not established.
Blockchain-Specific	Where blockchain is used: prefer off-chain storage with on-chain hashing; document the impossibility of erasure where applicable and implement cryptographic deletion as a compensating measure.
Breach Notification	Implement breach detection, containment, and notification procedures for the emerging technology system. Test procedures regularly.
Ongoing Monitoring	Monitor emerging technology systems on an ongoing basis for compliance with data protection obligations, emerging vulnerabilities, and privacy risks. Conduct periodic DPIA reviews.