DATA PROTECTION ACT (DPA)2019 COMPLIANCE CHECKLIST

AREA	DELIVERABLE	SECTION
REGISTRATION	☐ Mandatory registration is based on nature of industry, volume of data processed, if sensitive personal data is being processed and any other criteria the Data Commissioner may specify including: ☐ Have an annual turnover exceeding KES 5,000,000 and more than 10 employees. ☐ Canvassing political support among the electorate. ☐ Operating Credit Bureaus. ☐ Crime prevention and prosecution of offenders (including operating security CCTV systems). ☐ Debt administration and factoring. ☐ Gaming and betting operators. ☐ Provision of education. ☐ Health administration and provision of patient care. ☐ Hospitality industry firms. ☐ Insurance administration and undertakings. ☐ Faith based or religious institutions. ☐ Retirement benefits administration. ☐ Property management including the selling of land. ☐ Provision of financial services. ☐ Telecommunications network or service providers. ☐ Businesses that are wholly or mainly in direct marketing. ☐ Internet access provider. ☐ Transport services firms (including online passenger hailing applications)	Section 18, Regulation 11,Second and Third Schedule (Draft Data Protection (Registration of Data Processors and Data Controllers) Regulations)

SENTINEL

SENTINEL AFRICA CONSULTING
5th Floor Rainbow Tower, Muthithi Road, Westlands,
P.O. Box 39681-00623, NAIROBI, KENYA.
Telephone: +254 (0) 20 248 48 88 | Mobile: +254 (0) 715 48 48 88
E-mail: info@sentinelafrica.co.ke | Website: www.sentinelafrica.co.ke

	▯ Public sector bodies. Except for State Corporations or County Corporations, a public body at national or county government which operates within a state department or county department, is wholly funded from the Exchequer, provides a public service, and the fees payable shall be paid by the respective state department or county department. ▯ Businesses that process genetic data. ▯ Application for registration using Form A set out in the First Schedule, ▯ Accompany Form with registration fees specified in the Second Schedule. ▯ Accompany application for registration with: ▯ a copy of establishment documents, ▯ particulars of the data controllers or processors including name and contact details, ▯ a description of the purpose for which personal data is processed, ▯ a description of categories of personal data processed, and ▯ any other relevant information that the Data Commissioner may require. ▯ Verification process will commence after submission of application and payment of required fees. ▯ If the Data Commissioner is satisfied that the applicant fulfils the requirements for registration, the Data Commissioner shall within 14 days issue the applicant with a certificate of registration and may specify any conditions thereof and enter the	Regulation 5 Regulation 7 Regulation 8

SENTINEL

	particulars of the applicant in the register.	
	☐ The certificate of registration issued shall be valid for a period of one year.	Regulation 8(2)
	☐ Display the certificate of registration and any change of particulars of a certificate if any, at a conspicuous place at the principal place of business or on the organisation official website and a certified copy of the certificate of registration for each branch, where applicable.	Regulation 9
	☐ Application for renewal of certificate must be done thirty days before the expiry of the certificate of registration. Failure to renew a certificate of registration and continuing to process personal data after the expiry of the certificate amounts to an offence.	Regulation 10
REJECTION OF APPLICATION OR RENEWAL	☐ If an application for registration/renewal is declined, the Data Commissioner shall within 21 days from the day of such decision notify, in writing, the applicant of the refusal and provide reasons for such refusal.	Regulation 11(Draft Data Protection (Registration of Data Processors and Data Controllers) Regulations)
	☐ Grounds for refusal include: ☐ particulars provided for inclusion in an entry in the register are insufficient, ☐ appropriate safeguards for the protection of the privacy of the data subject have not been provided by the data controller or a data processor, or ☐ the data controller or data processor is in violation of any provisions of the Act.	Regulation 11(Draft Data Protection (Registration of Data Processors and Data Controllers) Regulations)

SENTINEL

CHANGE OF PARTICULARS	☐ Within 14 days of the occurrence of any changes in the particulars, notify the Data Commissioner in writing	Regulation 14(Draft Data Protection (Registration of Data Processors and Data Controllers) Regulations)
ELECTRONIC APPLICATION	☐ Application shall be submitted through electronic means provided for on the Office website.	Regulation 19(Draft Data Protection (Registration of Data Processors and Data Controllers) Regulations)
GOVERNANCE	☐ Document your Privacy Governance Model e.g., with clear roles and responsibilities and reporting lines to embed privacy compliance into the organisation, and address situations where there may be conflicting objectives internally (e.g., between marketing and legal functions)	Section 41
	☐ Appoint/Designate a **Data Protection Officer** (DPO) if necessary. A DPO may be necessary if: ☐ processing is carried out by a public body or private body, except for courts acting in their judicial capacity. ☐ core activities of the data controller or data processor consist of processing operations which, based on nature, scope and purposes, require regular and systematic monitoring of data subjects. ☐ core activities of the data controller or the data processor consist of processing of sensitive categories of personal data i.e., data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details	Section 24

SENTINEL

	including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject.	
	☐ DPO may be a staff member of the data controller or data processor. ☐ Group of entities may appoint a single data protection officer provided that such officer is accessible by each entity. ☐ If organisation is a public body, a single data protection officer may be designated for several such public bodies, considering their organisational structures. ☐ Qualification of DPO-person must have relevant academic or professional qualifications which may include knowledge and technical skills in matters relating to data protection. ☐ Publish the contact details of the DPO on the organisation website and communicate them to the Data Commissioner who shall ensure that the same information is available on the official website.	
	☐ Sign a data processing agreement between your organisation and any third parties that process your personal data on your behalf.	Section 48(b)
	☐ Develop and roll-out training across all personnel to ensure understanding of data protection principles, responsibilities, risks, etc.	Section 48(b)
RECORD OF PROCESSING	☐ Identify all data processed in a detailed Record of Processing, e.g., document what personal data is held by your organisation, where it came from, and who it is shared with.	Section19(2) (a)
	☐ Implement and maintain processes for updating and maintaining Record of Processing.	Section 41(4) (f)

SENTINEL

ACCOUNTABILITY	☐ Implement a data protection policy, which brings together all underlying related policies including processes for privacy by design and the creation and maintenance of a record of processing activities. It must also include: ☐ the nature of personal data collected and held, ☐ how a data subject may access their personal data and exercise their rights in respect to that personal data, ☐ complaint handling mechanisms, ☐ lawful purpose for processing personal data, ☐ obligations or requirements to transfer personal data outside the country, to third parties, or other data controllers or data processors located outside Kenya and where possible, specify such recipients, ☐ the retention period and schedule contemplated under regulation 18; and ☐ the collection personal data about a vulnerable segment of the ☐ community, including children, and the criteria applied.	Regulation 22 (Draft Data Protection (General)Regulations)
	☐ Integrate privacy compliance into your audit framework	
FAIR PROCESSING AND CONSENT	☐ Review your existing grounds (legal basis) for lawful processing and confirm that these will still be sufficient under the DPA (e.g., can you still solely rely on consent given the requirements)	Section 30
	☐ Ensure that the legal basis for processing is explained in the privacy policy.	Regulation 22 (Draft Data Protection (General)Regulations)

SENTINEL

	☐ Consider whether your organisation is processing any sensitive personal data (as listed above) and ensure the requirements for processing such data are satisfied.	Section 44-47
	☐ Where consent is relied upon as the ground for processing Personal Data, review existing consents to ensure they meet the DPA requirements, and if not implement a process to seek new consents.	Section 31 (1)
	☐ Ensure systems can accommodate withdrawal of consent	Section 31 (2)
NOTICES / VETTING - HR	☐ Review and update, where necessary, customer privacy notices to be DPA compliant. Consider whether your notices have to accommodate "child-friendly requirements.	Regulation 22 (Draft Data Protection (General)Regulations)
CHILDREN	☐ Identify whether you process personal data of children. ☐ Seek counsel advice regarding applicable law restrictions, codes and guidance.	Section 33
	☐ If data relating to a child will be processed, ensure that age-verification systems are in place, notices directed at that child are "child-friendly" and, if consent is relied upon, you have implemented a mechanism to seek parental consent.	Section 33 (2)
	☐ Consider alternative protections, e.g., age-gating.	Section 33 (4)
DATA SUBJECT RIGHTS AND PROCEDURES	☐ Identify which data subject rights are relevant given the legal basis on which you process each category of data. These are: ☐ to be informed of the use to which their personal data is to be put,	Section 26

SENTINEL

	▯ to access their personal data in custody of data controller or data processor, ▯ to object to the processing of all or part of their personal data, ▯ to correction of false or misleading data; and ▯ to deletion of false or misleading data about them	
	▯ Update data privacy policy and internal processes for dealing with requests.	Section 34
	▯ Ensure technical and operational processes are in place to ensure data subjects' rights can be met, e.g., right of rectification and erasure, data portability, the right to object, and subject access requests.	Section 38,39,40, 26
	▯ Establish a personal data retention schedule with appropriate time limits for the periodic review of the need for the continued storage of personal data that is no longer required for the purpose for which it was collected	Regulation 18(Draft Data Protection (General)Regulations)
	▯ Incorporate the duty to notify the data subject in the organization privacy policy in so far as: ▯ the rights of data subject specified under section 26, ▯ the fact that personal data is being collected, ▯ the purpose for which the personal data is being collected, ▯ the third parties whose personal data has been or will be transferred to, including details of safeguards adopted, ▯ the contacts of the data controller or data processor and on whether any other entity may receive the collected personal data, ▯ a description of the technical and organizational security measures taken to ensure the	Section 29

SENTINEL

	integrity and confidentiality of the data, - the data being collected pursuant to any law and whether such collection is voluntary or mandatory; and - the consequences if any, where the data subject fails to provide all or any part of the requested data.	
PRIVACY BY DESIGN AND DEFAULT	- Ensure processes are in place to embed privacy by design into projects (e.g., technical and organisational measures are in place to ensure data minimisation, purpose limitation and security) - Ensure that, by default, only personal data which is necessary for each specific purpose is processed, taking into consideration- - the amount of personal data collected, - the extent of its processing, - the period of its storage, - its accessibility; and - the cost of processing data and the technologies and tools used.	Section 41
DATA PROTECTION IMPACT ASSESMENT (DPIA)	- Conduct a DPIA if operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes. If the processing of personal data meets two or more of these criteria, a DPIA is required: - Biometric data processed for identification purposes. - Automated decision making i.e., using of algorithms to profile. - Data collected via third parties. - Use of new/ innovative solutions/ new technology. - Location data	Section 31

SENTINEL

	▯ Exception to the right to be informed. ▯ Migration from one system to at least another one. ▯ Processing for scientific/ historical purpose without consent. ▯ Large scale processing of personal data. ▯ Consult the Data Commissioner prior to the processing if a data protection impact assessment prepared under this section indicates that the processing of the data would result in a high risk to the rights and freedoms of a data subject. ▯ Submit DPIA report to the Office of the Data Protection Commissioner (ODPC) sixty days prior to the processing of data. ▯ Put in place a privacy impact assessment protocol	
COMPLIANT CONTRACTING AND PROCUREMENT	▯ Develop compliant contract wording for customer agreements and third-party vendor agreements. ▯ Identify all contracts that require relevant contract wording, prioritise and develop process for amending. ▯ Ensure procurement process has controls to ensure privacy by ▯ design (e.g., security diligence, data minimisation, visibility of onwards data flows)	Section 26, 31 (1),42(4)
DATA BREACH PROCEDURES	▯ Ensure appropriate security has been implemented, including backups, encryption, and regular testing to ensure technical security. ▯ Review and update (or develop where not in existence) Data Breach Response Plan. ▯ Review insurance coverage for data breaches and consider whether it needs to be updated in light of the higher fines and penalties under the DPA. ▯ Review liability provisions in agreements for breaches caused by services provider and other partners.	Section 41

SENTINEL

NOTIFICATION OF DATA BREACH	▯ Notify the Data Commissioner without delay, within 72 hours of becoming aware of such breach. ▯ If the notification to the Data Commissioner is not made within 72 hours, the notification shall be accompanied by reasons for the delay. ▯ Communicate to the data subject in writing within a reasonably practical period, unless the identity of the data subject cannot be established. ▯ Provide sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach i.e., • the nature of the breach, • measures to mitigate, • recommendation on measure to be taken by the data subject, • If identifiable, the identity of the unauthorised person • Name and details of DPO if applicable ▯ A data processor must notify the data controller without delay and where reasonably practicable, within 48 hours of becoming aware of a breach.	
DATA TRANSFER	▯ Transfer can take place if: ▯ proof is given to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data, ▯ safeguards include jurisdictions with commensurate data protection laws, ▯ transfer is necessary — • for the performance of a contract between the data subject and the data controller or data processor or implementation of precontractual measures	

SENTINEL

	taken at the data subject's request, • for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person, • for any matter of public interest, • for the establishment, exercise or defence of a legal claim, • to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or • for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects. ☐ Sensitive personal data transfer only to be effected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards ☐ Identify all cross-border data flows and review data export mechanisms. ☐ Update cross border mechanisms if necessary	
PENALTIES	☐ The Data Commissioner may serve an enforcement notice on a person requiring them to take such steps and within such period as may be specified in the notice. ☐ If satisfied that a person has failed or is failing to comply, the Data	

SENTINEL

	Commissioner may issue a penalty notice requiring the person to pay to the Office of the Data Commissioner an amount specified in the notice. - Infringement of a provision of the Act may attract a maximum amount indicated in a penalty notice of up to 5 million shillings, or in the case of an undertaking, up to 1% of its annual turnover of the preceding financial year, whichever is lower. - A person who suffers damage by reason of a contravention of a requirement of the Act is entitled to compensation for that damage.	

SENTINEL