COMPLIANCE	DELIVERABLE	REGULATION
Registration	The data processor/ controller during mandatory registration has specified the nature of industry it operates, this may include; ☐ Canvassing political support among the electorate. ☐ Crime prevention and prosecution of offenders (including operating security CCTV systems). ☐ Gambling. ☐ Operating an educational institution. ☐ Health administration and provision of patient care. ☐ Hospitality industry firms but excludes tour guides. ☐ 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. ☐ Transport services firms (including online passenger hailing applications) ☐ Businesses that process genetic data The data processor/ controller has specified personal data its collecting in the following manner; ☐ Category of data subjects [e.g. employee, client, students, supplier, shareholder] ☐ Description of personal data to be processed [e.g. name, address, identification number] ☐ Purpose of processing [e.g. marketing, survey, payroll, invoicing, Know Your Customer]	DPA [No. 24 of 2019]

	The data processor/ controller has indicated the categories of sensitive personal data and specified purpose(s) for processing sensitive personal data: The data processor/ controller has specified the list of the country/(ies) its in contractual agreement with appertaining transfer of data outside Kenya The data processor/ controller has put in place measures for protection of personal data by; Identifying risks to personal data [e.g. unauthorized access/ disclosure, theft] Safeguards, security measures and mechanisms implemented to protect personal data [e.g. access control, privacy policy, visitor's logbook, information security policy] The data processor/ controller has specified the number of employees it has in its organization; ☐ 1-9 employees ☐ 10-49 employees ☐ 50-99 employees ☐ More than 99 employees The data processor/ controller has specified its record for previous year annual turnover; ☐ Less than Kshs. 2,000,000 ☐ Kshs. 2,000,001 – 5,000,000 ☐ Kshs. 5,000,001 – 10,000,000 ☐ Kshs. 10,000,001 – 50,000,000 ☐ More than Kshs. 50,000,000	

	The data processor/ controller has per the regulation paid registration fees; ☐ Micro and small data controllers/ processors – Kshs 4,000 ☐ Medium data controller/ processors – Kshs 16,000 ☐ Large data controller/ processors – Kshs 40,000 ☐ Public entities – Kshs. 4,000 ☐ Charities and Religious entities – Kshs. 4,000 ☐ County department shall register and pay the fees on behalf of their respective entities.	
Governance	The data processor/ controller has appointed/ designated a certified Data Protection Officer who; ☐ Co-operates with the Data Commissioner and any other authority on matters relating to data protection. ☐ Ensures on behalf of the data controller or data processor that this Act is complied with; ☐ Facilitates capacity building of staff involved in data processing operations; ☐ Provides advice on data protection impact assessment; and ☐ Advises the data controller or data processor and their employees on data processing requirements provided under this Act or any other written law; ☐ Signs data processing arrangement between your organization and any third parties that process personal data on your behalf The data processor/ controller has ensured that the appointed DPO has relevant academic or professional qualifications which include	DPA [section 24 of 2019]

	knowledge and technical skills in matters relating to data protection. The data processor/ controller has published the contact details of the DPO on the organization website and communicates them to the Data Commissioner who shall ensure that the same information is available on the official website.	
Commercial use of personal data	The data processor/ controller has gotten consent from a data subject for purposes of direct marketing by informing data subject of; ☐ The identity of the data controller or data processor; ☐ The purpose of each of the processing operations for which consent is sought; ☐ The type of personal data that is collected and used; ☐ Information about the use of the personal data for automated decision-making, where relevant; ☐ The possible risks of data transfers due to absence of an adequacy decision or appropriate safeguards; ☐ Whether the personal data processed shall be shared with third parties; ☐ The right to withdraw consent; and ☐ The implications of providing, withholding or withdrawing consent The data processor/ controller presents consent information through a written notice, oral statement, audio/ video message where the data controller/ processor ensures that; ☐ Data subject has capacity to give consent; Processing on the basis of consent. ☐ Data subject voluntarily gives consent; and ☐ Consent is specific to the purpose of processing The data processor/ controller relies on one legal basis for processing at a time when processing data	DPA [section 37 of 2019]

	without consent of data subject; which is established before processing and shall be demonstratable at all times; Where a data controller uses multiple bases for different processing, the data controller shall; ☐ Distinguish between the legal bases being used; and ☐ Respond to any data subject rights requests. Data processor/ controller pursuant to section 28(2) of the Act, collects personal data indirectly from; ☐ Any person other than the data subject; ☐ Publications or databases; ☐ Surveillance cameras, where an individual is identifiable or reasonably identifiable; ☐ Information associated with web browsing; or ☐ Biometric technology, including voice or facial recognition. The data controller/ processor ensures, in collecting personal data; ☐ Ensures that processing is limited to personal data which the data subject has permitted the data controller or data processor to collect; ☐ Undertakes steps to ensure that personal data is accurate, not in excessive and up to date; ☐ Undertakes processes to secure personal data; and ☐ Complies with the lawful processing principles set out under part IV of the Act	

	The data processor/ controller pursuant to section 34 of the Act obliges to a request by the data subject to restrict the processing of their personal data on grounds that; ☐ The data subject contests the accuracy of their personal data; ☐ The personal data has been unlawfully processed and the data subject opposes the erasure and requests restriction instead; ☐ The data subject no longer needs their personal data but the data controller or data processor requires the personal data to be kept in order to establish, exercise or defend a legal claim; or ☐ A data subject has objected to the processing of their personal data under regulation 8 and a data controller or data processor is considering legitimate grounds that override those of the data subject. The data processor/ controller under section 34 avails Form DPG 1 for a request for restriction to processing of personal data; The data processor/ controller pursuant to sub-regulation (2) within fourteen days of the request for restriction and without charging any fee does the following; ☐ Admit and implement the request; ☐ Indicate on the data controller or data processors system that the processing of the personal data has been restricted; and ☐ Notify any relevant third party of the restriction where personal data, subject to such restriction, may have been shared.	

	The data controller/ processor implements a restriction to processing request by; ☐ Temporarily moving the personal data to another processing system; ☐ Making the personal data unavailable to third parties; or ☐ Temporarily removing published data specific to the data subject from its website or other public medium in its control. The data controller/ processor under section 34(2) of the Act, declines a request by the data subject shall within fourteen days issue a notification for the refusal in writing, and shall provide the reasons for the decision. The data controller/ processor where the right to object to processing is not absolute and the request by a data subject has been declined shall inform the data subject of; ☐ The reasons for declining the request for objection; and ☐ The right to lodge a complaint to the Data Commissioner where dissatisfied.	

	The data controller/ processor avails channels where a data subject has the right to obtain 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 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 or territories; ☐ 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. The data controller/ processor avails Form DPG 2 where a data subject may request to access their personal data whereby; ☐ On request, provide access to a data subject of their personal data in its possession; ☐ Put in place mechanisms to enable a data subject to proactively access or examine their personal data; or ☐ Provide the data subject with a copy of their personal data The data controller/ processor complies with a request by a data subject to access their personal data within seven days of the of the request. The data controller/ processor provides information requested by the data subject in a commonly used electronic form, unless otherwise requested by the data subject.	

	The data controller/ processor ensures that compliance with the request for access to personal data is free of charge. The data controller/ processor pursuant to section 40 of the Act avails Form DPG 3 where a data subject may request for a rectification of their personal data which is untrue, inaccurate, outdated, incomplete or misleading The data controller/ processor within fourteen days of the request, rectify an entry of personal data in the database where the data controller or data processor is satisfied that a rectification is necessary The data controller/ processor notifies the data subject where a request for rectification is declined reasons for refusal within seven days; where a request for refusal is made free of charge.	
Permitted commercial use of personal data	The data controller/ processor uses personal data, other than sensitive personal data, concerning a data subject for the purposes of direct marketing where; ☐ The data controller or data processor has collected the personal data from the data subject; ☐ A data subject is notified that direct marketing is one of the purposes for which personal data is collected; ☐ The data subject has consented to the use or disclosure of the personal data for the purpose of direct marketing; ☐ The data controller or data processor provides a simplified opt out mechanism for the data subject to request not to receive direct marketing communications; or ☐ The data subject has not made an opt out request The data controller/ processor does not transmit, for purposes of marketing, messages by any means unless the data controller or data processor indicates particulars to which a data subject may send a request to restrict such communications without incurring charges	DPA [section 37 of 2019]

	The data controller/ processor neither transmits, nor instigates the transmission of, a communication for the purposes of direct marketing by means of electronic mail; ☐ Where the identity of the person on whose behalf the communication has been sent has been disguised or concealed; ☐ Where a valid address to which the recipient of the communication may send a request that such communications cease has not been provided; or ☐ Where there is use of automated calling systems without human intervention. The data controller/ processor has provided an opt out mechanism contemplated under regulation 15(1)(d) that shall; ☐ Have a visible, clear and easily understood explanation of how to opt out; ☐ Include a process for opting out that requires minimal time and effort; ☐ Provide a direct and accessible communication channel; ☐ Be free of charge or where necessary involve a nominal cost to a data subject; and ☐ Be accessible to persons with a disability The data controller/ processor does not use or disclose personal data for the purposes of direct marketing where a data subject has opted out, in accordance with the data subject's request The data controller/ processor includes a statement which is prominently displayed, or otherwise draws the attention of the data subject to the fact that the data subject may make an opt out request in communicating with a data subject on direct marketing.	

	The data controller/ processor in compliance with an opt out requirement; ☐ Clearly indicate, in each direct marketing message, that a data subject may opt out of receiving future messages by replying with a single word instruction in the subject line; ☐ Ensure that a link is prominently located in the email, which takes a data subject to a subscription control centre; ☐ Clearly indicate that a data subject may opt out of future direct marketing by replying to a direct marketing text message with a single word instruction; ☐ Inform the recipient of a direct marketing phone call that they can verbally opt out from any future calls; and ☐ Include instructions on how to opt out from future direct marketing, in each message.	
Request for restriction of further direct marketing	The data controller/ processor has mechanism whereby the data subject may request restrict use or disclosure of their personal data, to a third party, for the purpose of facilitating direct marketing. The data controller/ processor does not charge fee for making or giving effect to a request under this part The data controller or data processor restricts use or disclosure of personal data for the purpose of facilitating direct marketing by a third party within seven days of the request.	DPA [section 37 of 2019]

Data portability request	The data controller/ processor pursuant to section 38 of the Act allow a request from a data subject to port or copy their personal data from data controller/ processor to another in Form DPG 4 The data controller/ processor ports personal data to the data subject's choice of recipient within thirty days of request upon payment of the prescribed fees; where fee is charged under sub-regulation (2) and is reasonable and does not exceed the cost incurred to actualize the request The data controller/ processor within seven days notify the data subject of the decline of portability request and reasons for such decline in writing	DPA [section 38 of 2019]
Right of erasure	The data controller/ processor pursuant to section 40(1) (b) of the Act avails Form DPG 5 whereby a data subject may, request for erasure/ destruction of personal data held where; ☐ The personal data is no longer necessary for the purpose which it was collected; ☐ The data subject withdraws their consent that was the lawful basis for retaining the personal data; ☐ The data subject objects to the processing of their data and there is no overriding legitimate interest to continue the processing; ☐ The processing of personal data is for direct marketing purposes and the individual objects to that processing; ☐ The processing of personal data is unlawful including in breach of the lawfulness requirement; or ☐ The erasure is necessary to comply with a legal obligation.	DPA [section 40 of 2019]

	The data controller/ processor responds to request for erasure under sub-regulation (2) within fourteen days of the request The data controller/ processor may not apply the right of erasure due to the following reasons; ☐ To exercise the right of freedom of expression and information; ☐ To comply with a legal obligation; ☐ For the performance of a task carried out in the public interest or in the exercise of official authority; ☐ For archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or ☐ For the establishment, exercise or defense of a legal claim.	
Retention of personal data	The data controller/ processor pursuant to section 39 of the Act, retains personal data processed for a lawful purpose, for as long as may be reasonably necessary for the purpose for which the personal data is processed; ☐ Establish 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 necessary or where the retention period is reached; and ☐ Erase, delete anonymize or pseudonymize personal data upon the lapse of the purpose for which the personal data was collected. The personal data retention outlines; ☐ Purpose for retention; ☐ The retention period; ☐ Provision for periodic audit of the personal data retained; and	DPA [section 39 of 2019]

	☐ Actions to be taken after the audit of the personal data retained. An audit of the retained data seeks to; ☐ Review records with a view of identifying personal data that no longer requires to be retained and permanently delete the personal data; ☐ Ensure the retained data is accurate and up-to-date; ☐ Specify the purpose for retention of personal data; ☐ Ensure that the personal data security measures are adequate; and ☐ Identify the best cause of action where personal data retention period lapses. The data controller/ processor establishes appropriate time limits for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes	
Requests to deal anonymously or pseudonymously	The data controller/ processor with request from a data subject has a mechanism whereby personal data is processed anonymously or pseudonymously where the data subject wishes; ☐ Not to be identified; ☐ To avoid subsequent contact such as direct marketing from an entity or third parties; ☐ To enhance their privacy on the whereabouts of a data subject; ☐ To access services such as counselling or health services without it becoming known to others; ☐ To express views in a public arena without being personally identified; or ☐ To minimize the risk of identity fraud.	DPA [regulation 20(1) of 2021]

	The data controller/ processor accedes to the request where satisfied that the request is based on any of the reasons specified under sub-regulation (1) and where the request is in the best interests of the data subject.	
Sharing of personal data	The data controller/ processor subject to section 25 of the Act, exchanges personal data collected, upon request, by another data controller, data processor, third party or a data subject and determines the purpose and means of sharing personal data from one data controller or data processor to another; ☐ Providing personal data to a third party by whatever means by the data controller or data processor; ☐ Receiving personal data from a data controller or data processor as joint participant in a data sharing arrangement; ☐ Exchanging or transmission of personal data; ☐ Providing third party with access to personal data on the data controller's information systems; ☐ Separate or joint initiatives by data controllers or data processors to pool personal data making the data available to each other or a third-party subject to entering into an agreement, as may be applicable; or ☐ Routine data sharing between data controllers on a regular or pre-planned basis. The data controller/ processor has entered into agreements prior to data sharing in carrying out any routine data sharing The data controller/ processor request for sharing of personal data is in writing and specifies; ☐ The purpose for which personal data is required; ☐ The duration for which personal data shall be retained; and	DPA [regulation 21(1) of 2021]

	☐ Proof of the safeguards put in place to secure personal data from unlawful disclosure.	
Automated individual decision making	The data controller/ processor pursuant to section 35 of the Act; ☐ Inform a data subject when engaging in processing based on automated individual decision making; ☐ Provide meaningful information about the logic involved; ☐ Specific transparency and fairness requirements are in place; ☐ Rights for a data subject to oppose profiling and ☐ specifically profiling for marketing are present; and ☐ Where conditions specified under section 31 of the Act arise, a data protection impact assessment is carried out; ☐ Explain the significance and envisaged consequences of the processing; ☐ Ensure the prevention of errors; ☐ Use appropriate mathematical or statistical procedures; ☐ Put appropriate technical and organizational measures in place to correct inaccuracies and minimize the risk of errors; ☐ Process personal data in a way that eliminates discriminatory effects and bias; and ☐ Ensure that a data subject can obtain human intervention and express their point of view	DPA [regulation 22(1) of 2021]

Data protection policy	The data controller/ processor develops, publishes and regularly updates a policy reflecting their personal data handling practices which includes; ☐ 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; ☐ Complaints handling mechanisms; ☐ Lawful purpose for processing personal data; ☐ Obligations or requirements where personal data is to be transferred 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 19; and ☐ The collection of personal data from children, and the criteria to be applied.	DPA [regulation 23(1) of 2021]
Contract between data controller and data processor	The data controller engages a data processor through a written contract subject to section 42(2)(b) of the Act as envisaged under sub-regulation (1) including the following particulars; ☐ Processing details including ○ The subject matter of the processing; ○ The duration of the processing; ○ The nature and purpose of the processing; ○ The type of personal data being processed; ○ The categories of data subjects; and ○ The obligations and rights of the data controller;	DPA [regulation 24(1) of 2021]

	☐ Instructions of the data controller; ☐ Duty on the data processors to obtain a commitment of confidentiality from any person or entity that the data processors allow to process the personal data; ☐ Security measures subjecting the data processor to appropriate technical and organizational measures in relation to keeping personal data secure; ☐ Provision stipulating that all personal data must be permanently deleted or returned on termination or lapse of the agreement, as decided by the data controller; and ☐ Auditing and inspection provisions by the data controller	
Obligations of a data processor	☐ The data processor does not engage the services of a third party without the prior authorization of the data controller ☐ The data processor enters into a contract with the third party where authorization is given; ☐ The data processor remains liable to the data controller for the compliance of any third party that they engage	DPA [regulation 25(1) of 2021]
Requirements for processing to be done in Kenya	The data controller/ processor pursuant to section 50 of the Act who processes personal data for the purpose of strategic interest of the state outlined under sub-regulation (2) complies by; ☐ Processing such personal data through a server and data centre located in Kenya; or ☐ Storing at least one serving copy of the concerned personal data in a data centre located in Kenya.	

	The purpose contemplated under sub-regulation (1) includes the processing of personal data for the purpose of; ☐ Administering of the civil registration and legal identity management systems; ☐ Facilitating the conduct of elections for the representation of the people under the Constitution; ☐ Overseeing any system for administering public finances by any state organ; ☐ Running any system designated as a protected computer system in terms of section 20 of the Computer Misuse and Cybercrime Act, 2018; ☐ Offering any form of early childhood education and basic education under the Basic Education Act, 2013; or ☐ Provision of primary or secondary health care for a data subject in the country. ☐ The data controller who processes personal data outside Kenya complies with sub regulation (1) under the requirement of the Cabinet Secretary where; ☐ Has been notified that personal data outside Kenya has been breached or its services have been used to violate the Act and has not taken measures to stop or handle the violation; and ☐ Resists, obstructs or fails to comply with requests of the Data Commissioner or any other relevant authority in ○ Cooperating to investigate and handle such violations; or ○ Neutralizing and disabling the effect of cyber security protection measures.	

Data protection by design or default	The data controller/ processor in processing of personal data; ☐ Establishes the data protection mechanisms set out under the Act and these Regulations are embedded in the processing and; ☐ Designs technical and organizational measures to safeguard and implement the data protection principles.	DPA [regulation 27 of 2021]
Elements for principle of lawfulness	The data controller/ processor has incorporated elements necessary to implement the principle of lawfulness that include; ☐ Appropriate legal basis or legitimate interests clearly connected to the specific purpose of processing; ☐ Processing that is necessary for the purpose; ☐ The data subject being granted the highest degree of autonomy possible with respect to control over their personal data; ☐ A data subject knowing what they consented to and a simplified means to withdraw consent; and ☐ Restriction of processing where the legal basis or legitimate interests ceases to apply	DPA [regulation 29 of 2021]

Elements for principle of transparency	The data controller/ processor has incorporated elements necessary to implement the principle of transparency that include; ☐ The use of clear, simple and plain language to communicate with a data subject to enable a data subject to make decisions on the processing of their personal data; ☐ Making the information on the processing easily accessible to the data subject; ☐ Providing the information on the processing to the data subject at the relevant time and in the appropriate form; ☐ The use of machine-readable language to facilitate and automate readability and clarity; ☐ Providing a fair understanding of the expectation with regards to the processing particularly for children or other vulnerable groups; and ☐ Providing details of the use and disclosure of the personal data of a data subject.	DPA [regulation 30 of 2021]
Elements for principle of purpose limitation	The data controller/ processor has incorporated elements necessary to implement the principle of purpose limitation that include; ☐ Specifying the purpose for each processing of personal data; ☐ Determining the legitimate purposes for the processing of personal data before designing organizational measures and safeguards; ☐ The purpose for the processing being the determinant for personal data collected; ☐ Ensuring a new purpose is compatible with the original purpose for which the data was collected; ☐ Regularly reviewing whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation; and ☐ The use of technical measures, including hashing and cryptography, to limit the possibility of repurposing personal data.	DPA [regulation 31 of 2021]

Elements for principle of integrity, confidentiality and availability	The data controller/ data processor has incorporated elements necessary to implement the principle of integrity, confidentiality and availability that include; ☐ Having an operative means of managing policies and procedures for information security; ☐ Assessing the risks against the security of personal data and putting in place measures to counter identified risks; ☐ Processing that is robust to withstand changes, regulatory demands, incidents, and cyber-attacks; ☐ Ensuring only authorized personnel have access to the data necessary for their processing tasks; ☐ Securing transfers shall be secured against unauthorized access and changes; ☐ Securing data storage from use, unauthorized access and alterations; ☐ Keeping back-ups and logs to the extent necessary for information security; ☐ Using audit trails and event monitoring as a routine security control; ☐ Protecting sensitive personal data with adequate measures and, where possible, kept separate from the rest of the personal data; ☐ Having in place routines and procedures to detect, handle, report, and learn from data breaches; and ☐ Regularly reviewing and testing software to uncover vulnerabilities of the systems supporting the processing.	DPA [regulation 32 of 2021]

Elements for principle of data minimization	The data controller/ processor has incorporated elements necessary to implement the principle of data minimization that include; ☐ Avoiding the processing of personal data altogether when this is possible for the relevant purpose; ☐ Limiting the amount of personal data collected to what is necessary for the purpose; ☐ Ability to demonstrate the relevance of the data to the processing in question ☐ Pseudonymizing personal data as soon as the data is no longer necessary to have directly identifiable personal data, and storing identification keys separately; ☐ Anonymizing or deleting personal data where the data is no longer necessary for the purpose; ☐ Making data flows efficient to avoid the creation of more copies or entry points for data collection than is necessary; and ☐ The application of available and suitable technologies for data avoidance and minimization	DPA [regulation 33 of 2021]
Elements for principle of accuracy	The data controller/ processor has incorporated elements necessary to implement the principle of accuracy that include; ☐ Ensuring data sources are reliable in terms of data accuracy; ☐ Having personal data particulars being accurate as necessary for the specified purposes; ☐ Verification of the correctness of personal data with the data subject before and at different stages of the processing depending on the nature of the personal data, in relation to how often it may change; ☐ Erasing or rectifying inaccurate data without delay; ☐ Mitigating the effect of an accumulated error in the processing chain; ☐ Giving data subjects an overview and easy access to personal data in order to control accuracy and rectify as needed;	DPA [regulation 34 of 2021]

	☐ Having personal data accurate at all stages of the processing and carrying out tests for accuracy at critical steps; ☐ Updating personal data as necessary for the purpose; and ☐ The use of technological and organizational design features to decrease inaccuracy	
Elements for principle of storage limitation	The data controller/ processor has incorporated e elements necessary to implement the principle of storage limitation include; ☐ Having clear internal procedures for deletion and destruction; ☐ Determining what data and length of storage of personal data that is necessary for the purpose; ☐ Formulating internal retention statements of implementing them; ☐ Ensuring that it is not possible to re-identify anonymized data or recover deleted data and testing whether this is possible; ☐ The ability to justify why the period of storage is necessary for the purpose, and disclosing the rationale behind the retention period; and ☐ Determining which personal data and length of storage is necessary for back-ups and logs.	DPA [regulation 35 of 2021]
Elements for principle of fairness	The data controller/ processor has incorporated elements necessary to implement the principle of fairness that include; ☐ Granting the data subjects the highest degree of autonomy with respect to control over their personal data; ☐ Enabling a data subject to communicate and exercise their rights; ☐ Elimination of any discrimination against a data subject; ☐ Guarding against the exploitation of the needs or vulnerabilities of a data subject; and ☐ Incorporating human intervention to minimize biases that automated decision-making processes may create.	DPA [regulation 36 of 2021]

Notification of data breach to Data commissioner	The data controller/ processor subject to section 43 of the Act sends a notification of a data breach to the Data Commissioner that includes; ☐ The date on which and the circumstances in which the data controller or data processor first became aware that the data breach had occurred; ☐ 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; ☐ Details on how the notifiable data breach occurred, where applicable; ☐ The number of data subjects or other persons affected by the notifiable data breach; ☐ The personal data or classes of personal data affected by the notifiable data breach; ☐ The potential harm to the affected data subjects as a result of the notifiable data breach; ☐ 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 Commissioner of the occurrence of the notifiable data breach to— ○ Eliminate or mitigate any potential harm to any affected data subject or other person as a result of the notifiable data breach; or ○ 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; or	DPA [regulation 37(1) of 2021]

	☐ Contact information of an authorized representative of the data controller or data processor The data controller/ processor that declines to communicate a notifiable data breach to a data subject affected by such breach, under the conditions set out in section 43(1) (b) of the Act, the notification to the Data Commissioner under sub-regulation (1) shall additionally specify the grounds for not notifying the affected data subject	
Transfer of personal data outside Kenya **General principles for transfers of personal data out of the country**	The data controller/ processor who is a transferring entity shall before transfer personal data out of Kenya ascertain that the transfer is based on; ☐ Appropriate data protection safeguards; ☐ An adequacy decision made by the Data Commissioner; ☐ Transfer as a necessity; or ☐ Consent of the data subject.	DPA [regulation 40 of 2021]
Transfers on the basis of appropriate safeguards	The data controller/ processor in processes where transfer of personal data to another country or a relevant international organization is based on the existence of appropriate safeguards must enforce the following; ☐ The transfer shall be documented; ☐ The documentation shall be provided to the Commissioner on request; and ☐ The documentation shall include ○ The date and time of the transfer; ○ The name of the recipient; ○ The justification for the transfer; and ○ A description of the personal data transferred.	DPA [regulation 41(1) of 2021]

	For the purpose of confirming the existence of appropriate data protection safeguards anticipated under section 49 (1) of the Act and these Regulations, any country or a territory is taken to have such safeguards if that country or territory has; ☐ Ratified the African Union Convention on Cyber Security and Personal Data Protection; ☐ A reciprocal data protection agreement with Kenya; or ☐ A contractual binding corporate rules among a concerned group of undertakings or enterprises.	
Binding corporate rules	The binding corporate rules shall specify; ☐ The structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members; ☐ The data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of ☐ another country or countries in question; ☐ Their legally binding nature, both internally and externally; ☐ The application of the general data protection principles; ☐ The rights of data subjects in regard to processing and the means to exercise those rights; ☐ The complaint procedures; and ☐ The mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules.	DPA [regulation 43(1) of 2021]

Transfers on the basis of an adequacy decision	The Data Commissioner may publish on its website a list of the countries, territories and specified sectors within that other country and relevant international organization for which the Data Commissioner has decided that an adequate level of protection is ensured	DPA [regulation 44(1) of 2021]
Transfers on the basis of necessity	Data controller/ processors may transfer personal data to another country or territory on the basis of necessity is such a transfer is necessary for any of the purpose outlined under section 48 (c) of the Act, and the transferring entity ascertains that; ☐ That the transfer is strictly necessary in a specific case outlined under section 48(c) of the Act; ☐ There are no fundamental rights and freedoms of the data subject concerned that override the public interest necessitating the transfer	DPA [regulation 45(1) of 2021]
Transfer on the basis of consent	The data controller/ processor in accordance with section 25 (g) of 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 another country shall take place only on the condition that the data subject; ☐ Has explicitly consented to the proposed transfer; and ☐ Has been informed of the possible risks of such transfers.	DPA [regulation 46(1) of 2021]

Subsequent transfers	The data controller/ processor where personal data is transferred in accordance with the Act, the entity effecting the transfer shall make it a condition of the transfer, that the data is not to be further transferred to another country or territory without the authorization of the transferring entity or another competent authority A competent authority may give an authorization only where the further transfer is necessary for a law enforcement purpose	DPA [regulation 47(1) of 2021]
Provisions for the agreement to cross border transfer	The data controller/ processor may enter into a written agreement with the recipient of personal data, which shall contain provisions relating to; ☐ Unlimited access by the transferring entity to ascertain the existence of a robust information system of the recipient for storing the personal data; and ☐ The countries and territories to which the personal data may be transferred under the contract	DPA [regulation 48 of 2021]
Processing activities requiring data protection impact assessment	The data controller/ processor in accordance with section 31 (3) of the Act, is required to consult the Data Commissioner on the data protection impact assessment prior to processing, such consultations shall be done within sixty days from the date of the receipt of the impact statement report. The data Controller/ processor shall provide; ☐ The data protection impact assessment prepared under section 31(1) of the Act; and ☐ Where applicable, the respective responsibilities of the data controller or data processors involved in the processing.	DPA [regulation 49(1) of 2021]
Exemption for national security	A data controller/ processor who processes personal data for national security and wishes to be exempt on that ground shall apply to the Cabinet Secretary for an exemption.	DPA [regulation 54(1) of 2021]

Exemptions for public interest	The processing of personal data is exempted from the Act on the grounds of public interest where such processing exists as a; ☐ Permitted general situation; or ☐ Permitted health situation. A permitted general situation referred to under regulation 55 (a)relates to the collection, use or disclosure by a data controller or data processor of personal data about data subject including for; ☐ Lessening or preventing a serious threat to the life, health or safety of any data subject, or to public health or safety; ☐ Taking appropriate action in relation to suspected unlawful activity or serious misconduct; ☐ Locating a person reported as missing; ☐ Asserting a legal or equitable claim; ☐ Conducting an alternative dispute resolution process; or ☐ Performing diplomatic or consular duties. A permitted health situation referred to under regulation 55 (b) relates to the collection, use or disclosure by a data controller or data processor of personal data about a data subject, including for; ☐ The collection of health information to provide a health service; ☐ The collection, use, or disclosure of health data is for health research and related purposes; ☐ The use or disclosure of genetic information where necessary and obtained in course of providing a health service; ☐ The disclosure of health information for a secondary purpose to a responsible person for a data subject.	DPA [regulation 55(1) of 2021]

	A permitted health situation under sub-regulation (1) applies where a data controller or data processor discloses health data about a data subject, and; ☐ They provide a health service to the data subject; ☐ The recipient of the personal data is a responsible person for the data subject; ☐ A data subject is either physically or legally incapable of giving consent to the disclosure, or physically cannot communicate consent to the disclosure; ☐ The disclosure is necessary to provide appropriate care or treatment of a data subject, or the disclosure is made for compassionate reasons; ☐ The disclosure is not contrary to any wish expressed by the data subject before the data subject became unable to give or communicate consent of which the carer is aware or of which the carer could reasonably be expected to be aware; ☐ and ☐ The disclosure is limited to the extent reasonable and necessary to provide appropriate care or treatment of the individual or to fulfil the purpose of making a disclosure for compassionate reasons.	