NATIONAL ASSEMBLY OF THE REPUBLIC OF KENYA

Privacy & Data Protection Bill 2018 Mastercard Memorandum

12 SEPTEMBER 2018

mastercard

The National Assembly of the Republic of Kenya's Data Protection Bill represents an important opportunity to help define the fourth fastest-growing digital economy in the world.[1] In 2017, one in every ten mobile transactions in the world was made in Kenya.[2] Between 2012 and 2017, the number of point of sale terminals in Kenya grew by 107 per cent, and the number of payment cards by 150 per cent.[3] Kenya is a rapidly-growing digital economy and Mastercard is grateful to be able to contribute to this important legislation for its future.

Mastercard is a technology company in the global payments industry. We operate the world's fastest payment processing network, connecting consumers, financial institutions, merchants, governments and businesses in more than 210 countries and territories. We are not a bank and do not extend credit to individuals or businesses. Our products and solutions make everyday commerce activities – such as shopping, travelling, running a business and managing finances – easier, more secure and more efficient for everyone.

Beyond this, Mastercard is committed to financial inclusion: bringing those who presently do not benefit from financial services into the banking system. We have partnered with the Government of Kenya to bring the first multipurpose social payment card, Huduma, to the nation in February 2017. The pre-paid card empowers individuals to make payments whilst automatically enrolling them in government schemes such as the National Social Security Fund (NSSF) and National Hospital Insurance Fund (NHIF). The Mastercard Farmer Network (formerly 2Kuze) and Kionect digital supply chain platform are providing smallholder farmers and micro-retailers with access to mobile-based lending. In partnership with Unilever, we also provide banks in Kenya with a low-cost means of assessing credit eligibility. All of these initiatives are possible because we and our partners are able to process personal data to supply these services.

Our comments reflect our experiences in providing both payment processing and financial inclusion initiatives, as well as observations we have given on similar laws in jurisdictions throughout the world.

EXECUTIVE SUMMARY

Privacy, human rights and the digital economy can be protected together

In his speech at a symposium on the digital economy at the Strathmore College, Nairobi, on 28 February 2018, President Kenyatta stated that "the internet and associated digital trade of goods and services have led up to 10 percent rise in employment in Africa." The President further remarked that "the potential for digital dividends is enormous if its transformational potential is harnessed by creating the right policy framework." We believe that the present Bill is an essential part of this framework, with the potential to enable digital growth and establish Kenya as an African paradigm for data protection.

[1] The Fletcher School, Tufts University, *Digital Planet 2017: How Competitiveness and Trust in Digital Economies Vary Across the World*, available at: https://sites.tufts.edu/digitalplanet/2017-digital-evolution-index/ (last accessed 20 July 2018)
[2] Lafferty Group, *Country Report: Kenya 2017*, available at: http://reports.lafferty.com/reports-store/cards-payments-research-service/country-reports/africa/kenya.html (last accessed 06 September 2018)
[3] *Ibid*.

As part of that framework, we believe that an individual's human right to privacy is best safeguarded by data protection laws that embed individual rights into every stage of data processing. Art 31(c) of the Constitution of the Republic of Kenya guarantees that no Kenyan citizen should have their private information unnecessarily required or revealed. We believe this can be achieved by legislation that incorporates data protection principles and norms that seek to ensure the proper management of privacy risks.

Summary of our recommendations

1. **Definition of sensitive personal data:** The rigorous protection and restrictions placed upon sensitive personal data should protect data with an inherent risk of prejudice to individuals, and not their "personal financial expenditures"
2. **Definition of personal data:** The Bill should encourage greater use of de-identification techniques to protect individuals' information by removing pseudonymised and otherwise de-identified data from its scope
3. **Local storage requirements:** The Bill should enable the movement of data outside Kenya to support its international digital economy
4. **Registration of entities:** The Bill should encourage greater self-regulation by avoiding imposing onerous registration requirements on entities
5. **Breach notification:** Compulsory notification should occur where there is a risk of serious harm to individuals only, to protect individuals' interests whilst ensuring the Commission is not overburdened

Our detailed proposals are followed by a chart of suggested drafting amendments for ease of reference.

OUR RECOMMENDATIONS

Definition of 'Sensitive Personal Data'

The Bill defines "sensitive personal data" to include information relating to "personal financial expenditures" (clause 2). This inclusion is unusual in global data protection laws,[4] and subjects information relating to an individual's purchases, banking and consumption patterns to the protections usually afforded to data with the inherent potential to cause prejudice or discrimination to the individual. Such protections are incredibly restrictive and would prohibit such data being used to provide financial and payment services to individuals and organisations across Kenya.

The Bill prohibits processing sensitive personal data except in limited conditions that would not permit most business processing,[5] and prohibits its transfer out of Kenya[6] or use in producing automated decisions completely.[7] These restrictions would prevent most of the operations of international fintechs like Mastercard in Kenya, including financial inclusion initiatives and fraud prevention technology.

[4] DLA Piper's *Data Protection Laws of the World 2017* identifies 68 countries with definitions of 'sensitive personal data' in their privacy legislation. Of these, only Israel includes any financial information (defined as "economic circumstances"). See also Rama Vedashree's note on the Indian Personal Data Protection Bill 2018, available as part of the Committee of Experts' Report, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, available at: http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last accessed 06 September 2018)

[5] Clauses 39-43

[6] Clause 44(3)

[7] Clause 31(3)

Payment processing does not involve any of the grounds listed in clauses 40 or 41 in relation to sensitive personal data,[8] yet represents a vital part of the digital economy in Kenya. There are currently over 212 million payment card transactions processed in Kenya each year, and over 1.8 billion mobile payments.[9] Without the ability to process such information, the major benefits the digital economy is able to bring to Kenya could not be realised.

The ability to transfer financial transaction data outside Kenya is also vital for the management of the payments system, including for the performance of fraud analytics and prevention measures. These techniques rely on identifying fraud trends across countries, and utilising these insights in Kenya to prevent fraudulent transactions. The technology used to identify and prevent fraud also involves computer algorithms which may be classed as "automated decision-making" in relation to affected transactions. The prohibition of such automated analysis with transaction data would have the effect of preventing fraud prevention techniques across the payment processing network, threatening the financial wellbeing of Kenyan financial institutions, merchants and consumers.

Recommendation: The reference to "personal financial expenditures" in the definition of "sensitive personal data" in clause 2 should be removed.

De-identified Data

The Bill recognises that anonymised data – from which identification of any individual is no longer possible – should not be regulated as 'personal data.' We welcome this approach and recommend further that the use of pseudonymised and otherwise de-identified data – where re-identification is only possible through use of onerous and disproportionate means unlikely to be used by the data controller or processor – should also be removed from the scope of the Bill.

Data about a person is often processed to reduce the risk of identification (known as de-identification), including techniques referred to as 'anonymisation' and 'psuedonymisation.' This type of processing is an important way to protect individuals whilst allowing analysis to be carried out for the benefit of all participants in the digital economy, and for Kenya as a whole. Uses include developing detailed insights into how the economy is functioning, where potential service gaps exist, and where fraud may be committed. Several jurisdictions have provided greater regulatory certainty for the use of these de-identification techniques, recognising their importance in enabling innovation and supporting broader economic objectives. These include the United Kingdom, Singapore, Australia, and European Union.[10]

[8] These are: processing for not-for-profit bodies (cl 40(1)(a)), where data is manifestly made public by the subject (cl 40(1)(b)), where necessary for the establishment, exercise or defence of legal claims (cl 40(1)(c)(i)), where necessary for carrying out obligations and exercising rights under employment law (cl 40(1)(c)(ii)), where necessary to protect the vital interests of the data subject or another where the subject cannot consent (cl 40(1)(c)(iii)), and where necessary for the provision of healthcare (cl 41).

[9] Lafferty Group, *Ibid*.

[10] United Kingdom Information Commissioner's Office, *Anonymisation: managing data protection risk code of practice*, available at: https://ico.org.uk/media/1061/anonymisation-code.pdf (last accessed 23 July 2018); Singapore Personal Data Protection Commission, *Guide to Basic Data Anonymisation Techniques*, available at: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-

We propose that the definition of personal data include a "reasonableness" test to require processing agencies to consider the scope of personal data *in the context of each use*. This reasonableness approach has been adopted in other countries including Hong Kong, Australia, Singapore, the Philippines, and the European Union in its General Data Protection Regulation (GDPR).[11]

Recommendation: The definition of 'personal data' in clause 2 should include a reference to reasonableness, and exclude data from which the identification of the data subject may only be achieved through onerous or disproportionate means that are unlikely to be used by the controller or processor.

Local storage requirements

The requirement in clause 44 for a "serving copy" of all data within the territory of Kenya creates undue administrative, technical and financial burdens on entities operating in the digital economy, with no concomitant benefits to Kenyan citizens. The requirement to copy data and store it within Kenya would slow the ability of payment technology companies like Mastercard to carry out payment processing, particularly of international payments, and to perform additional security and fraud prevention analytics that rely upon international data trends to operate.

'Data localisation' has been shown to have detrimental effects on economies, notably in Africa. Research from the Faculty of Economic & Political Science at Cairo University recently found that restrictions on international data transfers hinder "the necessary and essential role of global trade in realising economic development."[12] The report found that "this is evident in production costs as reflected in the increase in the prices of goods, which would lead to a decline in incomes." Prohibiting transfers or requiring expensive 'mirror' storage will prevent the operations of many fintech companies in Kenya, such as fraud prevention analysis, and more broadly will limit the benefits of the international digital economy that Kenya is able to enjoy.

We welcome the recognition of multiple legal bases to transfer personal data outside Kenya, following data hubs such as Singapore, Hong Kong and Malaysia, as well as the European Union,[13] but recommend that the prohibition on transferring certain data outside Kenya be lifted in accordance with such international standards. The designation of "critical personal data"

Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf (last accessed 23 July 2018); Office of the Australian Information Commissioner, *De-identification and the Privacy Act*, available at: https://www.oaic.gov.au/agencies-and-organisations/guides/de-identification-and-the-privacy-act (last accessed 23 July 2018); European Union, *Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques*, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (last accessed 23 July 2018).

[11] Hong Kong Personal Data (Privacy) Ordinance 1995, s2(1); Australia Privacy Act 1988, s6(1); Singapore Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 27 July 2017), para 5.13, available at: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisory-guidelines-on-key-concepts-in-the-pdpa-(270717).pdf (last accessed 23 July 2018); General Data Protection Regulation, Art 4(1).

[12] Mona Farid Badran, (2018) "Economic impact of data localization in five selected African countries", *Digital Policy, Regulation and Governance*, Vol. 20 Issue: 4, pp.337-357, available at: https://doi.org/10.1108/DPRG-01-2018-0002 (last accessed 20 July 2018).

[13] Singapore, Personal Data Protection Act, s26(1); Hong Kong, Personal Data (Privacy) Ordinance (to be brought into force in near future), s33; Malaysia, Personal Data Protection Act 2010, s129; General Data Protection Regulation, Arts 44-50.

in clause 44(2) should be subject to clear, published guidelines on which data may be affected, and designation should follow consultation with potentially-affected entities, and an appeals process. This is to ensure that any restrictions upon processing are implemented only after careful consideration of the risks and benefits to the Kenyan economy, on a case-by-case basis. Whilst Mastercard maintains that the storage of copies of data within the country adds no security or efficiency benefit for data subjects, the requirement to store a copy in Kenya may be a more practical solution to any concerns the Government of the Republic of Kenya may have over maintaining physical availability of critical data, whilst allowing processing of additional sets to take place outside the country to reduce impediments upon the digital economy.

The transfer of sensitive personal data outside Kenya should be permissible where strict safeguards are in place and there is no disproportionate risk to data subjects. Whilst Mastercard supports the protection of data with inherent risk of prejudice to data subjects,[14] we recommend that processing this data outside the territory of Kenya continue to be permissible, in order to facilitate important initiatives relating to public health, employee welfare and legal claims. Prohibiting sensitive employee data from being processed centrally by multi-national organisations such as Mastercard will result in restrictions on internal auditing and controls, and may result in prejudice to employees themselves. As with critical data, a local secure copy would be a preferable measure to an outright prohibition of extraterritorial transfers.

Recommendations: The requirement to store a "serving copy" of all data should be removed from the Bill.

The designation of "critical personal data" should be subject to clear, published guidelines on the data categories that may be affected, and designation should follow consultation with potentially-affected entities as well as an appeals process. The requirement for all processing of critical data to take place in Kenya should be amended to the storage of a copy within Kenya.

The transfer of sensitive personal data outside Kenya should be permissible where strict safeguards are in place and there is no disproportionate risk to data subjects.

Registration of entities

Registration with supervisory authorities represents an administrative burden for controllers and processors, without concomitant benefits for data subjects. Other jurisdictions, most notably Europe in its GDPR, are moving away from registration in their regulatory frameworks, instead preferring self-assessment and internal controls as a means to ensure privacy compliance within entities. "Privacy by design" is an example of this principle, seen in GDPR and reports by Canada's Privacy Commissioner, the US Federal Trade Commission, Australia's Commissioner for Privacy in the State of Victoria and in the International Conference of Data Protection and Privacy

[14] Subject to comments in section 1 relating to the exclusion of financial information from the definition of "sensitive personal data"

Commissioners' *Mauritius Declaration on the Internet of Things*.[15] It ensures that those responsible for personal data embed privacy principles into their processes and activities from the outset, without the requirement to register with external organisations. This is the approach we recommend for Kenya.

Recommendation: The requirement for controllers and processors to register with the Data Commissioner should be removed from the Bill.

Data incident notification threshold and period

We welcome the inclusion of data security requirements in the Bill, as well as provisions requiring instances of unauthorised access to personal data to be identified and rectified. In particular we support the Bill's reserving of mandatory incident notification requirements to data to which security measures have not been applied. This encourages good practice and ensures that security issues relating to data suitably protected will not be subject to unnecessary notification to the Commission.

We propose that the concept of risk and harm to the individual be incorporated into all data breach requirements. Clause 38 presently requires notification to both the Commission and data subject in all instances in which data is held without additional security measures, where there are reasonable grounds to believe that an unauthorised person has accessed or processed personal data. This is a low threshold, and may have the effect of requiring many potential incidents to be reported, raising alarm with data subjects, where no actual harm has occurred.

We would recommend an approach where notification occurs to the Commission and data subjects only where unauthorised processing or access has occurred that is likely to result in significant harm to the data subject. This approach would ensure that the Commission is fully involved in data incident management, but remains able to respond in serious circumstances without being burdened by numerous trivial but compulsory notifications. Such a threshold may be seen in the European Union's GDPR, and the privacy laws of Australia and Canada.[16]

Setting a time period for notifications often mandates notification before all facts are known, causing concern for individuals without any additional protection of their interests. We recommend that no time period is set for

[15] See GDPR Art 25; Office of the Privacy Commissioner of Canada, 'Privacy, Trust & Innovation – Building Canada's Digital Advantage' (2010) available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_de_201007/ (last accessed 04 September 2018); US Federal Trade Commission, 'Protecting Consumer Privacy in an Era of Rapid Change' (2012), available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (last access 04 September 2018); Office of the Victorian Information Commissioner, 'Privacy by design: Effective privacy management in the Victorian public sector' (July 2018), available at: https://ovic.vic.gov.au/resource/privacy-by-design-effective-privacy-management-in-the-victorian-public-sector/?highlight=privacy%20by%20design (last accessed 04 September 2018); Mauritius Declaration on the Internet of Things (2014), in particular: "Privacy by design and default should no longer be regarded as something peculiar. They should become a key selling point of innovative technologies," available at: https://icdppc.org/wp-content/uploads/2015/02/Mauritius-Declaration.pdf (last accessed 04 September 2018).

[16] GDPR Art 33 requires notification to the supervisory authority only where the unauthorised access is likely to result in a risk to the rights and freedoms of the data subject. Australia, Privacy Act 1988, Part IIIC requires notification where the unauthorised access is "likely to result in serious harm to any individuals whose personal information is involved in the breach." Canada, Personal Information Protection and Electronic Documents Act (PIPEDA, as amended by the Digital Privacy Act 2015), s10.1 requires notification where there is a "real risk of significant harm to the individual."

mandatory notifications, or alternatively that notification be required only when the data controller is in possession of sufficient information to assess the real risk of harm to the individual data subject.

Recommendation: Data breach notification should be mandatory only when there is a real risk of serious harm to data subjects. No arbitrary time period for such notification should be set.

Conclusion

Mastercard would like to thank the National Assembly of the Republic of Kenya for receiving our submission on this important legislation. As a global payments and technology company, we are committed to respecting and safeguarding the personal data of our cardholders and customers. We are also committed to working with the Government of the Republic of Kenya to develop and refine this significant legislation in a manner that protects the individual, ensures ease of commerce, and helps to promote financial inclusion throughout Africa.

We remain at your disposal for any further insights you may require.

ANNEX
PROPOSED AMENDMENTS TO THE PRIVACY & DATA PROTECTION BILL 2018

CLAUSE	AMENDMENT	DRAFTING SUGGESTION Suggested amendments are shown in bold underline
2: Definition of personal data	The definition of 'personal data' in clause 2 should include a reference to reasonableness, and exclude data from which the identification of the data subject may only be achieved through onerous or disproportionate means that are unlikely to be used by the controller or processor.	"Personal data" means any information ~~**relating to an identified or identifiable natural person**~~ **from which a living individual can reasonably be identified using information in the possession of the controller or processor processing the data**;
2: Definition of sensitive personal data	The definition of 'sensitive personal data' in clause 2 should exclude reference to 'personal financial expenditures.'	"Sensitive personal data" means data revealing the natural person's race, health status, ethnic social origin, political opinion, belief, person preferences, location, genetic data, biometrics, sex life or sexual orientation, ~~**personal financial expenditures,**~~ of the data subject;
2: Definition of register	The requirement for data controllers and processors to register with the Data Commission should be removed.	~~**"Register" means the register as established and maintained by the Data Commissioner under section 19;**~~
15: Registration of entities	The requirement for controllers and processors to register with the Data Commission should be removed.	~~**15. Subject to exemptions provided under this act, no person shall act as a data controller or data processor unless registered with the data commissioner**~~
16: Application for registration		~~**16. (1) every person who intends to act as a data controller or data processor shall apply to the data commissioner in prescribed form.**~~ ~~**(2) an application under subsection (1) shall provide the following particulars –**~~ ~~**(a) a description of the personal data to be processed by the data controller or data processor, and of the**~~

		~~category of data subjects, to which the personal data relates;~~ ~~(b) a statement as to whether the data controller or data processor is likely to hold any categories of sensitive personal data;~~ ~~(c) a description of the purpose for which the personal data is to be processed;~~ ~~(d) a description of any recipient to whom the data controller or data processor intends or may intend to disclose the personal data;~~ ~~(e) the name, or a description of, any country to which the proposed data controller intends or may wish, directly or indirectly, to transfer the personal data;~~ ~~(f) statement as to a representative for the purposes of this act and details of such representative;~~ ~~(g) a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of personal data; and~~ ~~(h) any other details as may be prescribed by the data commissioner.~~ ~~(3) a data controller or data processor who knowingly supplies any false or misleading detail under subsection (1) commits an offence.~~ ~~(4) the data commissioner shall issue a certificate of registration to an applicant who satisfies the criteria to be registered as a data controller or data processor.~~ ~~(5) where there is a change in any particular outlined under subsection (2), the data controller or data processor shall notify the data commissioner of such change in prescribed period.~~ ~~(6) on receipt of a notification under subsection (5), the data commissioner shall amend the respective entry in the register.~~ ~~(7) a data controller or data processor who fails to comply with the provisions of subsection (5) commits an offence.~~
17: Duration of the registration certificate		~~17. A registration certificate issued under section 16 shall be valid for a period of three years and the holder may apply for the renewal within a prescribed period.~~

18: Register of data controllers and data processors		~~**18. (1) the data commissioner shall keep and maintain a register of the registered data controllers and data processors.**~~ ~~**(2) the data commissioner may, at the request of a data controller or data processor, remove any entry in the register which has ceased to be applicable.**~~ ~~**(3) the register shall be a public document and available for inspection by any person.**~~ ~~**(4) a person may request the data commissioner for a certified copy of any entry in the register.**~~
19: Cancellation or variation of the certificate		~~**19. The data commissioner may, upon issuance of a notice to show cause, cancel or vary terms and conditions of the certificate of registration where—**~~ ~~**(a) any information given to by the applicant is false or misleading; or**~~ ~~**(b) the holder of the registration certificate, without lawful excuse fails to comply with any —**~~ ~~**(i) requirement of this act; or**~~ ~~**(ii) term or condition specified.**~~
21: Designation of the Data Protection Officer	The requirement for controllers and processors to register with the Data Commissioner should be removed.	21. (1) A data controller or data processor may designate or appoint a data protection officer on such terms and conditions as the data controller or data processor may determine, where— (a) the processing is carried out by a public body or private body, except for courts acting in their judicial capacity; (b) the core activities of the data controller or data processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the data controller or the data processor consist of processing on a large scale of sensitive categories of personal data.

		(2) A data protection officer may be a staff member of the data controller or data processor and may fulfil other tasks and duties provided that any such tasks and duties do not result in a conflict of interest. (3) A group of entities may appoint a single data protection officer provided that such officer is easily accessible by each entity. (4) Where a data controller or a data processor is a public body, a single data protection officer may be designated for several such public bodies, taking into account their organisational structures. (5) A person may be designated or appointed as a data protection officer, if that person has relevant academic or professional qualifications which may include knowledge and technical skills in matters relating to data protection. **~~(6) A data controller or data processor shall publish the contact details of the data protection officer and communicate them to the Data Commissioner.~~** (7) The responsibility of a data protection officer shall be to — (a) advise the data controller or data processor and their employees on data processing requirements provided under this Act or any other written law; (b) ensure on behalf of the data controller or data processor that this Act is complied with; (c) facilitate capacity building of staff involved in data processing operations; (d) provide advice on data protection impact assessment; and (e) Cooperate with the Data Commissioner and any other authority on matters relating to data protection.
38: Notification of breach of security of personal data	Data breach notification should be mandatory only when there is a real risk of serious harm to data subjects. No arbitrary time period for such notification should be set.	38. (1) Where **~~there is a breach of security of personal data or there is reasonable ground to believe~~** personal data has been accessed or acquired by an unauthorised person, **and there is a real risk of harm to the data subjects whose personal data has been subject to the unauthorised access,** the data controller or data processor, **~~within prescribed period,~~** shall— (a) notify the Data Commissioner; and

		(b) subject to subsection (3), communicate to the data subject, unless the identity of the data subject cannot be established. (2) Where a data processor becomes aware of a personal data breach, the data processor shall notify the data controller **~~within the prescribed period.~~** **as soon as reasonably practicable.** (3) The data controller may delay notification referred under subsection (1) (b), for purposes of prevention, detection or investigation of offences by the concerned public body. (4) The notification to the data subject shall be in writing and shall be communicated in the prescribed manner. (5) The notification and communication referred to under subsection (1) shall provide sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach, including — (a) description of the nature of the data breach; (b) description of the measures that the data controller or data processor intends to take or has taken to address the data breach; (c) recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise; (d) where applicable, the identity of the unauthorised person who may have accessed or acquired the personal data. (6) The notification of a breach of security of personal data shall not be required where the data controller or data processor has implemented appropriate security safeguards which may include encryption of affected personal data;
44: Rules as to data centres and servers	The requirement to store a "serving copy" of all data should be removed from the Bill. The designation of "critical personal data" should be subject to clear, published guidelines on which data may be affected, and designation should follow consultation with potentially-affected entities and an appeals	44. **~~(1) Every data controller or data processor shall ensure the storage, on a server or data centre located in Kenya, of at least one serving copy of personal data to which this Act applies.~~** (2) The Cabinet Secretary shall prescribe, based on grounds of strategic interests of the state or on protection of revenue, categories of personal data as critical personal data that shall only be processed in a server or data centre located in Kenya. **(3) Before designating categories of data as critical personal data, the Cabinet Secretary shall consult widely with controllers and processors potentially affected by such designation and provide such controllers and processors an**

	process. The requirement for all processing of critical data to take place in Kenya should be amended to the storage of a copy within Kenya. The transfer of sensitive personal data outside Kenya should be permissible where strict safeguards are in place and there is no disproportionate risk to data subjects.	**opportunity to make representations to him concerning the proposed designation.** **(4) Where the Cabinet Secretary receives representations from potentially-affected entities opposing the designation of certain categories of data as critical personal data, he shall, prior to designating such data as critical personal data, give written reasons to the potentially-affected entity for his decision to designate such categories of data as critical personal data.** **(5) The Cabinet Secretary shall publish guidelines on the designation of categories of personal data as critical personal data, including guidelines on the criteria to be used in determining the categories of personal data that may be considered for designation as critical personal data and on the strategic interests of state and protection of revenue to be taken into consideration in reaching such determination.** ~~**(6) Cross-border processing of sensitive personal data is prohibited.**~~
45: Conditions for transfer out of Kenya	The transfer of sensitive personal data outside Kenya should be permissible where strict safeguards are in place and there is no disproportionate risk to data subjects.	45. (1) A data controller or data processor may transfer personal data to another country where— (a) the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data; (b) the data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer such as the absence of appropriate security safeguards; **or** (c) the transfer is necessary for – (i) the performance of a contract between the data subject and the data controller or data processor or implementation of pre-contractual measures taken at the data subject's request; (ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person; (iii)for any matter of public interest; (iv) for the establishment, exercise or defence of a legal claim;

		(v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or (vi) 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. **(2) A data controller or data processor may transfer sensitive personal data to another country where—** **(a) the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the sensitive personal data;** **(b) the data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer such as the absence of appropriate security safeguards; or** **(c) the transfer is necessary –** **(i) for the conclusion or performance of a contract concluded in the interest of the data subject;** **(ii) for the establishment, exercise or defence of a legal claim; or** **(iii) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.**