ARTICLE 19

Uganda: Data Protection and Privacy Bill

July 2016

Legal analysis

Table of contents

Executive Summary

In July 2016, ARTICLE 19 analysed the Draft Data Protection and Privacy Bill (Draft Bill), proposed by the Government of Uganda, for its compliance with international freedom of expression standards.

The Draft Bill is a welcome step towards establishing a framework for protecting the fundamental right to privacy in the country. However, ARTICLE 19 finds that the Draft Bill needs to better harmonize its protections with the fundamental rights of freedom of expression and the right to information. ARTICLE 19 makes specific recommendations in this regard and calls on the Ugandan Government to consider these recommendations in the process of finalising the Draft Law.

Summary of recommendations:

1. Clause 1 of the Bill should clarify that the Bill applies both to natural and legal persons, namely that it also applies to the corporate sector;
2. The definitions in Clause 2 should be more closely aligned with best practice in this area;
3. Clause 3 should be more comprehensive and at the very least include the purpose limitation principle and the "minimality" principle;
4. The Bill should provide for a broad exemption for the purposes of communicating information to the public, communicating ideas, or opinions of general interest including for journalistic purposes, and the purposes of academic, artistic, or literary expression;
5. Processing of personal data by natural persons for purely personal or household purposes should be excluded from the scope of the Bill. Such an exclusion should be interpreted broadly to cover the use of social media and the Internet by private individuals;
6. Clause 15 on trans-border transfers of personal data should include an exception for the protection of freedom of expression consistent with best practice in this area;
7. Clause 14 should at the very least set an upper limit on data retention for the purposes of national security and law enforcement. If applicable, it should make reference to existing data retention laws in Uganda;
8. Clause 12 should ensure that any rules on the deletion of public information are balanced with freedom of expression;
9. An independent oversight body should be created, with full powers to oversee the law, as well as the ability to receive and resolve complaints about its implementation by both public and private bodies. Decisions handed down by this independent oversight body should be subject to a right of appeal to an independent and impartial court;
10. Clause 31, which criminalises the unlawful obtaining and disclosure of personal data, should be redrafted to include a public interest defence;
11. The custodial sentences available under Clause 31 should be reduced.

Introduction

There is currently no specific law regulating the protection of personal data in Uganda. In 2014, however, the Ugandan Government published a draft Data Protection and Privacy Bill.[1] A new draft of the Bill was subsequently published in 2016 (Draft Bill).[2]

The Draft Bill states that its purpose is to protect the privacy of the individual and of personal data by collecting and regulating the collection and processing of personal information; to provide for the rights of the persons whose data is collected and the obligations of data collectors, data processors and data controllers; to regulate the use or disclosure of personal information; and for related matters. The memorandum in support of the Draft Bill makes it clear that the Bill is aimed at addressing the current gap in the law for the protection of personal data. In particular, it seeks to give effect to article 27 (2) of the Constitution, which protects the right to privacy, by setting out the principles of data protection and a number of data subjects' rights and remedies. The Draft Bill further proposes to entrust the oversight of the Bill to the National Information Technology Authority, Uganda (NTIA).

In this legal analysis, ARTICLE 19 reviews the provisions of the Draft Bill (the version after the first reading in the Parliament) in the context of international standards on freedom of expression. Although data protection laws are primarily concerned with the protection of the right to privacy, they can nonetheless have a significant impact on the right to freedom of expression. This includes but is not limited to investigative journalism, the disclosure of personal information by whistleblowers and access to public information. ARTICLE 19 supports the adoption of well-designed data protection laws, which protect individuals' rights whilst ensuring government transparency and protecting freedom of expression.

We conclude that the Draft Bill fails to recognise the importance of protecting the rights to freedom of expression and information as part of any data protection law. In particular, the Draft Bill fails to include a number of exemptions from data protection obligations for journalistic, literary, academic, artistic and other expressive purposes, as well as exemptions for purely personal and households purposes. We further highlight a number of concerns and make recommendations in relation to the retention of personal records, the right to be forgotten, the need for an independent oversight body and criminal offences.

[1] See Privacy International, *The Right to Privacy in Uganda,* March 2016.
[2] In this analysis, ARTICLE 19 reviews the Draft Data Protection and Privacy Bill, 2016 as available on the Ugandan Parliament website, the First Reading version.

Data Protection and Freedom of Expression and Information

Right to freedom of expression and information

The right to freedom of expression is a fundamental human right recognized in international human rights law. The full enjoyment of this right is central to achieving individual freedoms and to developing democracy. Freedom of expression is a necessary condition for the realisation of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of all human rights.

The right to freedom of expression is recognised in nearly every national constitution and in most international and regional human rights treaties including the Universal Declaration of Human Rights (UDHR),[3] the International Covenant on Civil and Political Rights (ICCPR),[4] the African Charter on Human and Peoples' Rights (African Charter),[5] the American Declaration of the Rights and Duties of Man (American Declaration),[6] and the American Convention on Human Rights (American Convention),[7] and the European Convention on Human Rights (European Convention).[8]

In General Comment No. 34, the UN Human Rights Committee (HR Committee) - the treaty body that authoritatively interprets the scope of states' obligations under the ICCPR - re-affirmed that freedom of expression is essential for the enjoyment of other human rights and confirmed that Article 19 of the ICCPR protects all forms of expression and the means of their dissemination, including all electronic and Internet-based modes of expression.[9] In other words, freedom of expression is protected online in the same way as it is protected offline.

However, freedom of expression is not absolute. International standards make it clear that freedom of expression is a qualified right which may be limited, provided the restriction complies with a three-part test. The restriction must:

- be provided by law;
- pursue the legitimate aims explicitly enumerated in Article 19 of the ICCPR; and
- be necessary in a democratic society. In particular, the requirement of necessity entails that the measure adopted must be proportionate to the aim pursued. If a less intrusive measure is capable of achieving the same purpose as a more restrictive one, the least restrictive measure must be applied. International law thus allows that freedom of expression may be subject to certain restrictions for the sake of other legitimate interests including, among other things, the rights of others. This includes, in principle, the right to privacy.

[3] UN General Assembly Resolution 217A(III), adopted 10 December 1948, Article 19.
[4] GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc, Article 19.
[5] The African Charter on Human and Peoples' Rights, adopted 26 June 1981, in force 21 October 1986, Article 9.
[6] The American Declaration of the Rights and Duties of Man, adopted on 2 May 1948, Article 4.
[7] The American Convention on Human Rights, adopted 22 November 1969, in force 18 July 1978,
[8] The European Convention on Human Rights, adopted 4 November 1950, in force 3 September 1953, Article 10.
[9] General Comment No. 34: Article 19 (Freedoms of opinion and expression), 12 September 2011, para 12.

Right to privacy and data protection

The right to privacy is also recognised in international human rights treaties including the UDHR[10], the ICCPR,[11] the European Convention,[12] the American Declaration[13], and the American Convention.[14] Under these treaties, privacy is a broad concept relating to the protection of individual autonomy and the relationship between an individual and society, including governments, companies and other individuals. It is commonly recognised as a core right that underpins human dignity and other values, such as freedom of association and freedom of opinion. It is also understood to be essential to private breathing space for individuals to be able to realise their other rights, including freedom of expression.

The protection of personal data (data protection) is recognized by the HR Committee as a fundamental part of privacy as protected by Article 17 of the ICCPR. The HR Committee in General Comment 16 stated that:

> The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant.[15]

The protection of personal data was guaranteed for the first time as a separate right granted to an individual in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).[16] It was adopted by the Council of Europe in 1981. In 1990, the UN General Assembly approved a Resolution on guidelines for the data protection of personal information held in computer databases.[17] The Guidelines set out 6 basic principles of data protection based on fair information practices. The European Union Charter of Fundamental Rights recognises the right of everyone to the protection of personal data concerning him or her, including that such data be processed fairly and for specified purposes and on the basis of consent or some other legitimate basis laid down by law.[18] The European Union Charter of Fundamental Rights also guarantees everyone's right of access to data which has been collected concerning him or her, the right to have it rectified, and that compliance with data protection rules be subject to control by an independent authority.[19] The rights of data protection have also been adopted in administrative and legal procedures across the globe.[20] For example, the EU Directive 95/46

---

[10] UDHR, *op.cit.*, Article 12.
[11] ICCPR, *op.cit.*, Article 17.
[12] European Convention, *op.cit.*, Article 8.
[13] American Declaration, *op.cit.*, Articles 5, 9 and 10
[14] American Convention, *op.cit.*, Article 11.
[15] HR Committee, CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, para 10.
[16] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108.
[17] Guidelines for the Regulation of Computerized Personal Data Files, G.A. res. 45/95, 14 December 1990, available at http://bit.ly/2arckCX..
[18] European Union Charter of Fundamental Rights, Articles 8(1) and 8(2).
[19] *Ibid.*, Articles 8(2) and 8(3).
[20] See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980); Canadian Standards Association (CSA) International, Model Code for the Protection of Personal Information, 1996; APEC

EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 95/46 EC) – to be replaced by the General Data Protection Directive by 2018 - also sets a benchmark in this area.

Privacy and freedom of expression and information

Privacy and freedom of expression are intertwined rights in human rights law. They appear together in international instruments, national constitutions and laws. Together they ensure the accountability of the state and other powerful actors to citizens.

It is important to note that the rights are mutually supportive. Freedom of expression and freedom of information allow individuals to investigate and challenge abuses to human rights including violations of privacy. Privacy allows individuals to work and communicate in a space unhindered by authority. As a practical matter, limits on privacy affect the ability of the media to operate. Journalists are not able to effectively pursue investigations and receive information from confidential and other sources.[21] Privacy laws can support freedom of expression by placing limits on the unlawful collection of personal information for political purposes, such as bodies creating dossiers or collecting data through surveillance activities to put pressure on journalists and others.

The European Commission in a recent impact assessment on the revised data protection regime noted that:

> Privacy and the protection of personal data ... play a key role for the exercise of fundamental rights in a broader sense. Many of the fundamental freedoms can only be fully exercised if the individual is reassured that it is not subject of permanent surveillance and observation by authorities and other powerful organisations. Freedom of thought, freedom of expression, freedom of assembly and association, but also the freedom to conduct a business will not be exercised fully by all citizens in an environment where the individual feels that each of her or his moves, acts, expressions and transaction is subject to scrutiny by others trying to control him or her. Exercise of these freedoms is crucial to maintain all fundamental rights.[22]

As two equal human rights, it is essential that states balance the two in a fair manner without giving precedence to one over the other. International human rights law does not recognise a hierarchy of rights, in which one trumps the other.

Privacy Framework, 2005; The Madrid Privacy Declaration, Global Privacy Standards for a Global World, 3 November 2009; Economic Commission of Western Africa, Supplementary Act A.SA.1/01/10 on Personal Data Protection within ECOWAS, 2010; Southern African Development Community (SADC) Model Law on Data Protection, 2012; and the Commonwealth Draft Model Law on the Protection of Personal Information, 2004.

[21] See e.g. IFEX Alert, Thirty IFEX members call on governments to respect fundamental human rights of free expression and privacy of communications, 5 June 2009.

[22] European Commission, Commission Staff Working Paper, Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) And Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, SEC(2012) 72 final, 25 January 2012.

At the same time, both rights can be limited under certain circumstances, subject to the three-part test outlined above. This means inter alia that States are not required to adopt measures that would protect the right to privacy where that would constitute an undue restriction on freedom of expression.[23] Simultaneously, under international human rights law, States are obliged to provide remedies for violations of either right.

[23] For example, a requirement for newspapers to notify the subjects of a news article before its publication; see European Court, *Mosley v the UK*, Appl. no. 48009/08, 10 May 2011.

Analysis of the Draft Bill

The Draft Bill consists of eight parts and one schedule. Part I deals with preliminary issues, such as definitions. The schedule specifies the currency in which the specified penalties would be incurred. The remaining parts contain substantive provisions, as follows:

- Part II outlines the principles of data protection, including accountability, lawfulness of processing, data security safeguards and data subject participation.
- Part III sets out the conditions for the collection and processing of personal data and provides for the right of correction and conditions for data export.
- Part IV deals with the security of data and the response to security breaches.
- Part V outlines the rights of data subjects, including the right to access personal information and the right to prevent the processing of personal data.
- Part VI establishes a Data Protection Register, in which every person, institution or public body collecting personal data will need to be registered.
- Part VII addresses complaints of non-compliance with the Bill and the National Information Technology Authority, Uganda's authority to investigate complaints.
- Part VIII sets out the offences and penalties for non-compliance with the obligations set out in the bill.

In the absence of comprehensive legislation for the protection of the rights to privacy and personal data in Uganda, the Bill is a welcome step forward for the protection of these rights. At the same time, the Bill has some significant shortcomings that need to be addressed. In this analysis, we outline our concerns with the Bill primarily from the perspective of freedom of expression.[24]

Scope, definitions and basic principles

Clause 1 of the Draft Bill provides that it applies to "any person, institution or public body collecting, processing, holding or using personal data." However, clause 1 does not specify whether the Act applies to both natural and legal persons. In other words, it fails to make clear that the Act applies to the corporate sector. Moreover, it is unclear what the term "institution" is intended to cover.

Clause 2 of the Draft Bill deals with a number of definitions. They generally constitute an improvement over an earlier version of the Bill, particularly as regards the definition of 'processing' and 'personal data.'[25] ARTICLE 19 notes, however, that some definitions could be further improved and brought more closely in line with international standards and best practice in this area, such as the Convention 108 or the European Directive 95/46 EC, mentioned above. In particular:

- **Personal data**: under Clause 2 (e), personal data includes information about a person from which the person can be identified, including *"other information which is in the*

[24] For a more detailed analysis of the privacy concerns with the Data Protection Bill 2014, we refer to Privacy International's Universal Periodic Report on *The Right to Privacy in Uganda*, available at http://bit.ly/2aFOPHa.
[25] See fn 23 above.

possession of the data controller, and includes an expression of opinion about the individual". The reference to someone's opinion about an individual is surprising and appears unduly subjective. We would refer to the definition under Directive 95/46 EC as a model clause in this area. Article 2 of the Directive provides that personal data means "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*" (our emphasis).

- **Data controller**: the definition of a data controller in the Bill refers to "a person" or "persons" determining the purpose and manner of processing. It is therefore not clear whether controllers include legal persons, such as companies. By contrast, Convention 108 or Directive 95/46 EC refer to a "natural or legal person, public authority, agency or any other body."

Part II, Clause 3 sets out basic principles of data protection. Whilst some improvements have been made (e.g. including a requirement that data is processed fairly and lawfully), we note that key data protection principles are still missing. In particular, Clause 3 fails to elaborate on the data quality principle, which at the very least should include a requirement that data be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.[26] Although Clause 8 goes some way towards addressing this problem, in our view, this should not prevent Clause 3 from setting out the principle of purpose limitation as part of *basic* data protection principles. Similarly, the data quality principle according to which personal data should be accurate and, where necessary, kept up to date is not included under Clause 3 but can be found in Clause 11. The same is true of Clause 10 (minimality). In our view, the drafters of the Bill should endeavour to regroup all principles related to data quality under the same clause (Clause 3) in order to bring greater clarity to the governing principles of data protection.[27] As it stands, the current approach appears piecemeal and makes the Bill harder to read.

Recommendations:

- Clause 1 should clarify that it applies both to natural and legal persons, i.e. that it also applies to the corporate sector;
- The definitions in Clause 2 should be more closely aligned with best practice in this area;
- Clause 3 should be more comprehensive and at the very least include the purpose limitation principle and the "minimality" principle.

Lack of exemption for journalistic, academic, artistic, literary or any other forms of expression

In ARTICLE 19's view, one of the most significant flaws of the Draft Bill is the failure to recognise the importance of the right to freedom of expression and information and its interaction with the rights to privacy and personal data. In particular, the Bill fails to make any reference to the right to freedom of expression, which is protected under Article 29 of the

[26] See for instance Article 6 of Directive 95/46 EC.
[27] *Ibid.*

Ugandan Constitution. Nor does it make any reference to the Uganda Access to Information Act 2005, despite the fact that the Act makes explicit reference to the protection of information relating to the privacy of a person (Section 26).[28]

Most importantly, the Bill entirely fails to provide for a broad exemption for the exercise of freedom of expression, including for journalistic, academic, artistic, literary or any other forms of expressive purposes. Rather, the Bill exempts the processing of personal data for statistical, historical or research purposes (Clauses 5(2), 13(3)(e) and 14(2)(f)). This is clearly insufficient and out of step with international standards and best practice in this area.

The common approach in most countries around the world that have adopted data protection acts is to include a specific exemption for journalistic, academic, artistic, literary and other cultural purposes, which allows for the rules limiting processing to be waived for those purposes.[29]

ARTICLE 19 believes, however, that even such exemptions should be expanded to reflect a broader recognition of freedom of expression interests. This is consistent with the language used in the revised data protection framework of the European Union, which will come into force in 2018. For example, for comparative purposes, we note that under the new EU General Data Protection Regulation (GDPR), Article 85 states that:

> ***Processing and freedom of expression and information***
> 1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.
> 2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information (...)[30]

Specific protections for freedom of expression are also being incorporated into the revisions of the Convention 108 on Data Protection. In the draft currently being considered, Article 9 states that member states should incorporate an exemption when it constitutes a necessary and proportionate measure for "the protection of the data subject or the rights and freedoms of others, notably freedom of expression."[31] Furthermore, revised Article 12.4 provides that

[28] The Access to Information Act of Uganda, 19 July 2005.
[29] *C.f.* also Article 14 (3) of the African Union Convention on Cyber-security and Data Protection.
[30] EU Directive 95/46/EC, The Data Protection Directive.
[31] Council of Europe, Ad Hoc Committee on Data Protection (CAHDATA), Working Document Consolidated Version of the Modernisation Proposals of Convention 108 with reservations, CAHDATA (2016)1, 3 May 2016 read in conjunction with CAHDATA (2016)RAPAbr, 16 June 2016.

each Party may provide that the transfer of personal data may take place if "it constitutes a necessary and proportionate measure in a democratic society for the freedom of expression."[32]

In the absence of a broad exemption for journalistic, artistic, literary or any other form of expressive purposes, anyone undertaking such activities would have to comply with a host of data protection obligations, which are incompatible with these expressive purposes. In particular, the obligation to ensure the accuracy of any information processed (Clause 11), the duty to inform the data subject of the processing (Clause 9), and the risk of being ordered to pay compensation when failing to meet these obligations (Clause 29) would have a significant chilling effect on freedom of expression in general and journalistic activity in particular. Clause 9, for instance, would in essence be tantamount to a pre-notification regime, which has been ruled as incompatible with the right to freedom of expression by the European Court of Human Rights.[33] Similar concerns would arise in relation to the powers of the Authority to rectify, block, erase or destroy inaccurate personal data under Clause 24.

Recommendations:

- The Bill should provide for a broad exemption for the purposes of communicating information to the public, communicating ideas, or opinions of general interest including for journalistic purposes, and the purposes of academic, artistic, or literary expression.

Lack of personal activities exemption and social media

The Draft Bill currently does not exclude any type of collecting or processing of personal data by natural persons in the course of purely personal or household activities. This has potentially significant implications for individuals who may be subject to extensive data protection obligations as a result.

For instance, in its current form, individuals who keep contact details of family members, friends or acquaintances on a personal computer in their home would be subject to the obligations under the Bill. Other activities that, in themselves, form part of an individual's right to privacy would also be subject to these data protection obligations, including the storing of a diary on a personal computer that contains the opinions of other individuals and private communications with friends or family over the internet that include personal data.

Furthermore, in its current form, posting information about another person on social media, such as posting a photo on Facebook or Instagram, could similarly trigger the applicability of obligations under the Data Protection Bill. This is deeply problematic in circumstances where the Draft Bill fails to provide for any meaningful way in which the rights to freedom of expression, data protection and privacy should be balanced. In any event, data protection law is ill-suited to regulate what it is acceptable for one individual to say or share about another. This is especially the case of the Uganda Data Protection Bill, which generally fails to include sufficient safeguards for the protection of freedom of expression. In particular, the Bill fails to include a public interest test or a reasonable expectation of privacy test in relation to the disclosure of personal information.

---

[32] *Ibid.*
[33] *Mosley v the UK*, *op.cit.*, para 132.

Recommendations:

- Processing of personal data by natural persons for purely personal or household purposes should be excluded from the scope of the Bill.
- Such an exclusion should be interpreted broadly to cover the use of social media and the Internet by private individuals.

Lack of exceptions for the protection of freedom of expression in trans-border transfers of data

The Bill places an obligation on data processors and data controllers to ensure that, where they process personal data outside Uganda, the country in which the data is processed has adequate measures in place for the protection of the personal data which are at least equivalent to the protection afforded by the Bill (Clause 15). Whilst this provision is relatively standard in relation to trans-border data flows, it is nonetheless incomplete. As noted above, both Article 85 of the General Data Protection Regulation and Article 12 (4) of the draft modernized version of Convention 108 provide for exemptions or exceptions for the protection of freedom of expression in relation to trans-border transfers of personal data. In the absence of such exceptions, Clause 15 could have a significant chilling effect on online expression and internet use more generally in Uganda.

Recommendation:

- Clause 15 should include an exception for the protection of freedom of expression consistent with best practice in this area.

Retention of records of personal data

Clause 14 of the Draft Bill deals with the retention of personal data records. Under Clause 14 (2), there is no limit to the period of retention of personal data collected for the purposes of national security or law enforcement. Furthermore, under Clause 34, the Minister is given broad powers to make regulations for the retention period of personal data. The Draft Bill otherwise fails to make any reference to any specific data retention law that might provide for such an upper limit. In our view, this is a grossly disproportionate interference with the rights to freedom of expression, privacy and data protection and out of step with best practice in this area.[34]

Recommendation:

- Clause 14 should at the very least set an upper limit on data retention for the purposes of national security and law enforcement. If applicable, it should make reference to existing data retention laws in Uganda.

[34] See *Digital Rights Ireland* case, CJEU C-293/12, 08 April 2014.

Public information and the "right to be forgotten"

Clause 12 of the Draft Bill gives data subjects the right to correct or delete personal data that is "inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully".

Although the Draft Bill does not expressly provide for a "right to be forgotten", we note that such a right has been inferred from the "right to delete" or "right to erasure", as interpreted by the Court of Justice of the European Union (CJEU) in the *Google Spain* case.[35] In our view, such an interpretation is clearly unsatisfactory. ARTICLE 19 does not support the recognition of a "right to be forgotten", nor do we support the CJEU's interpretation of the "right to delete" or "right to erasure" in the *Google Spain* judgment. Nonetheless, we set out our concerns in relation to the "right to delete" or the "right to erasure", should it be derived from Clause 12 of the Uganda Data Protection Bill:

- Clause 12 (1) (a) of the Bill gives data subjects the power to have personal data deleted on decidedly vague grounds such as "irrelevance", being "excessive" or "out of date". In our view, this wording is overly broad, opening the door to a disproportionate infringement of the right to freedom of expression and access to information if the data were to be deleted or amended.

- The above-mentioned clause is especially problematic in circumstances where it makes no allowance for the possibility that the personal data could pertain to a matter of public interest. This applies in particular to personal information relating to the public activities of public officials or others acting under public authority or spending public money. The fact that the data concerns the data subject does not exclude that they could be of interest to the public at large, nor should it imply an exclusive right of the individual to control that information. Even the mere fact that information was obtained unlawfully does not necessarily exclude the possibility that the information can be a matter of public interest. Instead, a proper balancing should take place, which should include consideration of the following factors:[36]
    - Whether the information in question is of a private nature;
    - Whether the applicant had a reasonable expectation of privacy, including the consideration of issues such as prior conduct, consent to publication or prior existence of the information in the public domain;
    - Whether the information at issue is of public interest;
    - Whether the information at issue pertains to a public figure;
    - Whether the information is part of the public record;
    - Whether the applicant has demonstrated substantial harm;
    - How recent the information is and whether it retains public interest value;

  In any event, it should be possible to refuse a request for deletion or correction if the public interest overrides the interest of the data subject.
- Clause 12 requires data controllers, i.e. potentially private companies, to determine what personal data may be deleted or corrected. Whilst this process makes sense outside the

[35] CJEU, Case C-131/12, Google Spain, 13 May 2014, available at http://bit.ly/1MKoqFS.
[36] See ARTICLE 19, Right to be Forgotten: Remembering Freedom of Expression, 2016, available at http://bit.ly/2aWf3tr.

context of the "right to be forgotten", it is deeply problematic from a due process perspective when applied to search engines and the accessibility of public information about a person. In particular, private companies lack the independence or are otherwise insufficiently well-equipped to deal with "right to be forgotten" requests.[37]
- Finally, should a "right to be forgotten" be derived from the Bill, the Bill fails to provide for minimum procedural requirements, including access to court and a right of notification to publishers of the information at issue.[38]

Recommendation:
- Ensure that any rules on the deletion of public information are balanced with freedom of expression.

Independent oversight body

A significant missing element of the Draft Bill is the lack of a specific independent oversight body to ensure its functioning. The Bill appoints the National Information Technology Authority, Uganda (NITA) as the party overseeing the bill. NITA is an agency of the Government of Uganda and therefore acts under the general supervision of the Minister for Technology, as established under the National Information Technology Uganda Act.[39]

It is extremely unusual for a comprehensive data protection law to lack an independent oversight body. A recent analysis of over 100 laws in countries around the world found that nearly 90 percent of them had created a Data Protection Authority.[40] The Council of Europe describes oversight bodies as "an essential component of the data protection supervisory system in a democratic society". As noted above, the Charter of Fundamental Rights of the European Union explicitly recognizes as an aspect of the right to protection of personal data that compliance should be subject to the control of an independent authority.[41]
The lack of an independent agency raises serious concerns about the likelihood that the law will be implemented consistently and effectively across all sectors.

In addition, decisions of NITA are subject to an appeal to the Minister responsible for information and communications technology. This results in a government official having ultimate oversight and control over compliance with the Data Protection Bill. In order to adequately safeguard individuals' rights against arbitrary interference under the Bill, provision should be made for appeals regarding enforcement of the Bill to be made to an independent and impartial judicial body.

Furthermore, the Draft Bill's oversight provisions are weak. The procedures for enforcement, forums where complaints can be taken, as well as the remedies available are not clearly set out throughout the Bill, making it difficult for both data subjects to enforce their rights and for an oversight body to properly execute its role.

---

[37] For more details, see ARTICLE 19's policy brief on the Right to be Forgotten, *op.cit.*
[38] *Ibid.*
[39] National Information Technology Uganda Act, 2009 (Act No. 4 of 2009).
[40] Graham Greenleaf, Global data privacy laws 2015: DPAs and their organisations, Privacy Laws & Business International Report, May 2015.
[41] Charter of Fundamental Rights of the European Union, Article 8(3).

Recommendation:

- Create an independent oversight body with full powers to oversee the law, as well as the ability to receive and resolve complaints about its implementation by public and privacy bodies. Decisions from this oversight body should be subject to an appeal to an independent and impartial judicial body.

Criminal offences

Among other things, the Draft Bill provides for the offence of the "unlawful obtaining and disclosure of personal data" (Clause 31). In particular, Clause 31 makes it a criminal offence to knowingly or recklessly (a) obtain or disclose personal data or the information held or processed by a data controller; (b) procure the disclosure to another person of the information contained in personal data.

In our view, Clause 31 is inadequately drafted, and could have a disproportionate impact on freedom of expression and press freedom. In the absence of a public interest defence, this criminal offence could have a particularly detrimental impact on whistleblowers, who may intentionally release personal data or information exposing criminality, corruption or malpractice in a corporation, public body, or political party. This provision is also inconsistent with best practice in this area. We note, for instance, that section 55 of the UK Data Protection Act 1998 contains several defences in relation to the offence of 'unlawful obtaining of personal data', including a public interest defence. Section 55 of the UK Data Protection Act 1998 reads as follows:

> **55 Unlawful obtaining etc. of personal data.**
> (1)A person must not knowingly or recklessly, without the consent of the data controller—
> (a)obtain or disclose personal data or the information contained in personal data, or
> (b)procure the disclosure to another person of the information contained in personal data.
> (2)Subsection (1) does not apply to a person who shows—
> (a)that the obtaining, disclosing or procuring—
> (i)was necessary for the purpose of preventing or detecting crime, or
> (ii)was required or authorised by or under any enactment, by any rule of law or by the order of a court,
> (b)that he acted in the reasonable belief that he had in law the right to obtain or disclose the data or information or, as the case may be, to procure the disclosure of the information to the other person,
> (c)that he acted in the reasonable belief that he would have had the consent of the data controller if the data controller had known of the obtaining, disclosing or procuring and the circumstances of it, or
> (d)<u>that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest.</u>
> (3)A person who contravenes subsection (1) is guilty of an offence. (our emphasis)

Finally, we note that the sentences available under Clause 31 appear excessively harsh (up to 10 years imprisonment) and as such could have a chilling effect on freedom of expression.

We note, for instance, that in France the equivalent offences attract only 3 or 5 years imprisonment.[42]

Recommendation:

- Clause 31 should be redrafted to include a public interest defence. We also suggest that the drafters should draw inspiration from section 55 of the UK Data Protection Act, which provides for further defences, including disclosures made with the reasonable belief that they are made pursuant to a right or duty.
- The custodial sentences available under Clause 31 should be reduced.

[42] See *e.g.* Article 226-22 of the Penal Code.

About ARTICLE 19

ARTICLE 19 advocates for the development of progressive standards on freedom of expression and freedom of information at the international and regional levels, and their implementation in domestic legal systems. The Law Programme has produced a number of standard-setting publications which outline international and comparative law and best practice in areas such as defamation law, access to information and broadcast regulation.

On the basis of these publications and ARTICLE 19's overall legal expertise, the organisation publishes a number of legal analyses each year, comments on legislative proposals as well as existing laws that affect the right to freedom of expression. This analytical work, carried out since 1998 as a means of supporting positive law reform efforts worldwide, frequently leads to substantial improvements in proposed or existing domestic legislation. All of our analyses are available at http://www.article19.org/resources.php/legal.

If you would like to discuss this analysis further, or if you have a matter you would like to bring to the attention of the ARTICLE 19 Law Programme, you can contact us by e-mail at legal@article19.org. For more information about the ARTICLE 19's work in Kenya and East Africa, please contact Henry Maina, Director of ARTICLE 19 Kenya and East Africa, at henry@article19.org.