



Cayman Islands Human Rights Commission

promoting, protecting and preserving human rights

Secretary to the Data Protection Working Group
c/o Cabinet Office
Government Administration Building
133 Elgin Avenue
Box 105 Grand Cayman KY1-9000
CAYMAN ISLANDS

2 November, 2012

Via Email: consult@dataprotection.ky

Dear Secretary,

The Human Rights Commission (HRC) takes this opportunity to thank the Data Protection Working Group for providing a copy of and presentation on the Data Protection Bill in order to provide feedback during the public consultation phase.

The HRC recognises that the various branches of Government as well as private corporations hold a vast amount of information about individuals for the benefit of whom safeguards should be in place. It further recognises that the development of a Data Protection Bill is necessary with the growth of technology and globalisation which have direct impact on privacy rights, property rights, freedom of expression, and other rights ingrained in the Bill of Rights, Freedoms and Responsibilities for all persons in our society.

A major concern, however, is the timing of the implementation of a Data Protection Bill given the impending implementation of the Bill of Rights, Freedoms and Responsibilities. The HRC acknowledges that the Cayman Islands Government, and by extension the country, will have a new Human Rights regime to adapt to imminently together with a significant financial cost. Implementing a Data Protection Law at this time will increase the burden for both the Government as well as local businesses. While the HRC supports a modern, sensible, and easy to understand data protection law that preserves personal privacy rights it is our opinion that there are practical reasons for delay in implementation at this time in the knowledge (from your Working Group) that individual data protection agreements may be entered into.

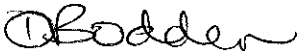
HRC would request the Working Group and legislative drafters to consider a Data Protection Law that is in easily understood 'plain English' rather than extensive 'legalese' as is the case with the current draft Bill. The aim of a Data Protection Law is to protect individuals' rights with regard to data specific to them; however, persons cannot grasp, defend, nor exercise such rights without the requisite understanding of the law itself. The extent to which persons, especially small business owners, will receive assistance in adhering to this new piece of legislation is therefore very concerning.

Although the Data Protection Bill has been modeled on similar legislation in other more experienced jurisdictions, the Commission would like to think there must be a case for building up the intent of a data protection regime from a new template (a "Cayman template") rather than from a Jersey adaptation of a UK adaptation of an EU directive. This would assist legislators in achieving adequacy over the more serious issues highlighted in Appendix A, including areas of national security and Bill of Rights compliance.

The choice of FOI Commissioner seems a strange one. In many respects the principles behind FOI and Data Protection are diametrically opposed. One promotes dissemination of information and the other promotes privacy.

Until the Grand Court develops local case law on these matters, the HRC suggests that the Data Protection Working Group and/or relevant legal advisors should collectively develop a guide of best practices to assist the public service, private organisations, and individuals to understand the rights and responsibilities that ground this legislation.

Kind regards,

A handwritten signature in black ink, appearing to read "R. Coles".

PP Richard Coles

Chairman, Human Rights Commission

Appendix A - HRC's comments on the Data Protection Bill.

Part 1 - Interpretation, Principles, Application and Obligations and office

Definition of "sensitive personal data"

1. The HRC is concerned to note that financial information seems to be omitted from the definition of "sensitive personal data". Just as more non-personal data has become personal data at the international best practice level, so too, more personal data is becoming recognised as sensitive personal data subject to heightened security requirements. In realisation of this trend, for example and as a possible solution, consider India's Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011, which defines sensitive personal information somewhat differently than either the EU or United States to include passwords; personal financial information; physical, physiological and mental-health conditions; sexual-orientation; medical records and history, and biometric information.

Part 2 - Rights and Responsibilities of Data Subjects and Others

Fundamental rights of access to personal data

2. Privacy is not merely instrumental to the achievement of other goals; privacy is a basic human right that applies to all persons in the Cayman Islands in virtue of their status as human beings. It is not possible to overstate just how fundamental privacy is in a civilised legal system such as our own.
3. The obligation to provide personal data, the release of personal data without consent, and the collection and storage of personal data all amount to interferences with an individual's right to respect for his or her privacy. Whether or not such interferences amount to a breach of the Bill of Rights will depend on an assessment of whether the disclosure was "reasonably justifiable in a democratic society" for a legitimate aim (including, although not limited to, the interests of defence, public safety, public morality, public health, for the protection of the rights and freedoms of others), and proportionate. The adequacy of the safeguards in the overall regime is central to this assessment.
4. The right to respect for private life in the Bill of Rights imposes a positive obligation on the Cayman Islands Government to ensure that the laws provide adequate protection against the unjustified disclosure of personal information. The Data Protection Law will, therefore, be a necessary and important part of the detailed implementation of that positive obligation. However, its mere existence does not exhaust the obligation on the Government to provide adequate safeguards. The Data Protection Law must itself be interpreted so as to be compatible with the Bill of Rights, and it may still be necessary for legislation which authorises the disclosure of personal information to contain significantly detailed provisions circumscribing the scope of that power and providing safeguards against its arbitrary use.
5. With regard to security procedures, the HRC anticipates that Government's Data Controllers will have a responsibility under the data protection regulations or internal policy directives to ensure there are appropriate technical and security measures to protect personal data. For example, portable and mobile devices including laptops, cellular phones, and other

portable media used to store and transmit personal data should be encrypted using advanced encryption software which meets the current standard or equivalent.

Fee charged by the Data Controller

6. Section 8 (4) (b) discusses a data controller's ability to prescribe "such fee as the data controller may require", which causes some alarm to the HRC on the grounds that the section essentially appears to afford Data Controllers the power to charge any sum of money for the processing service. In turn, the Commission suggests building a mandate into the legislation insofar as to prohibit a fee, or as is the case under the UK Data Protection Act, prescribing a maximum fee similar to the £10.00 for access to data except for health and education records which is £50 max "depending on the circumstances". As it is currently written in the Data Protection Bill, non-capped fees may disproportionately affect the lower-income persons and possibly leave open a challenge under the Bill of Rights with regard to engaging non-discrimination on the basis of the right to property.

Right to stop processing that causes distress or damage:

7. The HRC cannot overstate the importance of ensuring that public officers who handle personal data are fully aware of the requirements of data protection legislation in combination with their duty under section 19 of the Bill of Rights. In this regard, there are always two dimensions to any kind of privacy issue. One is the framework and the context within it, as well as the organizational culture underpinning the public authority in question. For this reason, the Commission believes that there is no question that if public officers have the idea of the right to privacy in the forefront of their minds there will be a far smaller number of breaches with respect to persons' human rights.
8. Authorities overseeing Data Protection in other jurisdictions have implemented privacy impact assessment tools, which we encourage the Data Protection Working Group to explore in its capacity as the authority for data protection oversight. Privacy impact assessments are intended to ensure that privacy concerns are systematically identified and addressed at an early stage in a project's conception, rather than employed ad hoc as an expensive and inadequate afterthought. The HRC supports initiatives to ensure that data protection and right to privacy issues are dealt with at an early stage in the planning of Government projects, including legislative proposals and data sharing.

Part 3 - Notifications by Data Controllers

Register of notifications

9. In keeping with the advances in technology and the convenience in which it affords the public, the HRC encourages the Data Protection Working Group to make the register available to the public through display on the appropriate website, wherein the register is easily searchable through input of various parameters as a means in which to encourage public inspection.

Part 4 – Exemptions

Exemption modification for sake of health, education or social work

10. In the context of medical records, the European Court of Human Rights has stated:

The protection of personal data, particularly medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the European Convention on Human Rights. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. The domestic law must afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention (MS v Sweden (1997) 28 EHRR 313, para. 41).

The same comments could be made in respect of personal data of any kind held by any organ of the State.

Exemption for sake of journalism, literature or art

11. 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. In this regard, the International Covenant on Civil and Political Rights, Article 17, of the ICCPR protects the right to privacy, and states that:

- i. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
- ii. Everyone has the right to the protection of the law against such interference or attacks.

It is recognised that this exemption ensures certain necessary freedoms of the press and individuals' right to freedom of expression. However, while the right to freedom of expression is fundamental, it is not guaranteed in absolute terms in our Bill of Rights. A consistent interpretation is required with regards to that which is deemed of "public interest" to avoid unwarranted infringements of other persons' rights through subjective interpretation of the phrase.

In effect, regulations assist in the process of balancing competing rights. Implementing the Data Protection Bill without regulations or codes of practice appears to leave open the possibility for data controllers to arbitrarily apply a "public interest test".

Exemption based on national security

12. The Commission ponders whether or not the certificate of exemption for national security reasons should be a matter for the Governor acting together with or on the advice of

National Security Council (NSC) rather than the Governor in his discretion alone (as is currently envisaged). The starting point must be that, so far as possible, the NSC should have input on national security matters, especially where privacy rights are being suspended on national security grounds.

Section 58(4) of the Constitution stipulates that the NSC shall advise the Governor on matters relating to internal security and he (or she) is obliged to act in accordance with that advice unless he considers it contrary to the interests of the UK. Therefore, it is a mandatory provision.

The current provision at section 27(2) of the draft Bill giving the exemption power to the Governor alone may represent a significant inroad into the privacy protection otherwise offered by the draft Bill with real questions as to whether the provision strikes the right balance as envisaged in the Constitution for the management of national security issues. If it does not achieve that balance, there must at least be an argument that the provision falls foul of section 9 of the Bill of Rights and possibly other sections.

The other concern is whether the issuance of the certificate is likely to be subject to judicial review, save for the apparent purpose of identifying the scope of the certificate as set out in section 27(4) - (6) of the draft Bill. Admittedly, this is a complicated area, to which the HRC does not profess to hold the "correct" solution. However, it is at least likely that the Governor, acting on Her Majesty's instructions on questions of national security, as the HRC believes he would, could not be reviewed. Section 31(4) of the Constitution provides that "Notwithstanding the jurisdiction of the courts in respect of functions exercised by the Governor, the question of whether or not the Governor has in any matter complied with any instructions addressed to him or her by or on behalf of her Majesty shall not be inquired into by any court". There is a real question here about the nature and scope of judicial review proceedings which could be brought to challenge an exemption certificate issued on national security grounds if HM's instructions are in issue. In fairness to the Caymanian public's interests, although there may be a way around this, the HRC contends that the question is worthy of further examination.

Additionally, the Commission notes the wording of the Data Protection Bill itself, which says the certificate shall be "sufficient evidence" of the national security exemption. This brings to mind similar concerns expressed by the Commission in the past in relation to telecommunication message interception; not the least, issues of oversight. As a result, the HRC is keen to understand exactly how it is proposed that the process for issuing those certificates of exemption would work and what safeguards are proposed.

Exemption for the sake of history, research or statistics

13. While, overall, section 32 was difficult to grasp, the main gist appears to be that data collected for the purposes of statistical, historical or scientific research would be exempt from Section 8, under certain circumstances. This is of concern because section 8 is quite broad, yet fundamental to allowing data subjects to access data collected about them. Section 32 (4) explicitly states that personal data that identifies an individual can be kept only as long as it is needed to be processed, and during this period a data subject cannot request access to this data under Section 8.

- i. Firstly, this statement appears to conflict directly with Section 32(6) which states that all statistical, historical and scientific research is exempt from the 5th data principle, (which states that personal data can only be kept for as long as is necessary for the purpose which it were collected).
- ii. Secondly, it is concerning that a data subject would not be allowed access to their personal data during a period when they can be identified. This is particularly concerning because there seems to be no good reason why a data subject should not have access to personal data gathered for statistical, historical or scientific research as the accessing of such data has no apparent impact on the integrity of research design or methodology. On the contrary, the ability for a data subject to access personal data gathered for research implies transparency and validity, which bolster research integrity. While data subjects may have access to such personal data when it is gathered by a government agency via an FOI request, this Section 32(4) exemption could allow the abuse of personal data gathered by private groups/individuals which could go on to be published as reliable statistical, historical or scientific research.

Part 6 – Enforcement

Unlawful obtaining etc. of personal data / Power of the Commissioner to impose monetary penalty

14. While recognising the legitimate importance of information to the continuity of public sector and private sector business, the HRC believes that individual privacy is a key human right and that the subsequent data protection law must provide protection for individual privacy as a necessary part of ensuring a fair balance of power between individuals and the Government or private organisations. In this regard, the Commission encourages and supports strong sanctions, including proportionate monetary fines, as deterrents to prevent the fundamental rights of persons living in the Cayman Islands from being unjustifiably, unnecessarily, or disproportionately infringed.

Schedule 2 – Conditions for Processing of Any Personal data

Conditions for Processing

15. Rightfully, organisations and Government agencies that process personal data need to be able to satisfy certain conditions as set out in the Bill. However, the HRC is mindful that this will not, on its own, guarantee that the processing is fair and lawful. For this reason, the Commission suggests that the elements of ‘fairness’ and ‘lawfulness’ will be examined separately to one another and in conjunction with the obligations for public authorities under the Bill of Rights. Moreover, the HRC supports a framework wherein the conditions for processing are more exacting with respect to sensitive personal data.

