

Data Protection Working Group

Final Report on the Draft Data Protection Bill

Background

In August 2009, upon a request from the Hon. Attorney General, the Governor-in-Cabinet established a Data Protection Working Group (“the Working Group”) tasked with the drafting of a Data Protection Bill (“the draft Bill”). The Working Group was chaired by Mr. David Archbold, then Managing Director of the Information and Communication Technology Authority, and counted among its members various representatives from the private and public sectors.¹ Mr. Bilika Simamba acted as legislative draftsman for the Working Group.

Different international data privacy models were initially considered, and in June 2010 the Working Group proposed to draft a Bill which would meet the “Adequacy” requirement of the European Data protection Directive² (“the Directive”), and which was specifically modeled on the Data Protection (Jersey) Law, 2005 of the Bailiwick of Jersey.³ This proposal was accepted by the Cabinet.

The EU’s Data Protection Directive is generally regarded as the most rigorous data privacy standard in the world. Gaining “Adequacy” status would allow personal data to move between the EU Member States (and Members of the European Economic Area) and the Cayman Islands without further safeguards. It would also pair the data privacy regime in the Cayman Islands with the expectations of its international business partners, including non-European businesses, and enhance compliance with the European Convention on Human Rights. The Working Group recognized the Jersey Law as an example of national legislation that meets the European Commission’s “Adequacy” standard, and that balances the needs of the financial industry with the broader expectations of protection of the fundamental right to private and family life.

Although the subject matter of any Data Protection law is by nature complex and multifaceted, the Working Group at first made swift progress. However, a complication arose when the European Commission announced that it would urgently review and modernize the Directive. A Draft EU Data Protection Regulation was published in January 2012, and the discussions between Member States remain ongoing to this day.

The Working Group also became aware that various, credible criticisms had been raised against the UK’s Data Protection Act 1998 which was a close model for the 2005 Jersey Law. The Working Group decided

¹ Information about membership of the Working Group and the IT-Subcommittee can be found on www.dataprotection.ky/index.php/

² *Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the process of personal data and on the free movement of such data* O.J. No. L 281/31.

³ *Data Protection (Jersey) Law 2005 L.2/2005.*

to proceed with the drafting of a bill by taking these developments and criticisms into account, while at the same time simplifying and strengthening certain provisions relevant to the Cayman Islands.

During the drafting process the Working Group sought input from selected industry groups in the first part of 2012, and issued a broad invitation for comments in a well-publicized public consultation later that same year. In the course of this consultation members of the Group delivered presentations to various interested stakeholder organizations, and a number of lengthy comments and views were received in return, in one case up to several months later.

The core Working Group⁴ considered each of the comments and views received in detail, making amendments to the consulted draft. This was followed by a careful final reading and review of outstanding questions raised within the Group itself, which resulted in the final draft Bill attached to this report.

The Need for Data Protection

As the Information Society becomes a reality in the Cayman Islands, more and more personal information is collected, processed and shared by public authorities, private entities and individuals, often without the consent or even knowledge of the individuals concerned. The associated risks have caused concern worldwide, and have led to the enactment of data protection legislation in most developed countries.

Data protection legislation seeks to protect an individual's rights with respect to the collection, use and disclosure of his or her personal data, while balancing these rights against the need for legitimate processing of such data by public authorities, businesses and organizations.

With the coming into effect of the Cayman Islands Bill of Rights, Freedoms and Responsibilities in 2012, in particular section 9 relating to the protection of family and private life, the need for domestic legislation to provide specific protection in the area of data privacy has become urgent. Personal data are equally at risk in the public and private sectors, and it is important to set a clear standard for their use and misuse in the Cayman Islands. The current gap in applicable legal provisions relating to the use of CCTV, and the need for privacy protection in the context of some of the international agreements which the Cayman Islands is subject to, suggest that a Data Protection Law is long overdue.

Given the recent advancements in technology and ease of data transfers across national boundaries, international businesses and their clients expect jurisdictions to have in place comprehensive data protection regimes that satisfy their compliance requirements, and facilitate the legitimate transfer of personal information throughout their organizations.

The draft Bill has been developed in line with international best practices but a conscious effort has also been made to ensure that it reflects the specific needs of the Cayman Islands. The core Working Group believes that the draft Bill meets these requirements and - if enacted - will create a robust and

⁴ The number of active members of the group has gradually diminished to a core comprising Messrs. David Archbold, Peter Broadhurst, Bilika Simamba, Russell Richardson and Jan Liebaers.

proportionate data protection regime that will enhance Cayman's reputation and competitiveness in the global marketplace.

The Data Protection Bill

The draft Bill proposes a framework of rights and duties designed to safeguard individuals' personal data, balanced against the need of public authorities, businesses and organizations to collect and use personal data for legitimate purposes.

The draft Bill:

- defines "personal data" as data relating to an individual, including an expression of an opinion about, or an indication of intentions in respect of, the individual;
- defines "processing" broadly, so as to include the collection, organization, storage, alteration, use, disclosure or destruction of personal data;
- applies to all types of personal data in every medium;
- applies to both public and private sectors;
- places limits on how personal data may be used by, or shared with, third parties;
- provides special protections for particularly sensitive types of personal data;
- anticipates that the Information Commissioner under the Freedom of Information Law, 2007, will also be the Data Protection Commissioner, and will be tasked with ensuring that the rights and protections in the draft Bill are upheld; and,
- is modeled after, and compliant with the requirements of the Directive.

❖ *Data protection principles*

The draft Bill is centred around eight straightforward data protection principles, which form the basis of many of its provisions. The data protection principles are:

1. Personal data must be used fairly and only when specific conditions are met, for instance where consent has been given, where there is a legal obligation, or where it is necessary for performance of a contract.
2. Personal data must be obtained for one or more specified, lawful purposes, or compatible purposes.
3. Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are collected or used.
4. Personal data must be accurate and up to date.
5. Personal data must not to be kept for longer than necessary.
6. Personal data must be used in accordance with the rights of individuals as specified in the remainder of the draft Bill.
7. Personal data must be protected by appropriate technical and organizational measures against unauthorized or unlawful use, and against loss, destruction or damage.

8. Personal data must not to be transferred abroad unless an adequate level of protection can be guaranteed.

❖ **Rights**

The proposed legislation grants individuals (“data subjects”) specific rights in relation to their own personal data. These include, subject to specified limitations:

- the right to access your own personal data and certain information about its use;
- the right to require that processing of your personal data cease;
- the right to require that processing of your personal data for the purpose of direct marketing cease;
- the right to require that a decision which significantly affects you, and which is made solely by automatic means, is reconsidered on another basis;
- the right to seek compensation for damages caused by contravention of the Data Protection legislation;
- the right to seek rectification, blocking, erasure or destruction of inaccurate personal data; and,
- the right to complain to the Information Commissioner where it appears that a violation has occurred.

❖ **Duties**

The proposed legislation also imposes certain specific obligations on the persons who control the use of personal data (“data controllers”), including:

- the duty to apply the data protection principles;
- the duty to register certain details, and changes in details, with the Information Commissioner, without which the processing is not allowed;
- the duty to respond in a timely fashion to requests from data subjects in relation to their personal data; and,
- the duty to notify data subjects and the Information Commissioner of any personal data breaches.

❖ **Exemptions**

The draft Bill recognizes a number of exemptions to certain obligations in order to ensure that personal data can be used in appropriate circumstances.

These include national security, law enforcement, certain public functions, health care, education, social work, journalism, literature, art, research, history, statistics, information available under an enactment, legal proceedings, personal family or household affairs, honours, corporate finance, negotiations, legal privilege. The Cabinet may also develop further regulations relating to exemptions.

❖ **Compliance and enforcement**

The draft Bill requires effective oversight to ensure compliance and processing of complaints. It anticipates that the Information Commissioner, currently tasked with oversight of the Freedom of Information Law, 2007, will assume a similar role for Data Protection, and will be given the powers, responsibilities and resources necessary to ensure the successful functioning of the legislation once passed. This combined role is similar to the vast majority of international jurisdictions.

The Information Commissioner is expected to have **powers**, including:

- to hear, investigate and rule on complaints;
- to monitor, investigate and report on the compliance of data controllers under this Law;
- to intervene and deliver opinions and orders related to processing operations;
- to order the rectification, blocking, erasure or destruction of data;
- to impose a temporary or permanent ban on processing;
- to make recommendations for reform both of a general nature and directed at specific data controllers;
- to maintain a public register of data controllers and their processing operations under this Law;
- to engage in proceedings where the provisions of this Law have been violated, or refer these violations to the appropriate authorities;
- to cooperate with international data protection supervisory authorities;
- to publicize and promote the requirements of this Law and the rights of data subjects under it; and,
- to do anything which appears to him to be incidental or conducive to the carrying out of his functions under this Law.

The draft Bill also identifies a number of **offences and penalties**, including for:

- processing personal data without registration;
- failing to notify the Commissioner of changes to the registration;
- failing to make certain particulars available to a data subject in response to a request;
- failing to notify the data subject and the Commissioner of a personal data breach;
- withholding, altering, suppressing or destroying information requested by the Commissioner;
- knowingly or recklessly disclosing information;
- obstructing a warrant, or making a false statement;
- unlawfully obtaining, disclosing, selling or procuring personal data;
- failing to comply with an enforcement or monetary enforcement order; and,
- offences otherwise specified in Regulations.

Next Steps

After diligent analysis, productive cooperation and public consultation, the core Working Group is pleased to submit this report and the attached draft Data Protection Bill for consideration by the Hon. Attorney General.

❖ *Implementation*

The core Working Group recommends that after the draft Data Protection Bill is passed into Law by the Legislative Assembly it should be implemented over at least a twelve month period, with phased registration of data controllers occurring first. Training and guidance will be provided and at the end of the implementation period the full provisions of the Law should be brought into effect by Order of the Governor.

The number and length of registration and implementation phases will be dependent upon the resources available to the supervisory authority, the success of the registration procedures and the response from data controllers. The draft Bill therefore grants the Information Commissioner discretion to vary the implementation phases and their timing.

It is recommended that at an early phase in the implementation process the views of the European Commission should be sought as to whether the proposed Bill meets all the requirements for "Adequacy" status, as anticipated by the drafters. The core Working Group remains at the disposal of the Hon. Attorney General to assist this process further, if required.

20 February 2014