SUBMISSIONS ON DATA PROTECTION BILL

In the matter of the **Data Protection Bill** and comments on behalf of the Jamaica Computer Society and the Jamaica Information Technology and Services Alliance.

We, the Jamaica Computer Society ("JCS") and the Jamaica Information Technology and Services Alliance ("JITSA"), make the following submissions with reference to your request for submissions on the Data Protection Bill ("the Bill") which has been tabled before the lower house of the parliament of Jamaica.

1. **Methodology**
2. These submissions are made from the perspective of the Jamaican electronic/computer user (called a "data subject" under the Bill), as well as from the perspective of JCS/JITSA business stakeholder interests. These stakeholder interests include technology firms, training providers and IT officers/contractors for major institutions. The common objective of the group is to provide feedback which is in the interest of the public given the increasing global concerns regarding the protection of privacy in data rich environments.

3. **Context of Submissions**

4. The Bill largely incorporates the current United Kingdom Data Protection Act which is modelled on the European Data Protection Directive. That level of data protection could be termed Data Protection 1.0. However, the EU and the UK, (even post

Brexit), will be adopting the European Union General Data Protection Regulations (GDPR) (which could be called Data Protection 2.0). The Jamaican Bill is still at Data Protection 1.0 standards.

5. In summary, the Bill creates an obligation on non-domestic data processing (inclusive of manual file keeping) to maintain strict privacy and accuracy standards and to prevent breaches in relation to that data. To comply with this requirement, data controllers, which direct how data is collected and processed, must register **and** appoint data protection officers. These data protection officers are compliance officers (analogous to anti money laundering compliance officers which banks are now required to have). The data controllers must be registered and must submit annual reports and notices of assessment. The enforcement mechanisms for non-compliance are fairly strict with companies being liable for penalties up to 10% of their gross annual income in the event of breaches of the Bill.

6. Submissions - At a Glance

7. Generally, the Bill, given the Data Protection 1.0 standard, does not take into effect modern modalities such as the use of the internet and applications by minors and the prospects of behavioural/cookie based advertising. Nevertheless, it is a start as Jamaica grapples with the effect of being in an information society.

8. The major areas of concern are the definition of consent (especially for minors), breach notification in the event of a hack or other illicit disclosure, the significant reporting/regulatory obligations and the enforcement of measures to be levied by the regulator, the Information Commissioner (referred to as “the regulator” throughout these submissions). The concerns highlight the need for a sectoral approach by the government.

9. It is our submission that a greater self-regulatory model be used to lessen the burden on the business community. However, we suggest more rigorous approach to data protection by public authorities through (1) less exemptions and, (2) more

specificity in respect of the handling of data by public authorities. We recommend the approach by Mexico in this regard[1].

10. Further, we strongly recommend an industry code of conduct which provides guidelines for controllers of different types of data beyond the types noted in the Bill. These codes can be referred to as industry standard in the text of the Bill. This recommendation is made given that the Bill will be onerous in its application on Small and Medium sized enterprises.

[1] Mexico's General Law on the Protection of Personal Data Held by Regulated Subjects.

Section of Bill	Comments and Recommendations
s.2 (Definition of consent)	Worldwide, the matter of consent is one of the most crucial areas of data protection law. It is very unfortunate that, as a matter of drafting, substantive provisions on consent are placed in the definitions section. We recommend that consent be place in a separate and distinct section of the Bill consistent with the approach under, for instance, the EU General Data Protection Regulations ("EU GDPR"). This will allow for ease of future amendment. In respect of consent, we make the additional recommendations: 1. The definition should also include the "data subject" him or herself. This appears to be a drafting error. 2. There is no elaboration on the form which "consent" should take but in any event controllers will have to ensure that persons consenting are not misled or deceived in giving consent. 3. As a matter of drafting, there appears to be a conflation of the standard of "lawful processing" with the "sufficiency of consent". These are distinct principles. 4. The manner of consent may be less than required under significant international legislation such as the proposed European Union General Data Protection Regulations. The lack of a sufficient standard could impact on the certification of Jamaican data transfers in the long run. 5. The EU has recognized that data is often submitted by children for information society purposes (online) under the

age of 18, accordingly, the EU allows member states to lower that “age of consent” for information society activities provided that it not be lowered below age 13. This is consistent with the view that children are allowed to use online applications, such as Facebook, from age 13 upwards. To create a requirement for consent at the age of 18 would, at this technological stage, immediately create unnecessary non-compliance.

6. The data protection jurisprudence has placed emphasis on how one may withdraw consent. This withdrawal may be the means of terminating a service. In fact, the data subject should be told that he/she has the ability to withdraw consent from mailing lists, direct marketing and other services which use personal data. There is a general provision allowing an “opt out” under the Electronic Transactions Act but specific requirements for withdrawal should be set out in the data protection law.

7. Generally, there needs to be a recognition of the concept of “informed consent” and a recognition that applications and other products may use modes of consent outside the general terms and conditions “I accept” methodology such as “privacy by design”. These creative forms of consent (more opt in rather than opt out should be considered as be acceptable under Jamaican laws).

8. Please see Article 7 of the EU GDPR as an example of a much more robust provision on the matter of consent. We urge the drafters to consider this more full-fledged approach.

s. 3 (1)(b)

It appears that the intent of the Bill is to exclude data processors and controllers in overseas jurisdictions and to concentrate on local processors/controllers. The committee should, however, be aware that the wording of the Bill may still cover overseas controllers given the interpretation that has been given to the word "equipment" particularly in the EU.

In the EU, "equipment" has been taken to include cookies[2]. The committee should note that cookies have been deemed to be equipment being used "otherwise than for the purpose of transit". Cookies serve an important role in gathering data for third party behavioural advertising purposes. Such use is more than transitory.

In that event, overseas data processes which use cookies on websites may be required to comply with the regulatory requirements under the Bill.

We recommend that the Committee make its legislative intention clear in this regard. While we understand the need to protect the right of privacy of individuals, this right has to be weighed against need to regulate within current capacity with thought given to regulatory creep in the future.

[2] A cookie is a small file, typically of letters and numbers, downloaded on to a device when the user accesses certain websites. Cookies are then sent back to originating website on each subsequent visit. Cookies are useful because they allow a website to recognise a user's device.

s. 5(a) (i)

Please see comment above regarding consent to be given by minors in the context of the information society. We recommend that for information society matters, that consent be provided by minors age 13 and above.

s. 5(a)(iii)

The provision is curious as it will be difficult to determine the individuals who fit the definition of “common law spouse” or an individual acting for another with a physical or mental infirmity without an order from a court of law. We recommend more thought given to the section so that some sort of legal authorization or appointment is recognized such as an attorney under a Power of Attorney, a “next friend” ordered by a court of law or a person appointed under the auspices of the Mental Health Act.

This is important as the lack of precise authority may allow unauthorized persons to have a right of access to data (under s.6). This defeats the very purpose of the Bill in securing privacy rights particularly for those most vulnerable.

s. 6 *(Right of Access to Personal Data)*

In other jurisdictions, similar provisions have been used as fishing expeditions (and for phishing purposes) to uncover the reasons for decisions made particularly by public authorities. That is not the remit of this statute. Accordingly, the section should be better drafted to restrict improper usage of the right of access.

6(2)(d)

In respect of s. 6(2)(d) we recommend the inclusion of the words "significantly meaningful information" so that the section following (ii) will read:

> "…to be informed by the data controller, upon payment of the prescribed fee, **of significantly meaningful information** about the logic involved in that decision-making".

This amendment would align the provision with that under the EU regime and is necessary given the growth of artificial intelligence in decision making.

s. 9

(Personal data held other than in a relevant filing system by a public authority)

The main concern with the provision is that public authorities, which tend to hold the bulk of personal data, will be exempt from some of the requirements post an application for access by a data subject under the Bill.

The implementation of the National Identification Number under the NIRA Act and related systems will place very large datasets in the hands of public authorities almost in disregard to the data minimization principle. It is crucial that there be strict measures for the handling of data by public authorities.

We also suggest a more refined definition of public authorities to exclude some executive agencies etc. There are no comparable laws which could ensure that these bodies protect the privacy of individuals or ensure accuracy. Such an obligation does not exist under the Access to Information Act.

s. 12 (7) (b)

(Rights in relation to automated decision-making)

We are mindful that other exemptions to the automated data processing/decision-making may be developed. This is a heavily pro-consumer/data-subject provision and we applaud this approach. However, we suspect that the provision will have an impact on data mining and the use of large datasets at a time when such industries are becoming lucrative internationally.

However, it would be useful for the Committee to note the additional contemplated areas of exemption.

The exemptions to automated processing include circumstances in which the data subject is entering into or performing a contract or otherwise authorized or required by or under another law.

s. 12 (8)	The wording of section 12(8)(b)(i) appears to be ambiguous and can lend itself to several meanings. It could mean that the data subject has consent to the decision being based on solely automated processing **or** it could mean that the data processor/controller, in its sole discretion, is of the view that the effect of processing the data in that manner grants the request of the data subject. For clarity, we suggest the deletion of 12(8)(b)(i) and the insertion of the words "***based on the data subject's explicit consent***". At 12(8)(b)(ii), we suggest the the inclusion of the following words at the end of the sentence ***"…after reasonable prior notice has been given to the data subject***".
s.13 *(Rectification of inaccuracies etc.)*	It will be very important for data processors to understand the ambit of this provision. Curiously, given the limited jurisdiction of the Bill, it may not apply to Google or similar international search engines (which do not fall within the definition of "controller"), however, it ***may*** apply to local search engines and archives such as www.jamaicagleaner.com. This difference in application is perhaps something to note so that a true balancing of the impact of the Bill can be undertaken before the Bill is passed. The Bill is silent on how the controller will make the determination of when the rectification is required. The objective of the drafters in doing so is quite unclear (unless it was presumed that the controller will have reference to the standards). However, better drafting of this section could protect both the interest of the controller and the data subject. For instance, consideration could be given to:

1. Whether the data subject withdrew consent;
2. Any overriding legitimate grounds (e.g. freedom of expression vs. defamatory material)
3. Whether the consent of a minor was not real/informed.
4. Cost and technology available to procure erasure.

s. 20

(Appointment of Data Protection Officers)

The appointment of data protection officers should be limited to entities which the regulator certifies as being in control of sensitive or other data requiring internal control. For instance, we expect data brokers, financial institutions, health institutions and other regulated bodies to have a data compliance officer but certainly not small schools or retail shops which may keep records of customers. Compliance may present an additional burden since the provision requires that the person be “appropriately qualified”.

However, we recommend that the regulator under the Act be empowered to carry out a continuous assessment process to make a determination of whether entities reach a particular threshold requiring a data protection officer/compliance officer. In the alternative, the law may use a small/large company designation as is used under the Companies Act/International Financial Reporting Standards in determining when a company reaches a particular size. We suggest that when a company increases in size, there is a statutory trigger leading to the enforcement of the data protection officer requirement.

s. 15-18

(Registration of Data Processors)

This provision introduces over regulation and will be onerous given the extensive application of the Act. Most businesses will have to register as a data controller (though the Minister has the power to exempt certain bodies, the Ministerial exemptions are not yet known).

In any event, jurisdictions which have impact assessment provisions (as Jamaica will have) and compliance officers do not ordinarily require registration. Please see table, in footnotes below, of Latin American countries which have active data privacy laws[3]. Argentina and Columbia are the only jurisdictions which require registration **and** the appointment of a data protection officer. In a small developing country, such as Jamaica, the registration requirement is onerous. Given limitations in size, it is fair to rely on self-regulation through the implementation of data protection officers where the data processor/controller is processing certain types of data or has reached a certain size. (We will discuss this more extensively below).

The information age, increase in smart phone usage and social media have all broadened the ability of individuals to be data

3

Country	Registration Requirement	DPO Required
Argentina	Yes	Yes
Aruba	No	No
The Bahamas	No	No
Chile	No	No
Columbia	Yes	Yes
Costa Rica	Yes	No
Curacao	No	No
Dominican Republic	No	No
Mexico	No	Yes
Nicaragua	Yes	No
Peru	Yes	No
Trinidad and Tobago*	No	No
Uruguay	Yes	No

processors and blurred the lines between data controllers and data processors. Further, the implementation of a registration regime would not be pro-business and be anti-investor. We recommend the deletion of sections 15-17.

S. 23 & 24

(Conditions for processing personal data in accordance with the first standard)

There appears to be a significant loophole available to public authorities in the processing of data for the administration of justice and generally by the Government of Jamaica under s. 23(1)(e). The effect of this loophole/exemption is that there is an exemption for the first standard of the "processing fairly and lawfully" and consequentially a *carte blanche* exemption from the law since its very premise is to ensure fair and lawful processing.

Generally, we feel that more precise references should be made to data held by public authorities. As read now, the law does not provide any real assurance regarding the safeguarding of information when used by public authorities. This reassurance can come in the form of published regulations on encryption, data sharing codes between public authorities or regulatory codes for storage of data by government bodies (for example the Mexican Data Protection Law has requirements on the types of cloud storage facilities which may be used by public authorities). The public needs greater assurance as to the data protection standard implementation by public authorities as opposed to the blanket exemptions (and

room for Ministerial exemptions) provided under the Act.

s. 28

(Fifth Standard on Data Retention)

The specific retention periods should be given to stakeholders before the passing of the Bill. The Ministry should either insert the timeframes as a Schedule to the Bill or ensure that the Regulations are presented for review prior to the passing of the Bill. Educational institutions, for instance, will need to be guided in respect of the student's data which must be retained.

Retention periods will involve significant data dumps by companies which companies will be guided by the Statute of Limitations on the bringing of legal claims.

s. 30

(Seventh Standard – Data Breaches)

The language used in the provisions dealing with breach notification suggests that the government is aware that different entities will have varying capabilities to provide technology up to a certain standard but the government is also concerned that particular types of data will require additional security provisions. For instance, controllers holding confidential health records or banking information must ensure their security standards are at the highest level.

This generalization is good from an implementation standpoint but not from the standpoint of enforcement of measures when a breach does occur.

The EU has a more streamlined approach which takes into consideration any code of conduct developed by stakeholders in the

industry. For instance, stakeholders can create breach notification codes of conduct relative to the type of data involved and the EU regulator will take such codes into consideration when applying a penalty, if any. JCS and JITSA are willing to assist in the development of these industry codes/benchmarks.

We note that there is no need to inform the data subject in the event a breach occurs. However, there is a growing trend for data subject /customer notification worldwide and the proposed EU regulations now make provision for such. In fact, in the EU, the **regulator** may make the data subject aware of the breach in high risk contexts.

We think breach notification **for certain types of data** would be pro-user/consumer and is consistent with what an individual would require from any internationally reputable organization. Notice of certain types of hacks in respect of sensitive data should be given to the data subject.

s. 43	Consistent with EU approach, it would have been good to clarify that charitable purposes are not excluded. Processing by charities does not constitute domestic use and so they should be captured by the provisions of the Bill.
s. 49 (*Assessment Notices*)	We are of the view that this is a bit of overregulation. The regulator should only be empowered to enter the premises of the controller after the filing of a complaint from a data subject and after the data controller has responded to the complaint.

ss 59-60	There should be provision for specific industries to apply for a code or for guidance on how the code will operate before undertaking activities.
(Data Sharing Codes)	The section states that the regulator **must** seek the input of the relevant trade association, the applicable data subjects or anybody appearing to represent the data subjects.
s.64	We find this provision is too subjective. We suggest a re-wording so that what is considered a “serious contravention” is more precise.
(Power of Commissioner to Impose Fixed Penalty)	The emphasis on the need for knowledge before it can be determined that there is a contravention is appreciated. However, there is an introduction of implied knowledge. In a constantly changing industry, such implied knowledge can be imprecise. We again recommend a statutory recognition of an industry Code of Conduct which would provide a benchmark for the type of knowledge a small, medium or large scale controller would need to possess.

s. 70 (Liability of body corporates/directors)	The imposition of a fine not exceeding ten percent of the gross income of the body corporate is very high. We recommend that a precise sum be noted, as is the case under other laws. Varying fines could be stated taking into consideration the type of breach of whether the breach involves a particular type of data (sensitive, financial etc.).
s. 74 (3) (Application to the Crown)	We note that while the Act binds the Crown, it (and specifically public authorities) will not be liable for prosecution. This seems grossly unfair given that there are some public bodies which as executive agencies compete in ways similar to private bodies. We recommend that civil penalties be recoverable by the data subject for any breach occasioned by the public authority and that this proviso be explicitly stated to prevent ambiguity.

s.77 (Transitional)	A year is too short to implement the Bill into law even if our recommended reduced regulation is taken on accepted. We recommend a three (3) year period for implementation of the law.
Third Schedule	We recommend that orders under the Bill be sought from a Supreme Court judge (and not a parish judge) as is the case for similar warrant requests under the Interception of Communications Act.

Prepared, under instructions, by Grace Lindo, Attorney:4105, Nunes, Scholefield, DeLeon & Co. Attorneys-at-law of 6A Holborn Road, Kingston 10.