CLOUD COMPUTING IN GEORGIA

REGULATORY FRAMEWORK

FOREWORD

We are pleased to introduce to you this Cloud Computing in Georgia – Regulatory Framework.

This publication addresses the most important legal issues relevant for legal practitioners and business people dealing with cloud computing products and services in Georgia.

This survey was prepared and coordinated by the specialist cloud computing and data protection team at **PIERSTONE, a technology law firm in Prague, Czech Republic** in collaboration with **Mikheil Gogeshvili** of the law office **Mgaloblishvili Kipiani Dzidziguri in Tbilisi, Georgia.**

The article Cloud Computing – Brief Technical Overview for Legal Professionals was written by Zdeněk Jiříček, National Technology Officer at Microsoft s.r.o., Czech Republic.

We would like to thank Dr. Jochen Engelhardt, CEE Legal Director, Legal and Corporate Affairs at Microsoft who proposed the idea for this publication and supported its realization.

Editors: Lenka Suchánková, Partner (lenka.suchankova@pierstone.com), and Jana Pattynová, Partner (jana.pattynova@pierstone.com), PIERSTONE.

Disclaimer: This publication is for informational purposes only. The information contained in this publication is intended only as general guidance on selected data protection aspects of cloud computing. It does not deal with every relevant topic or may not address every aspect of the topics covered. This publication may be updated from time to time. The application and impact of laws may vary widely based on the specific facts involved. The information does not constitute professional legal advice and should not be used as a substitute for consultation with a legal adviser. Before making any decision or taking any action requiring legal assessment, you are advised to consult a legal professional in the relevant jurisdiction.

COUNTRY SPECIFIC REQUIREMENTS BASED ON LOCAL PRIVACY LAW:

GEORGIA

COUNSEL DETAILS:

Country: Georgia

Attorney: Mikheil Gogeshvili

Law Firm: Mgaloblishvili Kipiani Dzidziguri (MKD) Law Office
71 Vazha Pshavela Ave., Office 24, 0186 Tbilisi,
0186 Tbilisi
Georgia

Website: www.mkd.ge

E-mail: mgogeshvili@mkd.ge

The following briefly outlines the non-sector-specific data protection requirements that organizations or institutions need to bear in mind in relation to their use of cloud computing.

INTRODUCTION

1

In general, what is the statutory basis for the protection of personal data (hereinafter referred to as the "Privacy Act")?

The Law of Georgia on Personal Data Protection (in Georgian: კანონი პერსონალურ მონაცემთა დაცვის შესახებ), dated 28 December 2011 (the "Privacy Act").

Unofficial English translation of the Privacy Act can be found at: http://personaldata.ge/res/docs/Kanoni/PDP%20Law.pdf

2

Which authority oversees the data protection law (hereinafter referred to as the "data protection authority" or the "DPA")? Summarize its powers.

საქართველოს პერსონაღურ მონაცემთა დაცვის ინსპექტორი Office of the Personal Data Protection Inspector (in Georgian: საქართველოს პერსონაღურ მონაცემთა დაცვის ინსპექტორი) (hereinafter referred to only as the "DPA").

Address: 15 Apakidze str., Tbilisi, Georgia

Web: http://personaldata.ge/en/home

The DPA represents an independent administrative entity not subordinated to any governmental body but accountable to both the Parliament and the Government of Georgia. The DPA's authority encompasses the following broad competences:

(i) consulting public bodies, natural and legal persons on issues related to personal data protection;

(ii) overseeing compliance with personal data protection legislation by various stakeholders;

(iii) reviewing complaints and hearing appeals on alleged violations of personal data protection legislation;

(iv) conducting investigations (including on-site visits);

(v) application of administrative sanctions in case of violations of data protection legislation which constitute administrative offences under the Privacy Act;

(vi) granting approvals for trans-border flow of personal data;

(vii) maintaining the registry of filing system catalogues (holding records of the filing systems managed by various data controllers).

3

Identify the requirements for the applicability of local data protection laws.

The Privacy Act applies to the processing of data on the Georgian territory (including at the Georgian diplomatic missions abroad) by automated or semi-automated means as well as to the processing of the data by non-automated means which form, or are intended to form, part of a filing system.

The Privacy Act also applies to the activities of a data controller who is not registered in the territory of Georgia but exploits technical means located in Georgia for data processing purposes, except when these technical means are used solely for the transit of data.

IMPORTANT DEFINITIONS

4

What is the definition of "personal data"? Is encrypted data regarded as personal data in case the cloud provider does not possess access to the encryption key?

Personal data is defined as any information relating to an identified or identifiable natural person. A person will be regarded identifiable when he/she may be identified directly or indirectly, in particular by an identification number or by any physical, physiological, psychological, economic, cultural or social features/factors specific to this person.

There is no conclusive guidance on the status of encrypted data but the Privacy Act does define "de-identification" as data modification that makes it impossible to link specific data to the relevant data subject. Hence, encrypted data may be regarded as "de-identified" and therefore not constituting personal data.

5

Does the Privacy Act differentiate between different categories of data to which it affords a level of protection that goes beyond the normal requirements for personal data outlined in this questionnaire; e.g. sensitive data, such as health information? Please list the most relevant differences.

The Privacy Act recognizes so called sensitive data which represents data connected to a person's racial or ethnic origin, political views, religious or philosophical beliefs, membership of professional organizations, state of health etc. Biometric data also falls in the definition of sensitive data.

Sensitive data must be processed on the basis of legitimate grounds prescribed by the Privacy Act and a data subject's written consent; the level of protection afforded to sensitive data is similar to the protection granted to other personal data.

CUSTOMER / CLOUD PROVIDER / SUB-PROCESSOR – ROLES AND RESPONSIBILITIES

6

In general, who is the data controller and who is the data processor in a cloud computing service? Describe their key obligations.

Data controller is a public agency, natural or legal person who individually or jointly with others determines purposes and means of personal data processing and who, directly or through a data processor, processes personal data. Data processor is any natural or legal person who processes personal data for or on behalf of the data controller.

In the context of cloud services, the customer purchasing the services is usually deemed the data controller while the cloud service provider is deemed a (mere) data processor.

Primary obligations of the data controller include:

(i) provide data subject with information regarding identity of the data processor, nature of data being processed, purpose of data processing;

(ii) not to engage a data processor who is likely to misuse personal data;

(iii) monitor the processing of personal data by the data processor;

(iv) interact with the DPA when data processing activities require notifications to or approvals by the DPA.

Primary obligations of the data processor include:

(i) process data within the scope and in conformity with the purpose determined, e.g. in the agreement concluded with the data controller;

(ii) implement relevant organizational and technical measures to protect the personal data that is being processed;

(iii) not to subcontract data processing activities without the data controller's consent;

(iv) cease the processing and return to the data controller any data received prior to the termination of its processing authority.

7

Does the Privacy Act require an agreement between a customer and a cloud provider? Describe its minimum content.

Yes, an agreement between a customer and cloud provider is required. The Privacy Act does not prescribe its minimum content except for the requirement that the agreement should include the data processor's obligations with respect to the measures related to personal data security.

8

Is the use of sub-processors by the cloud provider permissible? If so, are there any specific conditions or restrictions on the use of sub-processors?

Yes, subject to the data controller's consent. The data controller should not engage a data processor who, given the latter's profile (e.g. the nature of the data processor's professional activities) is likely to misuse the personal data. No other statutory conditions apply.

INTERNATIONAL DATA TRANSFERS

9

What are the requirements to transfer personal data to the EU?

The Privacy Act provides for an unrestricted transfer of personal data to countries which are specifically "whitelisted" pursuant to the Order N1 of the DPA dated 16 September, 2014. All EU Member States are "whitelisted".

10

What are the requirements to transfer personal data to a non-EU country?

Intended data transfers to countries not listed in the Order N1 (such as, for instance, the USA) are subject to the DPA's prior approval.

SECURITY

11

Does the Privacy Act impose any security requirements (technical and organizational measures) for cloud providers (or data processors, generally)? Please list the key requirements.

The Privacy Act does not elaborate on specific technical or organizational measures; rather, it provides for a general obligation of the data controller to implement appropriate organizational and technical measures to ensure the protection of data against accidental or unlawful destruction, alteration, disclosure, collection or any other form of illegal use, as well as accidental or unlawful loss thereof.

In addition, data controllers should maintain logs of all operations performed in relation to electronic data.

In case of data disclosure, the data controller and data processor must keep records of the following information: the specific data that was disclosed, to whom such data was disclosed, and when and on what legal grounds such data was disclosed. This information must be stored together with the data on a data subject it relates to for the entire (applicable) storage period.

12

Is the use of sub-processors by the cloud provider permissible? If so, are there any specific conditions or restrictions on the use of sub-processors?

No.

OTHER REQUIREMENTS

13

Is it permissible for a cloud provider to mine customer data for advertising purposes?

No. Under the Privacy Act, personal data may be processed only for predetermined, specific, clearly defined and legitimate purposes. Data processing for purposes that goes beyond and/or is incompatible with the original purpose or scope is therefore inadmissible.

14

Does the customer have the right to audit the cloud provider? Can the parties instead agree to an audit by an independent auditor selected by the cloud provider?

While the Privacy Act generally provides for the customer's right to monitor the processing of his personal data, it does not explicitly regulate the latter's audit right. In the absence of any restrictions, however, the parties are in principle authorized to: (i) include the customer's audit rights in their contract; and (ii) agree to an audit by an independent auditor nominated by the cloud provider.

15

Are there any prerequisites for a customer to use cloud services (such as notification or approval from the data protection authority)?

Apart from the general notification obligation of data controllers towards the DPA prior to the establishment of the personal data filing system (including subsequent notifications on additional entries of personal data in the respective filing system), and apart from the DPA's approval

required for data transfers to non-whitelisted countries (see questions 2 and10, respectively), the use of cloud computing services in itself is not subject to any specific notification or approval.

PUBLIC SECTOR

16

Are there any different data protection requirements applicable to cloud customers from the private or public sector?

No. The Privacy Act does not distinguish between public and private sector data controllers (a data controller is defined as any public or private institution, entity or natural person). Hence, the same statutory requirements generally apply to cloud customers from both private and public sector.

FINANCIAL DATA

17

Briefly summarize the key sector-specific legal and regulatory requirements that apply to financial data that financial institutions need to be aware of, if they wish to use cloud computing, if any.

Order N 47/04 of the National Bank of Georgia on Managing Operational Risks by Commercial Banks, dated 13 June 2014 ("NBG Order 47/04") regulates, among other things, requirements applicable to information technologies as well as outsourcing by commercial banks of their banking activities (and related information systems/technologies).

NBG Order 47/04 provides that commercial banks must employ policies and procedures that address the adequacy and security of their information systems which, in turn, should be based on recognized international standards (such as NIST or ISACA). Banks should regularly conduct information systems audits. Audits may be carried out either by internal audit units or external, recognized auditors.

Outsourcing agreement must provide for the authority of NBG to receive any information pertaining to the activities of a commercial bank.

Use of a foreign-based third-party service provider and the location of critical data and processes outside Georgia must not deprive or restrict NBG's ability to access or examine the commercial banks' banking operations. Outsourcing of the services to jurisdictions where full and complete access to information may be impeded by various legal or administrative constraints will be particularly sensitive and not acceptable.

18

Are there any notifications to or approvals on the use of cloud computing from the applicable regulator required?

Commercial banks should notify the NBG the details of the planned outsourcing arrangement. Within 30 business days of receipt of the notification (with a possible additional 30 day extension period), the NBG approves or disapproves the outsourcing arrangement. An outsourcing agreement which is not approved by the NBG is deemed invalid.

GUIDANCE NOTES AND RECOMMENDATIONS

19

Is there any local guidance on cloud computing issued by the data protection authority or any other relevant authority / regulator?

No. The DPA has not issued any guidance on cloud computing specifically.

PENDING LEGISLATION

20

Is there any pending legislation that will have significant impact on cloud computing?

No.