GAP ANALYSIS AND LEGISLATIVE ACTION PLAN – DIRECTIVE ON PRIVACY AND ELECTRONIC COMMUNICATIONS[1]

1 Introduction

1.1 Document purpose

Annex XV-B of the Association Agreement cites which parts of EU Legislative need to be implemented in Georgian Law in the field of Electronic communication networks and services. Relevant EU Legislative includes the: Framework Directive, Authorization Directive, Access Directive, Universal Service Directive, Directive on Privacy and Electronic Communications and the Radio Spectrum Decision.

This overview comprises of an analysis of gaps between the currently applicable Georgian law and the parts of the Directive on Privacy and Electronic Communications (the "**ePrivacy Directive**") which, according to the Accession Agreement, must be implemented in Georgian law by 1 September 2017.

1.2 Scope of review

The review has been conducted for the purposes of performance of consulting services for the project „Georgia - Information Communication Technology Sector Development: Harmonisation of laws, regulation of next generation access and regulatory development" (the „**Project**") and is intended to be confidential and covered by the attorney-client privilege, the attorney work product doctrine, and any other applicable privilege and/or protection. All documents prepared in connection with the review, including this document, are intended to be confidential and privileged and are produced for the sole purpose of providing legal advice within the scope of the Project.

This document is provided to and is capable of being relied on exclusively by GNCC and EBRD. The document may not be disclosed to, used by, or relied on by third parties without our explicit written consent, except as otherwise explicitly provided by us within the Project. Even if given, the consent will neither imply nor create any contractual relationship between third parties and us.

We conducted the review under the EU law in the scope stipulated in the Project and based on the English translations of the relevant laws and/or other documents were provided to use by GNCC. We are not qualified to provide legal advice under Georgian law. Unless we state differently in the document, we did not take into account any other law and any other document other than those provided to us by GNCC.

1.3 Association Agreement Requirements

According to the Association Agreement, Georgian Law must be approximated with the following provisions/parts of the e Privacy Directive:

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 as amended by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 and Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009

- Implementing regulation to ensure protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and ensure the free movement of such data and of electronic communication equipment and services.

1.4 Colour code and document structure:

This overview analyses individual requirements contained in the Accession Agreement in relation to the ePrivacy Directive and indicates our initial conclusions on the level of harmonisation of the relevant Georgian legislation by the following colour code:

No Gap / Harmonised	Partial Gap / partially harmonised but additional legislative measures are needed	Gap / not yet harmonised	Not applicable

When "No Gap" is identified, we provide no further comments.

When "Partial Gap" or "Gap" is identified, we provide further comments on the nature of the gap and initial recommendations regarding how such gap could be addressed. Our initial recommendations are incorporated in this legislative Action Plan, taking into account also the outcome of our discussions with GNCC. "Not applicable" refers to the parts of the ePrivacy Directive that cannot apply in Georgia because Georgia is not yet a Member State. This would typically include provisions that implement certain competences or coordination roles of the European Commission or other bodies, such as BEREC.

In the last chapter of this document we provide initial guidance on the harmonisation of Georgian law with the remaining parts of the ePrivacy Directive, which are not included in the Association Agreement.

1.5 Abbreviations and terms used

– ECA – Law of Georgia on Electronic Communications,

– PDPA – Law of Georgia on Personal Data Protection

– PCRS – Protection of Consumer Rights Resolution[2]

– DPD – Data Protection Directive[3]

– GDPR – General Data Protection Regulation[4]

[2] Resolution No. 3 of Georgian National Communications Commission, Tbilisi, 17 March, 2006 Concerning the Approval of the Regulations in respect to the Provision of Services and Protection of Consumer Rights in the Sphere of Electronic Communications.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

2 Executive Summary

The scope of the ePrivacy Directive is currently under review as the European Commission seeks to assess possible changes to the existing legal framework to make sure it is up to date with the new challenges of the digital area; the new legislative proposal is expected by the end of 2016. The ePrivacy Directive will most likely be revised to reflect the obligations arising from the GDPR which will become binding as of May 2018. The GDPR and ePrivacy Directive overlap in several segments. Even though some of the current provisions will be most likely maintained, the exact scope of the changes cannot be assessed at the moment. As the ePrivacy Directive represents a package of mutually intertwined rights and obligations in the area of data protection in electronic communications, we recommend that the GNCC wait with harmonization steps until the new legislative proposal on ePrivacy is adopted. Our analysis is based on the current wording of the ePrivacy Directive; however, where certain provision or topic is likely to be subject to a change, we make a reference to the relevant discussion. In this respect, we have confirmed with the GNCC that all rights and obligations related to unsolicited communications and direct marketing will not be subject to further implementation under this Action Plan as there is a new amendment to the PDPA in the legislative process which should include also the regulation of unsolicited communication. Under the currently applicable wording, we have identified the following main gap areas where Georgian law would have to be further harmonised with the ePrivacy Directive:

- Data protection is currently regulated only by the PDPA which aims at natural persons (individuals) only. However, the ePrivacy Directive generally provides for the same scope of protection of (or at least an assurance of adequate protection of legitimate interest of) legal persons in the context of electronic communications. Therefore, we propose that the ECA, which should thus serve as a set of specific sector data protection regulation for electronic communications, be amended in this respect.
- The obligations on confidentiality and publication of directories of the subscribers must be amended to reflect the corresponding ePrivacy Directive requirements. This includes regulation of cookies, which are not currently governed under Georgian law. We propose to introduce these regulations into the ECA.
- Georgian law (the ECA) should contain notification process to the competent national authority (the GNCC) and to the individuals for the events of personal data breach. Notification of individuals concerned is not required when the service provider implemented appropriate technological protection measures that were applied to the data affected by the breach, rendering them unintelligible. We propose that the ECA be amended in this respect.
- Traffic, location and other data related to the electronic communications, automatic call forwarding, privacy protection related to itemised billing, presentation and restriction of calling and connected line identification and technical features and standardisation required under the ePrivacy Directive are not addressed by Georgian laws. We propose that relevant requirements of the ePrivacy Directive be thus transposed into the ECA;, however, in this connection we also wish to point out that the existing ePrivacy rules related to location, traffic and other data (within the meaning of the ePrivacy Directive) will most likely be further modified in the foreseeable future light of the GDPR.

3 Detailed Gap Analysis

A General provisions

	ePrivacy Directive		Georgian Legislation	Gap
Art 1/1	This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and **in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector** and to ensure the free movement of such data and of electronic communication equipment and services in the Community.	Art 3/1 PDPA	This Law shall apply to the processing of data through automatic or semi-automatic means, and to the processing of data through non-automatic means within the territory of Georgia, which data form part of the filing system or are intended to form part of the filing system. This Law shall also apply to automatic processing of data defined as a state secret for the crime prevention and investigation, operational-investigative activities and protection of the rule of law, except as provided in this article.	
		Art 3/2 PDPA	This Law shall also apply to: a) data processing by diplomatic representations and consular offices of Georgia abroad; b) activities of a data processor who is not registered in the territory of Georgia but employs technical means existing in Georgia for data processing, except when these technical means are used only for data transfer. In this case, the data controller must appoint/designate a registered representative in Georgia.	
Gap 1 – Scope of applicability The PDPA aims at protection of data processed through automatic, semi- or non-automatic means within the territory of Georgia. Such scope of applicability				

is compliant with the ePrivacy Directive.

We consider this to be a gap in the PDPA since it does not explicitly govern data processing in the electronic communication sector which has its specifics and which regulation is the purpose of the ePrivacy Directive. The general data protection on the EU level is subject to the DPD, which is not subject to this gap analysis. By contracts, the ePrivacy Directive governs the specifics of personal data processing in electronic communications. Therefore, the PDPA or, more likely, the ECA, needs to be harmonized (supplemented) in order to comply with this ePrivacy Directive. Furthermore, the focus on privacy as one of the fundamental rights and freedoms should also be stressed in the relevant implementing law.

Action plan

Legislation:	ECA
Section:	New chapter in the ECA
Proposed change:	We propose that the rights and obligations arising from the ePrivacy Directive be implemented into the ECA and/or into a separate law.
Notes:	As the scope of the ePrivacy Directive is rather broad - it regulates a number of various areas, including personal data protection - many EU Member States chose to implement the ePrivacy Directive into a broad range of laws, including the PCRS. For your reference, please see the overview of national laws implementing the ePrivacy Directive (http://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32002L0058) and its amendments enacted in 2006 (http://eur-lex.europa.eu/legal-content/EN/NIM/?uri=celex:32006L0024) and in 2009 (http://eur-lex.europa.eu/legal-content/EN/NIM/?uri=celex:32009L0136).

Art 1/2	The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.	N/A		

Gap 2 – Protection of legal persons

There is a gap arising from the absence of any data protection of legitimate interest of legal persons (entities). Under Georgian law, personal data are

protected only under the PDPA which aims at protection of natural persons; while this addresses compliance with the DPD, it does not address compliance with the ePrivacy Directive. The ePrivacy Directive as sector specific legislation protects data of both natural and legal persons in the context of electronic communications. The PDPA or the ECA, as applicable, should therefore be amended in this respect.

Action plan	
Legislation:	ECA
Section:	New chapter in the ECA
Proposed change:	We propose that the protection of legitimate interests of legal persons be implemented into Georgian laws in accordance with the requirements of the ePrivacy Directive. The protection applies to and permeates through the entire scope of the ePrivacy Directive and as such must be considered for every single right and obligation under the ePrivacy Directive.
Notes:	/

Art 1/3	This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.	Art 3/1 PDPA	**This Law shall also apply to automatic processing of data** defined as a **state secret for the crime prevention and investigation, operational-investigative activities and protection of the rule of law**, except as provided in this article.	
		Art 3/6 PDPA	Article 6 of this Law shall not apply to data processing for public safety, operational and investigative activities and criminal investigations if the a is directly and specifically regulated under the Criminal Procedure Code of Georgia or the Law of Georgia on Operational and Investigative Activities or other special laws.	
		Art 3/3/c PDPA	This Law shall not apply to: c) processing of the data defined as a state secret for the	

			purposes of state security (including economic security), defence, intelligence and counterintelligence activities;	
		Art 3/3/d PDPA	This Law shall not apply to: d) processing of information defined as a state secret (except for the data specified in paragraph 1 of this article).	

Gap 3 – Exemptions from applicability

The ePrivacy Directive does not apply to the areas of public security, defence, state security (including the economic well-being of the state when the activities relate to state security matters) and the activities of the state in areas of criminal law.

The PDPA, on contrary, applies to automatic processing of data defined as a state secret for the crime prevention and investigation, operational-investigative activities, but provides for several exceptions.

We consider the discrepancy in the scope of applicability of the ePrivacy Directive to be a partial gap and recommend that crime prevention and investigation be excluded from the scope of data protection in the electronic communications (given, in particular, the fact that the ePrivacy Directive is applicable both to individuals and entities).

Action plan

Legislation:	ECA
Section:	New chapter in the ECA
Proposed change:	We propose that crime prevention and investigation be excluded from the scope of data protection in the electronic communications (given, in particular, the fact that ePrivacy is applicable both to individuals and entities).
Notes:	/

Art 2	Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) shall apply. The following definitions shall also apply:	Art 2 PDPA	The terms used in this Law have the following meanings:	
Art 2/a	"user" means any natural person using a publicly available electronic communications service, **for private or business purposes**, without necessarily having subscribed to this service	Art 2/z[16] ECA	user - a natural or legal person who intends to use or that uses electronic communication services	
Art 2/b	"traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof	N/A		
Art 2/c	"location data" means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;	N/A		
Art 2/d	"communication" means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or	N/A		

	user receiving the information			
Art 2/f	"consent" by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC	Art 2/g PDPA	consent– a voluntary consent of a data subject, after receipt of the respective information, on his/her personal data processing for specific purposes expressed orally, through telecommunication or other appropriate means, which enables clearly establishing the will of the data subject	
Art 2/h DPD	*'the data subject's consent' - any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed)*	Art 2/h PDPA	written consent of the data subject – a voluntary consent expressed by a data subject, after receipt of the respective information on his/her personal data processing for specific purposes, which was signed or otherwise acknowledged by the data subject in writing or in any other equivalent form;	
Art 2/g	"value added service" means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof	N/A		
Art 2/h	"electronic mail" means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient	N/A		
Art 2/i	“personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.	N/A		

Gap 4 - Definitions

The current Georgian legislation does not govern data protection in electronic communications and therefore most of the terms are not included in the laws at all. We recommend that with the exception of the term of "consent" (which is already in the PDPA) and the term of "personal data breach" (which we recommend introducing in the PDPA) the above terms be amended and/or added into the ECA.

Action plan	
Legislation:	ECA
Section:	2
Proposed change:	We propose that the following definitions be added into the ECA to align with the ePrivacy Directive: - traffic data, location data, communication, consent, value added services, personal data breach, user (in the meaning of subscriber as defined under 2/a ePrivacy Directive).
Notes:	The definition of "user" should be aligned with the ePrivacy Directive (while, at the same time, should not be contradictory to its current use throughout the ECA) as well as with the Framework Directive. As discussed with the GNCC, the changes will be implemented in the ECA and subsequently, as a result of the activity of a working group, in the PCRS. For the purposes of this Action Plan, we only include change in the primary law.

Art 3	This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.	Art 25/1 PCRS	The protection of rights and legitimate interests of consumers in the sphere of electronic communications is supervised by the Commission, whereat there operates the agency of Public Defender of Consumers Interests.	

Gap 5 – Data protection in electronic communication

The current Georgian legislation does not generally govern data protection in electronic communications. The PCRS, a GNCC's resolution, partially

addresses the rights of individuals in the sphere of the electronic communications but only with regard to the protection of consumers. Therefore, adjustment of the laws in terms of a broader scope of application will be required.	
Action plan	
Legislation:	ECA
Section:	New chapter in the ECA
Proposed change:	We propose that the protection of legitimate interests of legal persons be implemented into Georgian laws in accordance with the requirements of the ePrivacy Directive. The protection applies to and permeates through the entire scope of the ePrivacy Directive and as such must be considered for every single right and obligation under the ePrivacy Directive.
Notes:	/

B Security measures

	ePrivacy Directive		Georgian Legislation	Gap
Art 4/1	The provider of a publicly available electronic communications service must **take appropriate technical and organisational measures** to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security.	Art 17/1 PDPA	A data controller shall be obliged to take appropriate organisational and technical measures to ensure protection of data against accidental or unlawful destruction, alteration, disclosure, collection or any other form of unlawful use, and accidental or unlawful loss.	
		Art 17/4 PDPA	Any employee of a data controller and of a data processor, who is involved in processing of data, shall be obliged to stay within the scope of powers granted to him/her. In addition, he/she shall be obliged to protect data secrecy, including after his/her term of office terminates.	
		Art 17/5 PDPA	The data security measures shall be defined by the legislation of Georgia.	
		Art 19/2/e ECA	An authorised person shall: e) maintain integrity and security of the network	
		Art 25/4/j PCRS	Service provider shall be obliged to: (j) if, for technical reasons, a service provider cannot ensure the protection of the network in his possession, he must inform the consumers about the existing risk of unauthorized access to the network on the part of third persons; in case of availability of relevant technical possibility, the service provider must offer to the consumers concerned the service designed to protect consumers from	

			such unauthorized access	

Gap 6 – Technical and organisational measures

The PDPA, ECA and PCRS all stipulate that a service provider (in case of the ECA an authorised person) shall implement and maintain appropriate technical and organisational measures in order to ensure the adequate protection.

There is a gap arising from the fact that none of the respective laws impose any obligations on the service provider (authorised person) to cooperate with the provider of the public communications network when required. The obligation should therefore be added into the relevant law (preferably into the ECA as the sector-specific law).

Action plan	
Legislation:	ECA
Section:	New chapter in the ECA
Proposed change:	We propose that the ECA be amended in respect of security measures that must be taken by a provider of a publicly available electronic communications service. In addition, an obligation on the service provider (authorised person) to cooperate with the provider of the public communications network when required should be added into the ECA.
Notes:	We propose an amendment of the ECA as we believe that the obligations of providers of electronic communications should be concentrated in one single law. The ECA would thus represent a unified code that would comprehensively cover all data protection-related obligations relevant to electronic communications.

Art 4/1	Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.	Art 17/3 PDPA	Measures taken to ensure data security must be adequate to the risks related to processing of data.	

Gap 7 – State of the art

While the provisions on security measures are largely aligned, there is a partial gap arising from the absence of consideration of the 'state of the art' with respect to the measure implemented, as well as the cost of implementation of the particular technical and organisational measures. Such specification is recommended with respect to measures adopted in electronic communications.

Action plan	
Legislation:	ECA
Section:	New chapter in the ECA
Proposed change:	We propose to introduce into the ECA an obligation on the service providers to implement such technical and organisational measures that take into account the 'state of the art' as well as implementation costs.
Notes:	/

Art 4/1a	Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least: – ensure that personal data can be accessed only by authorised personnel for legally authorised purposes, – protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and – ensure the implementation of a security policy with respect to the processing of personal data.	Art 17/1 PDPA	A data controller shall be obliged to take appropriate organisational and technical measures to ensure protection of data against accidental or unlawful **destruction, alteration, disclosure, collection or any other form of unlawful use, and accidental or unlawful loss**.	
		Art 25 PCRS	4. **Service provider** shall be obliged to: (h) protect the integrity and impenetrability of the network and prevent any unauthorized use of networks and facilities; (i) take **measures to protect consumers** from any possible risks posed by service; on request, to provide consumer with filtering software; 5. Based on the notification from a consumer, service provider	

			shall address the issue and adopt all available measures in order to prevent the use of his network for: (a) unauthorized access;	
		Art 17 PDPA	2. A data controller shall be obliged to ensure registration of all operations performed in relation to electronic data. When processing non-electronic data, a data controller shall be obliged to register all operations with respect to disclosure and/or alteration of data. 3. Measures taken to ensure data security **must be adequate to the risks related to processing of data**. 4. **Any employee** of a data controller and of a data processor, who is **involved in processing of data, shall be obliged to stay within the scope of powers granted to him/her**. In addition, he/she shall be obliged to protect data secrecy, including after his/her term of office terminates.	

Gap 8 – Security policy and other measures

The provisions on technical and organisational measures are largely aligned with ePrivacy Directive requirements. The only partial gap we have identified in the PDPA is the absence of specific obligation to implement a security policy as one of the technical and organisational measures. Further, the protection should be specifically extended to transmitted data (currently not addressed under the PDPA or PCRS).

Therefore we recommend that the security policy requirement and the guarantee of protection of transmitted data be added to the PDPA or, preferably, to the ECA, which would comprehensively cover all data protection-related obligations relevant to electronic communications.

Action plan

Legislation: ECA

Section:	New chapter in the ECA
Proposed change:	Add into the ECA the obligation on service providers to implement security policy and other necessary security measures as required by the ePrivacy Directive.
Notes:	We note that the necessary requirements are already implemented in the PDPA. However, we propose that all specifics related to the data protection in the field of electronic communications be implemented in the ECA as a unified code that would comprehensively cover all data protection-related obligations relevant to electronic communications.

Art 4/1a	Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.	Art 25/1 PCRS	The protection of rights and legitimate interests of consumers in the sphere of electronic communications is supervised by the Commission, whereat there operates the agency of Public Defender of Consumers Interests.	
		Art 35/2 PDPA	An inspection conducted by the Inspector shall mean to: b) inspect the compliance of procedures to protect data and of the organisational and technical measures with the requirements of this Law; e) inspect compliance with the procedures for data protection established by this Law and other normative acts.	
		Art 35/5 PDPA	The Inspector shall be authorised to enter any institution or organisation to conduct an inspection, and review any document and information, including information containing commercial and professional secrets, as well as materials concerning operative and investigative activities and crime investigation that are considered as state secrets, regardless of their content and form of storage.	
		Art 38/2	The Inspector's report must include general assessments of the	

		PDPA	situation in the area of data protection, conclusions and recommendations, as well as the information on significant violations detected during a given year and measures undertaken.	
Comment – Audit rights The ePrivacy Directive provides for audit rights for relevant national authority. According to the PDPA the audit rights are entrusted to the Inspector (who is generally responsible for personal data protection). We have identified no gap.				
Art 4/2	In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.	Art 25/4/j PCRS	Service provider shall be obliged to: (j) if, for technical reasons, a service provider cannot ensure the protection of the network in his possession, **he must inform the consumers about the existing risk of unauthorized access to the network on** the part of third persons; in case of availability of relevant technical possibility, the service provider must offer to the consumers concerned the service designed to protect consumers from such unauthorized access;	
Gap 9 – Information on security breach The ePrivacy Directive requires that the provider is obliged to inform its subscribers if there is a particular risk of a breach of the security of the network. Such obligation is currently governed only under the PCRS, i.e. only with regard to consumers. We assess this as a partial gap and recommend that the notification obligation be therefore imposed on services providers with respect to all persons (both legal and natural) to whom they provide electronic communications services.				
Action plan **Legislation:** ECA				

Section:	New chapter in the ECA			
Proposed change:	Include in the ECA a notification obligation for services providers (concerning the risk of security breach) that would extend to all subscribers, i.e. both natural and legal persons, to whom they provide electronic communications services.			
Notes:	/			
Art 4/3	**In the case of a personal data breach**, the provider of publicly available electronic communications services shall, without undue delay, **notify the personal data breach to the competent national authority**. When the personal data breach is **likely to adversely affect the personal data or privacy of a subscriber or individual**, the provider shall also **notify the subscriber** or individual of the breach without undue delay. **Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures**, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it. Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach,	N/A		

	may require it to do so. The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.			
Art 4/4	Subject to any technical implementing measures adopted under paragraph 5, the competent national authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made. They shall also be able to audit whether providers have complied with their notification obligations under this paragraph, and shall impose appropriate sanctions in the event of a failure to do so. Providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of paragraph 3. The inventory shall only include the information necessary for this purpose.	N/A		

Gap 10 – Data breach notification

There is a gap with regard to the absence of any notification obligation in case of a personal data breach and all measures related thereto. Service providers shall be obliged to notify the regulator and, where the breach is likely to adversely affect the personal data or privacy of a subscriber or individual, also that subscriber or individual.

However, the scope of the notification obligation under the ePrivacy Directive is currently under review and will likely be amended to reflect the breach notification obligations arising from the GDPR which shall become binding as of May 2018. The GDPR and ePrivacy Directive overlap in several areas, including in the area of data breach notification. While the data breach notification obligation is in any event expected to be retained, since the specific parameters are yet to be aligned with the GDPR, it is advisable to wait with the implementation of this obligation until the updated legislative proposal on ePrivacy is adopted.

Action plan	
Legislation:	ECA
Section:	New chapter of the ECA
Proposed change:	Introduce into the ECA service providers' obligation to notify the GNCC (and in some cases subscribers) in case of a personal data breach and all measures related thereto.
Notes:	The current scope of data breach notification under the ePrivacy Directive is likely to be reassessed in view of the GDPR. However, as the obligations arising out of the Association Agreement are binding upon Georgia, and following our discussion with the GNCC, the obligations related to data breaches will be enacted in the ECA notwithstanding any pending legislative processes in the EU concerning the ePrivacy Directive, and at least until generally applicable rules are introduced in the PDPA. Furthermore, as discussed with the GNCC, we note that the division of competences between NRAs and DPAs throughout the EU is not subject to a common approach. For example, in the Czech Republic all competences related to personal data protection (including in the field of the electronic communications) are generally exercised by the Czech DPA. By comparison, in Slovakia the Slovak NRA is responsible for personal data protection in the area of electronic communications.

Art 4/5	In order to ensure consistency in implementation of the measures referred to in paragraphs 2, 3 and 4, the	N/A		

	Commission may, following consultation with the European Network and Information Security Agency (ENISA), the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC and the European Data Protection Supervisor, adopt technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements referred to in this Article. When adopting such measures, the Commission shall involve all relevant stakeholders particularly in order to be informed of the best available technical and economic means of implementation of this Article. Those measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 14a(2).'			

C Confidentiality of communications

	ePrivacy Directive		Georgian Legislation	Gap
Art 5/1	Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1).	Art 8/1 ECA	Information on a user of electronic communication networks, also information transferred by a user via said networks, shall be confidential and its confidentiality shall be guaranteed by the legislation of Georgia.	
		Art 8/2 ECA	All persons employed in the field of electronic communications are obliged to maintain the confidentiality of information referred to in paragraph 1 of this article. Employees and other persons working in the field of electronic communications shall be held liable in accordance with the legislation of Georgia if they reveal such information.	
		Art 11/3/p ECA	The main functions of the Commission are to: (p) monitor the quality of the maintenance of confidentiality of information in the field of electronic communications.	
		Art 25/3 PCRS	Service provider shall be obliged to ensure the secrecy and safety of the information transmitted by consumers. The tapping of telephone conversation and the disclosure of the information on the said conversations shall be admissible in conformity with the procedure established under the Georgian Legislation.	
		Art 25/5/k PRCS	Service provider shall be obliged to: (k) in case if, as a result of the specificity of a service, the conversation with a consumer is being recorded, warn the consumer about this before the beginning of such service;	
Art 5/1	Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available	Art 8/3 ECA	The obligation of confidentiality of information provided for in paragraph 1 of this article shall not apply to cases where an authorised body carries out covert investigative activities	

	electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, **except when legally authorised to do so in accordance with Article 15(1).**		envisaged by Article 1431(1)(a, b) of the Criminal Procedure Code of Georgia.	
		Art 8^1 ECA	Upon the request of an authorised body, an electronic communications company should have a technical capability to deliver, in real time, to the monitoring system of an authorised body the content and identification data of communications sent via its networks.	
		Art 8^2 ECA	An electronic communications company shall record instances when the identification data of electronic communications are transferred under Articles 112 and 136 of the Criminal Procedure Code of Georgia to relevant state bodies and shall provide the relevant information to the Personal Data Protection Inspector.	
Art 5/1	This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.	Art 8/5 ECA	Information on the content of the communication made by a user via an electronic communication network shall be immediately and automatically destroyed. Said information may become available only to the entity specified in Article 81 of this Law in accordance with the procedure established by law.	
Art 5/2	Paragraph 1 **shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice** for the purpose of providing evidence of a commercial transaction or of any other business communication.	N/A		
Art 5/3	Member States shall ensure that the **storing of information, or the gaining of access to information already stored**, in the terminal equipment of a subscriber or user is only **allowed on condition that the subscriber**	N/A		

	or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.			

Gap 11 – Confidentiality of communications

There are gaps in the current obligations regarding the confidentiality of communications stipulated under the ECA. The PRCS provides for confidentiality, however, only in respect of consumers. The obligations regarding prohibition of listening, tapping etc. arising out of the ePrivacy Directive should be therefore implemented into the ECA in order to protect both natural and legal persons in the scope required therein. The regulation of cookies under Article 5/3 of the ePrivacy Directive is not currently reflected in the Georgian law and should be added, preferably, into the ECA, and may also be more detailed in the PCRS with respect to consumers.

However, the scope of the confidentiality (including regulation of cookies) under the ePrivacy Directive is currently under review and will likely be amended to reflect the obligations arising from the GDPR which shall become binding as of May 2018. The GDPR and ePrivacy Directive overlap in several areas, including in the area of confidentiality. It is thus advisable to wait with the implementation of the confidentiality obligation until the updated legislative proposal on ePrivacy is adopted.

Action plan	
Legislation:	ECA,
Section:	New chapter of the ECA.
Proposed change:	We propose that the obligations regarding prohibition of listening, tapping etc. in electronic communications arising out of the ePrivacy Directive be implemented into the ECA in order to protect both natural and legal persons in the scope required therein. We further propose to introduce regulation of cookies which is not currently reflected in the Georgian law, preferably into the

	ECA. The cookie regulation may also be further elaborated on in the PCRS with respect to consumers.
Notes:	The current regulation of confidentiality of communications, including regulation of cookies, under the ePrivacy Directive is likely to be reassessed in view of the GDPR. However, as the obligations arising out of the Association Agreement are binding upon Georgia, the obligations related to confidentiality of communications will be enacted in the ECA notwithstanding any pending legislative processes in the EU concerning the ePrivacy Directive.

D Traffic data

	ePrivacy Directive		Georgian Legislation	Gap
Art 6/1	**Traffic data relating to subscribers and users processed and stored** by the provider of a public communications network or publicly available electronic communications service **must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication** without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).	Art 8/5 ECA	Information on the content of the communication made by a user via an electronic communication network shall be immediately and automatically destroyed. Said information may become available only to the entity specified in Article 8^1 of this Law in accordance with the procedure established by law.	
Art 6/2	**Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed**. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.	N/A		
Art 6/3	**For the purpose of marketing electronic communications services or for the provision of value added services**, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and **for the duration necessary for such services or marketing**, if the subscriber or user to whom the data relate has given his or her **prior consent**.	Art 8/3 PDPA	Any data may be processed for direct marketing purposes on the basis of a written consent given by a data subject as determined by this Law.	
Art 6/6	**Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.**	Art 8/4 PDPA	A data subject shall have the right to require at any time that a data controller stop to use of his/her data for direct marketing purposes.	
Art 6/4	The service provider must inform the subscriber or user of	Art 15/1	If data are collected directly from a data subject, a data	

	the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.	PDPA	controller or a data processor shall be obliged to provide the data subject with the following information: a) identities and registered addresses of the data controller and the data processor (if applicable); b) purpose of data processing; c) whether provision of data is mandatory or voluntary; if mandatory – the legal consequences of refusal to submit them;	
Art 6/5	Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.	N/A		
Art 6/6	Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.	N/A		

Gap 12 – Traffic data

The ECA (or other Georgian laws under review) does not specifically address the treatment of traffic data. Some of the general provisions of the ECA relating to the content of the communication likely apply also to traffic data, but a specific regime for the processing and use of traffic data, reflecting the provisions of the ePrivacy Directive, should be implemented.

However, the scope of the regulation of traffic data under the ePrivacy Directive is currently under review. It can be anticipated that the obligations related to traffic data will be made even more restrictive. Some of the traffic data are undoubtedly personal data and must be treated as such. The current level of protection under the ePrivacy Directive might be thus reassessed in view of the GDPR. It is thus advisable to wait with the implementation of the obligations

related to traffic data until the updated legislative proposal on ePrivacy is adopted.

Action plan	
Legislation:	ECA
Section:	New chapter of the ECA
Proposed change:	We propose to implement the regulation of traffic data (including all related provisions) into the ECA.
Notes:	The current level of protection of traffic data under the ePrivacy Directive is likely to be reassessed in view of the GDPR However, as the obligations arising out of the Association Agreement are binding upon Georgia, the obligations related to traffic data will be enacted in the ECA notwithstanding any pending legislative processes in the EU concerning the ePrivacy Directive.

E Itemised billing

	ePrivacy Directive		Georgian Legislation	Gap
Art 7/1	Subscribers shall have the right to receive non-itemised bills.	Art 2/m	**billing information** - data on services provided to users or on the loading of relevant elements of the operator's network (traffic) and on the amount of the operational resources **used during a certain period of time**, which are shared between operators or provided to an end-user for payment;	
		Art 62/3 ECA	**Users shall be entitled to receive information**, including on the tariffs of the provided or selected electronic communication services, on the conditions of providing services and rules of payment, and **detailed billing information** for the relevant reporting period.	
		Art 4/1/c PCRS	Consumer shall have the right without delay to receive from the service provider the information, including: concerning the type, tariff, date, time of provision of service, duration of provision of service, and numbers of outgoing calls in respect to the services rendered during the reporting period; and in case of payment of the fee established by service provider (which fee must be cost-oriented) – a detailed account of incoming calls and the non-reporting period;	
Art 7/2	Member States shall apply national provisions in order to **reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers**, for example by ensuring that sufficient alternative privacy enhancing methods of communications	N/A		

	or payments are available to such users and subscribers.			

Gap 13 – Itemised billing

According to the ePrivacy Directive the subscribers are entitled to receive non-itemised billing and in case that they receive itemised billing, Member States are obliged to ensure that rights of calling users and called subscribers are protected.

Both the ECA and PCRS provide for that the users (customers in case of the PCRS) are entitled to receive information about the conditions of services provided to them including tariff and payment information. The ECA further stipulates that detailed billing information is to be provided to the users.

We consider missing provision on any additional protection of calling users and called subscribers to be a gap and recommend that these measures be added to the ECA.

Action plan	
Legislation:	/
Section:	/
Proposed change:	/
Notes:	The GNCC will confirm with the Georgian DPA that the rights of subscribers receiving itemised bills are reconciled with the right to privacy of calling users and called subscribers.

F Presentation and restriction of calling and connected line identification

	ePrivacy Directive		Georgian Legislation	Gap
Art 8/1	Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.	N/A		
Art 8/2	Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge for reasonable use of this function, of preventing the presentation of the calling line identification of incoming calls.	N/A		
Art 8/3	Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.	N/A		
Art 8/4	Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling user.	N/A		
Art 8/5	Paragraph 1 shall also apply with regard to calls to third	N/A		

	countries originating in the Community. Paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries.			
Art 8/6	Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available electronic communications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.	N/A		

Gap 14 – Presentation and restriction of calling

There is a gap in the ECA that relates to the absence of presentation and restriction of calling and connected line identification. We recommend that a corresponding procedure be added to the ECA.

Action plan

Legislation:	ECA
Section:	New chapter in the ECA
Proposed change:	Introduce into the ECA regulation on presentation and restriction of calling that would be aligned with the ePrivacy Directive.
Notes:	/

G Location data other than traffic data

	ePrivacy Directive		Georgian Legislation	Gap
Art 9/1	Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.	N/A		
Art 9/2	Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.	N/A		
Art 9/3	Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available	N/A		

	communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.			
Art 10	Member States shall ensure that there are transparent procedures governing the way in which a provider of a public communications network and/or a publicly available electronic communications service may override: (a) the elimination of the presentation of calling line identification, on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls. In this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public communications network and/or publicly available electronic communications service; (b) the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognised as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls.	N/A		

Gap 15 – Location and other than traffic data

There is a gap in the ECA regarding regulation of location data (other than traffic data), including any exemptions from such regulation. We recommend that the relevant provisions on location data be implemented into the ECA.

However, the scope of the regulation of location data (other than traffic data) under the ePrivacy Directive is currently under review. It can be anticipated

that the obligations related to location and other data will be made even more restrictive. Some of the location data are undoubtedly personal data and must be treated as such. The current level of protection under the ePrivacy Directive might be thus reassessed in view of the GDPR. It is therefore advisable to wait with the implementation of the obligations related to location data until the updated legislative proposal on ePrivacy Directive is adopted.

Action plan	
Legislation:	ECA
Section:	New chapter in the ECA
Proposed change:	We propose to implement the regulation of location and other and traffic data (and all related provisions) into the ECA.
Notes:	The current level of protection of location and other than traffic data under the ePrivacy Directive is likely to be reassessed in view of the GDPR. However, as the obligations arising out of the Association Agreement are binding upon Georgia, the obligations related to location data will be enacted in the ECA notwithstanding any pending legislative processes in the EU concerning the ePrivacy Directive.

H Automatic call forwarding

	ePrivacy Directive		Georgian Legislation	Gap
Art 11	Member States shall ensure that any subscriber has the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the subscriber's terminal.	N/A		

Gap 16 – Automatic call forwarding

There is a gap in the ECA concerning the absence of any regulation of automatic call forwarding. We recommend that corresponding provisions be implemented into the ECA.

Action plan

Legislation:	ECA
Section:	New chapter in the ECA
Proposed change:	Introduce an obligation on service providers to provide any subscriber with the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the subscriber's terminal.
Notes:	/

I Directories of subscribers

	ePrivacy Directive		Georgian Legislation	Gap
Art 12/1	Member States shall ensure that **subscribers are informed, free of charge and before they are included in the directory**, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.	Art 7 PCRS	Telephone guidebook shall contain following information: (a) Subject to the prior consent of a consumer, the name and surname of the consumer concerned, the address and telephone number of the intended venue of the installation of hardware;	

Gap 17 – Information to subscribers

Neither the PCRS or any other law reviewed include an obligation to inform subscribers about the purpose(s) of a directory of subscribers and its usage possibilities, which would help them decide whether to publish their contact details in the directory and which are required by the ePrivacy Directive. We recommend that the information obligation is introduced in the applicable law.

Action plan	
Legislation:	ECA, PCRS
Section:	New chapter in the ECA 7 PCRS
Proposed change:	We propose that a general provision concerning the directories of subscribers be implemented into the ECA. We further propose that the PCRS impose an obligation that the subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.

Notes:	/			
Art 12/2	Member States shall ensure that subscribers are given the opportunity to **determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose** of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.	Art 7 PCRS	Telephone guidebook shall contain following information: (a) **Subject to the prior consent** of a consumer, the name and surname of the consumer concerned, the address and telephone number of the intended venue of the installation of hardware;	
Gap 18 – Option to decide The PCRS provides that consumers must consent prior to use of their data in the telephone book. Such opt-in regime is compliant with the requirements of the ePrivacy Directive. The ePrivacy Directive further stipulates that the data subjects must be provided with an opportunity to verify and correct their data, and to withdraw their consent with such use. This right of a subscriber is not spelled out in the PCRS, and should thus be introduce in the applicable law.				
Action plan				
Legislation:	PCRS			
Section:	7/a			
Proposed change:	We propose that Article 7 PCRS be amended as to stipulate that the data subjects must be provided with an opportunity to verify and correct their data, and to withdraw their consent with such use.			
Notes:	/			
Art 12/3	Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of	N/A		

	the subscribers.			

Gap 19 – Use of telephone books data

According to the ePrivacy Directive, Member States may require additional consent of the subscriber in case the data in the telephone books (directories) are to be used for other purpose(s). Georgian laws do not include a corresponding requirement with respect to the use of subscriber data published in directories.

As such obligation is at a Member State's discretion, no action is required in this respect.

Action plan

Legislation:	PCRS
Section:	7/a
Proposed change:	We propose that the subscribers be provided with an option to state whether they consent with their data being used for other purposes than the purposes of telephone directories, especially if they consent to the use of the data for marketing purposes.
Notes:	/

Art 12/4	Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.	N/A		

Gap 20 – Legal persons in telephone guidebooks

The telephone guidebooks are regulated by the PCRS and the regulation is thus relevant only to subscribers who are consumers. The applicability of these provisions should be extended to all natural persons as required under the ePrivacy Directive and the national legislation should also ensure that legitimate interest of other persons are sufficiently protected, too.

Action plan	
Legislation:	ECA
Section:	New chapter in the ECA, general provision
Proposed change:	We propose that a general provision concerning directories of subscribers be introduced into the ECA that would guarantee sufficient protection of the legitimate interests of legal persons (entities)..
Notes:	/

J Unsolicited communications

	ePrivacy Directive		Georgian Legislation	Gap
Art 13/1	The **use of automated calling and communication systems without human intervention** (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be **allowed only in respect of subscribers or users who have given their prior consent**.	Art 8/1 PDPA	Data obtained from publicly available sources may be processed for direct marketing purposes.	
		Art 8/3 PDPA	Any data may be processed for direct marketing purposes on the basis of a written consent given by a data subject as determined by this Law.	

Gap 21 – Opt-in for automated calling

There is a gap with regard to the fact that the PDPA allows the use of publicly available data for direct marketing purposes without the data subject's consent, while the ePrivacy Directive requires that subscribers and users of electronic communication services give a prior consent with the use of their contact details for the purposes of direct marketing (i.e. the ePrivacy Directive prescribes a specific consent regime for direct marketing in electronic communications, which is stricter than the general regime for the use of data for direct marketing under the DPD). In addition, the PDPA does not distinguish between the ways in which the subscriber and user may be contacted based on this opt-in regime (automated calling, communication without human intervention, fax, e-mail). The applicable laws should thus be harmonised accordingly.

However, the ePrivacy Directive is currently under review and it can be anticipated that the regulation of unsolicited communication and direct marketing will be amended in light of the GDPR. It is therefore advisable to wait with the implementation of the rules on the use of subscriber and user contact data for direct marketing purposes until the updated legislative proposal on ePrivacy Directive is adopted.

Action plan

Legislation:	ECA
Section:	/
Proposed change:	/
Notes:	The current level of use of personal data for direct marketing purposes under the ePrivacy Directive is likely to be reassessed in view of the GDPR. It is therefore advisable to wait with the implementation of the obligations related to location data until the

			updated legislative proposal on the ePrivacy Directive is adopted. Further, the Georgian PDPA is currently under review and will most likely include the regulation of unsolicited communications, too.	
Art 13/2	Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their **electronic contact details for electronic mail, in the context of the sale of a product or a service**, in accordance with Directive 95/46/EC, the same natural or legal person **may use these electronic contact details for direct marketing of its** own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and on the occasion of each message in case the customer has not initially refused such use.	Art 8/1 PDPA	Data obtained **from publicly available sources** may be processed for direct marketing purposes.	
		Art 8/2 PDPA	**Regardless of the purpose of data collection**, the following data may be processed for direct marketing purposes: name (names), address, telephone number, **e-mail address**, fax number.	
Gap 22 – Use of electronic contact for direct marketing purposes The PDPA does not further distinguish the source of the data and thus does not reflect the rule (exception to the general op-in rule described above) according to which only e-mail contact details legally obtained from an existing customer in conjunction with sale of products/provision of services can be used for (own) direct marketing based without the customer's prior consent (opt-out rule).				
Action plan				
Legislation:	/			
Section:	/			
Proposed change:	/			
Notes:	The current level of use of personal data (including electronic contact) for direct marketing purposes under the ePrivacy Directive			

	is likely to be reassessed in view of the GDPR. It is therefore advisable to wait with the implementation of the obligations related to location data until the updated legislative proposal on the ePrivacy Directive is adopted. Further, the Georgian PDPA is currently under review and will most likely include the regulation of unsolicited communications, too.			
Art 13/3	Member States shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers or users concerned or in respect of subscribers or users who do not wish to receive these communications, the choice between these options to be determined by national legislation, taking into account that both options must be free of charge for the subscriber or user.	Art 8/4 PDPA	A data subject shall have the right to require at any time that a data controller stop to use of his/her data for direct marketing purposes.	
		Art 8/5 PDPA	A data controller shall be obliged to stop data processing for direct marketing purposes and/or ensure that a data processor stop data processing for direct marketing purposes not later than 10 working days after the request of a data subject is received.	
		Art 8/6 PDPA	When data are processed for direct marketing purposes a data controller shall be obliged to notify a data subject of the right under paragraph 4 of this article and to ensure the possibility to stop data processing for direct marketing purposes in the same form as the direct marketing is conducted, and/or to determine the available and adequate means to require discontinuation of data processing for direct marketing purposes.	
Comment – Opt-out option from direct marketing Pursuant to the ePrivacy Directive the subscribers need to be provided with an option to opt-out from direct marketing communication at any time. The PDPA is in this respect aligned with the ePrivacy Directive. No gap was identified and no action is required.				
Art 13/4	In any event, the practice of sending electronic mail for the purposes of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, which contravene Article 6 of Directive 2000/31/EC [*information to be provided to consumers*	Art 8/6 PDPA	When data are processed for direct marketing purposes a data controller shall be obliged to notify a data subject of the right under paragraph 4 of this article and to ensure the possibility to stop data processing for direct marketing purposes **in the same form as the direct marketing is conducted, and/or to**	

	under eCommerce Directive], which do not have a valid address to which the recipient may send a request that such communications cease or which encourage recipients to visit websites that contravene that Article shall be prohibited.		**determine the available and adequate means to require discontinuation of data processing for direct marketing purposes**.	

Gap 23 – Cease of use of electronic mail for direct marketing

The PDPA contains general obligations with regard to adequate and available (affordable) means to stop processing of data subjects' data for direct marketing purposes. The specific obligation that a valid address for ceasing the marketing emails should be included in the applicable law.

The PDPA does not impose specific obligations to inform the recipients of marketing emails of the identity of the sender (or of the seller on whose behalf the marketing emails are sent). Such obligation should be implemented in the applicable law.

Action plan

Legislation:	/
Section:	/
Proposed change:	/

Notes:	The current level of use of personal data (including electronic contact) for direct marketing purposes under the ePrivacy Directive is likely to be reassessed in view of the GDPR. It is therefore advisable to wait with the implementation of the obligations related to location data until the updated legislative proposal on the ePrivacy Directive is adopted. Further, the Georgian PDPA is currently under review and will most likely include the regulation of unsolicited communications, too.			
Art 13/5	Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.	Art 2/f PDPA	data subject – any natural person whose data is being processed	
		Art 8/6 PDPA	When data are processed for direct marketing purposes a data **controller shall be obliged to notify a data subject of the right under paragraph 4 of this article and to ensure the possibility to stop data processing for direct marketing purposes in the same form** as the direct marketing is conducted, and/or to determine the available and adequate means to require discontinuation of data processing for direct marketing purposes.	
Gap 23 – Protection of natural and legal persons Since direct marketing regulation is included in the PDPA, all related issues are covered by data processing provisions, i.e. the provisions protecting natural persons. The criteria of the ePrivacy Directive are thus met in this respect. As the provisions in the PDPA on direct marketing apply only to natural persons, there is a gap related to the absence of any statutory provisions stipulating the adequate protection and/or ensuring the legitimate interests of the subscribers other than natural persons. We therefore recommend that protection against unsolicited communication is extended also to subscribers other than natural persons (entities), by implementing the relevant provisions in Georgian laws (e.g. ECA).				
Action plan **Legislation:** / **Section:** /				

Proposed change:	/			
Notes:	The current level of use of personal data (including electronic mail) for direct marketing purposes under the ePrivacy Directive is likely to be reassessed in view of the GDPR. It is therefore advisable to wait with the implementation of the obligations related to location data until the updated legislative proposal on the ePrivacy Directive is adopted. Further, the Georgian PDPA is currently under review and will most likely include the regulation of unsolicited communications, too.			
Art 13/6	Without prejudice to any administrative remedy for which provision may be made, inter alia, under Article 15a(2), **Member States shall ensure that any natural or legal person adversely affected by infringements of national provisions adopted pursuant to this Article and therefore having a legitimate interest in the cessation or prohibition of such infringements**, including an electronic communications service provider protecting its legitimate business interests, **may bring legal proceedings in respect of such infringements**. Member States may also lay down specific rules on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of national provisions adopted pursuant to this Article.	N/A		
Gap 24 – Legal proceedings regarding infringements Neither PDPA nor the ECA specifically provide for the right to bring legal proceedings in respect of infringements. However, we have not been provided with any civil laws which, presumably, may address this.				
Action plan				

Legislation:	/
Section:	/
Proposed change:	/
Notes:	The current level of use of personal data for direct marketing purposes (including all related rights and obligations) under the ePrivacy Directive is likely to be reassessed in view of the GDPR. It is therefore advisable to wait with the implementation of the obligations related to location data until the updated legislative proposal on the ePrivacy Directive is adopted. Further, the Georgian PDPA is currently under review and will most likely include the regulation of unsolicited communications, too.

K Technical features and standardisation

	ePrivacy Directive		Georgian Legislation	Gap
Art 14	1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs 2 and 3, that no mandatory requirements for specific technical features are imposed on terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States. 2. Where provisions of this Directive can be implemented only by requiring specific technical features in electronic communications networks, Member States shall inform the Commission in accordance with the procedure provided for by Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services. 3. Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications.	Art 58 ECA	1. The list of the European harmonised standards applicable in the field of electronic communications shall be approved by the Government of Georgia. 2. Radio equipment and telecommunication terminal equipment shall conform to the basic requirements defined by the Regulations on Certifying Radio Equipment and Telecommunication Terminal Equipment.	
		Art 59 ECA	1. Radio equipment and telecommunication terminal equipment shall be certified in accordance with the Regulations on Certifying Radio Equipment and Telecommunication Terminal Equipment approved by the Commission. 2. Radio equipment and telecommunication terminal equipment shall be certified by testing centres and laboratories which are accredited by the National Agency for Standardisation, Metrology and Certification of Georgia upon the recommendation of the Commission. If an accredited testing centre (laboratory) violates the relevant normative acts, the accreditation shall be revoked upon the recommendation of the Commission. 3. Radio equipment and telecommunication terminal equipment shall be certified in accordance with the relevant technical standards.	

Gap 25 – Technical features and standardisation

In the law reviewed no such mandatory requirements on technical features were identified. We cannot assess whether they are included in other laws or technical standards applicable to manufacturers. A review of these is recommended and if such mandatory requirements are identified they should be (preferably) removed or otherwise addressed.

Recital 46 of the ePrivacy Directive stipulates that the functionalities for the provision of electronic communications services may be integrated in the network or in any part of the terminal equipment of the user, including the software. The protection of the personal data and the privacy of the user of publicly available electronic communications services should be independent of the configuration of the various components necessary to provide the service and of the distribution of the necessary functionalities between these components. Therefore, the existence of specific rules for electronic communications services alongside general rules for data protection for other components necessary for the provision of such services may not facilitate the protection of personal data and privacy in a technologically neutral way. It may thus be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected.

Action plan	
Legislation:	/
Section:	/
Proposed change:	/
Notes:	There is currently a new bill to be enacted in Georgia which should ensure rights and obligations related to technical features and standardisation. The GNCC will ensure that the bill is compliant with the requirements of the ePrivacy Directive.

L Final provisions

	ePrivacy Directive		Georgian Legislation	Gap
Art 15a/1	Member States shall lay down the rules on penalties, including criminal sanctions where appropriate, applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive and may be applied to cover the period of any breach, even where the breach has subsequently been rectified. The Member States shall notify those provisions to the Commission by 25 May 2011, and shall notify it without delay of any subsequent amendment affecting them.	Art 45 ECA	If a person fails to comply with the legislation of Georgia in the field of electronic communications, including with the resolutions and decisions of the Commission and/or if a license holder fails to observe the licence conditions, the Commission may warn the violator in writing, and in the case of failure to eliminate a continuous violation within the time limit specified by the Commission, or in the case of the commission of a new single infringement within a year, the Commission may impose a fine in the amount of 0.5 per cent of the of the last 12 months' income of the authorised person (total income without VAT as determined by the Tax Code of Georgia), but the amount shall not be less than GEL 3 000 nor more than GEL 30 000.	
Comment – Sanctions The ECA provides for general sanctions for any breach of the obligations stipulated therein. Since the ePrivacy Directive will be implemented into a new chapter of the ECA, these obligations will also be subject to general sanctions under the ECA. No further action is therefore required. We have not reviewed any criminal sanctions which we understand would be governed by specific criminal law, which is out of the scope of our review.				
Art 15a/2	Without prejudice to any judicial remedy which might be available, Member States shall ensure that the competent national authority and, where relevant, other national bodies have the power to order the cessation of the infringements referred to in paragraph 1.	Art 39/1 PDPA	If the Inspector detects a violation of this Law or other normative acts that regulate data processing, he/she shall be authorised to: a) **require elimination of the violation** and the deficiencies related to data processing in the form and within the period indicated by him/her;	

Comment [PIERSTONE1]: Of ECA?

			b) require temporary or permanent termination of data processing if measures and procedures applied by a data controller or a data processor for data protection fail to comply with the statutory requirements; c) require termination of data processing, their blocking, deletion, destruction or depersonalisation if he/she believes that the data processing is conducted unlawfully; d) require termination of data transfer to other states and international organisations if they are transferred in violation of the requirements of this Law;	
Art 15a/3	Member States shall ensure that the competent national authority and, where relevant, other national bodies have the necessary investigative powers and resources, including the power to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to this Directive.	Art 27 - 40 PDPA	*The enforcement of the PDPA is generally granted to the Inspector governed under the Chapter V – The Personal Data Protection Inspector.*	
Comment – Competent authority According to the PDPA, the Inspector is entitled to require elimination of the violation, which is aligned with the requirements of the ePrivacy Directive. The Inspector is also empowered to conduct audits on premises and in this respect the requirements of the ePrivacy Directive are fulfilled. No gap was identified.				
Art. 15a/4	The relevant national regulatory authorities may adopt measures to ensure effective cross-border cooperation in the enforcement of the national laws adopted pursuant to this Directive and to create harmonised conditions for the provision of services involving cross-border data flows. The national regulatory authorities shall provide the			

	Commission, in good time before adopting any such measures, with a summary of the grounds for action, the envisaged measures and the proposed course of action. The Commission may, having examined such information and consulted ENISA and the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC, make comments or recommendations thereupon, in particular to ensure that the envisaged measures do not adversely affect the functioning of the internal market. National regulatory authorities shall take the utmost account of the Commission's comments or recommendations when deciding on the measures.'			

This document has been prepared in connection with the project "**Georgia - Information Communication Technology Sector Development**" financed by the **European Bank for Reconstruction and Development**. Any legal advice contained in this document has been provided under the EU law. Georgian legislation has been taken into account based on the English translations provided to us by GNCC. We are not qualified to provide legal advice under Georgian law.

This document has been prepared by the following consultants:

Grant Thornton Advisory s.r.o., Bratislava, Krížkova 9, 811 04, registered in the Company Register held with the District Court in Bratislava I, Insert 44639/B, ID number 367 39 715.

PIERSTONE s.r.o., advokátní kancelář, organizačná zložka, Dvořákovo nábrežie 4, Bratislava, 811 02, ID number: 505 83 123, registered in the Company Register held with the District Court in Bratislava I, Insert 3641/B. PIERSTONE is an international alliance of lawyers registered by the Brussels Bar Association.

Analysys Mason Limited, Bush House, Aldwych, London, England, WC2B 4PJ, Company number 05177472.