MEMORANDUM

on the

DRAFT LAW OF GEORGIA ON PROTECTION OF PERSONAL DATA

by

ARTICLE 19
Global Campaign for Free Expression

London
February 2004

I. Introduction

This Memorandum analyses the draft Law of Georgia on Protection of Personal Data (the draft Law) against international standards on freedom of expression and information.[1]

The draft Law is an important part of the on-going drive to open up public bodies to greater scrutiny, which would result in enhanced openness and transparency in public life. Equally important, an effective data protection law would also contribute to the regime of protection for the right to information by granting individuals the right to demand to be told what information is held on them by both public and private bodies.

ARTICLE 19 welcomes efforts to introduce measures to ensure effective access to personal information but we believe that the version of the draft Law received by us is flawed and would endanger the right of the media freely to gather information and report on critical issues. In particular, pursuant to the draft Law, anyone has the right to approach journalists and media organisations to demand access to personal data used to research a story, even an unpublished one. This would seriously hinder the ability of

[1] We have received an unofficial translation of the draft Law through the Liberty Institute in Georgia. ARTICLE 19 takes no responsibility for the accuracy of the translation or for comments based on mistaken or misleading translation.

journalists to do their jobs, for example by enabling public figures to 'harass' journalists who are investigating a potential corruption story. It would also have important implications for the protection of confidential sources, a key issue in investigative journalism. Not only does the draft Law introduce the problem noted above, but it also fails effectively to enhance transparency of several crucial public bodies. The police will be largely outside the remit of the draft Law and the transparency provisions of draft Law itself will be subject to the far stricter application of the Law on State Secrets. The draft Law also fails, in our view, to establish an effective mechanism for implementation and oversight.

This Memorandum aims to inform further discussion around the draft Law by examining it against international standards on freedom of expression and information. Its focus is on how the draft Law will impact on the exercise of the right to freedom of expression in general and the work of the media in particular. Suggestions and recommendations will be provided throughout.

II. International and Constitutional Obligations

II.1 Freedom of Expression

Article 19 of the *Universal Declaration on Human Rights* (UDHR),[2] a United Nations General Assembly Resolution, guarantees the right to freedom of expression and information in the following terms:

> Everyone has the right to freedom of opinion and expression; this right includes the right to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

The *International Covenant on Civil and Political Rights* (ICCPR),[3] a legally binding treaty to which Georgia acceded in 1994,[4] guarantees the right to freedom of opinion and expression in very similar terms to the UDHR, also in Article 19. A Council of Europe Member State since 1999, Georgia is also a party to the *European Convention on Human Rights*,[5] which guarantees freedom of expression at Article 10.

Article 19 of the Constitution of Georgia protects the right to freedom of expression in the following terms:

> 1. Every individual has the right to freedom of speech, thought, conscience, religion and belief.
> 2. The persecution of an individual for his thoughts, beliefs or religion is prohibited as is compulsion to express opinions about them.

Article 24 of the Constitution provides:

[2] UN General Assembly Resolution 217A(III), adopted 10 December 1948.
[3] UN General Assembly Resolution 2200A(XXI) of 16 December 1966, in force 23 March 1976.
[4] 3 May 1994.
[5] Adopted 4 November 1950, in force 3 September 1953.

> 1. Every individual has the right to freely receive and disseminate information, to express and disseminate his opinion orally, in writing or in any other form.

The particular importance of freedom of expression in a democratic society has been stressed many times by international human rights courts. For example, the European Court of Human Rights has stated, in a quotation which now features in almost all its judgments involving freedom of expression:

> [F]reedom of expression constitutes one of the essential foundations of [a democratic] society, one of the basic conditions for its progress and for the development of every man.[6]

Freedom of information is an important component of the international guarantee of freedom of expression, which includes the right to seek and receive, as well as to impart, information and ideas. There can be little doubt as to the importance of freedom of information. During its first session in 1946, the United Nations General Assembly adopted Resolution 59(1) which stated:

> Freedom of information is a fundamental human right and… the touchstone of all the freedoms to which the UN is consecrated.[7]

As this Resolution notes, freedom of information is both fundamentally important in its own right and is also key to the fulfilment of all other rights. It is only in societies where the free flow of information and ideas is permitted that democracy can flourish. In addition, freedom of expression and information is essential if violations of human rights are to be exposed and challenged.

Basic standards on freedom of information are laid down in the Council of Europe's Recommendation 2002(2), which provides that States should "guarantee the right of everyone to have access, on request, to official documents held by public authorities."[8] Restrictions on this right should be set out in law and be limited to those which are strictly necessary to achieve a number of listed aims. The 'harm test' outlined in the Recommendation is crucial, requiring that government agencies refusing to disclose certain information must show that disclosure of the information will, in the particular case, cause substantial harm to a protected interest.[9] In addition, the Recommendation requires States to disclose information, even if it can be shown that such disclosure poses a serious risk of harm, whenever the public interest in disclosure outweighs that harm.[10] For example, certain information may be private in nature but at the same time expose high-level corruption within government. In such cases, the benefit in having the information disclosed will normally outweigh the harm done to the private interests of the official concerned. This test implies that every request for access has to be judged on an

[6] *Handyside v. United Kingdom*, 7 December 1976, Application No. 5493/72, para. 49.
[7] 14 December 1946.
[8] Recommendation Rec(2002)2 of the Committee of Ministers to member states on access to official documents, 21 February 2002.
[9] Principle 4.
[10] Principle 4.

individual basis and that a blanket-rule limiting access to an entire class of information cannot be justified.

II.2 Access to Personal Information

The right to access personal information is a right that straddles both the right to freedom of expression and information protected under Articles 10 of the ECHR and Article 19 of ICCPR, and the right to privacy and 'data protection', protected under Article 8 of the ECHR and Article 17 of the ICCPR.[11] Elaborating the general guarantee of respect for privacy found in Article 17 of the ICCPR, the UN Human Rights Committee has stated:

> The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorises or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[12]

Specific instruments regulating the collection and use of personal data were developed by inter-governmental organisations in the 1970s and 1980s. This development arose from a concern that increasing amounts of personal information were stored in databanks, by government organisations as well as by private corporations, and that individuals had a right to know exactly what personal information regarding them was being collected and how it was used.[13] As such, 'data protection' guarantees can be seen as a subset of more generic measures to protect the right to access information, although international data protection laws both cast a wider net – including all private as well as public bodies that process personal data within their scope – but may also act as a restriction on the general right of access – by limiting the access of third parties to personal information. Together with the specific issues that arise from data processing, this has led to somewhat different standards being applied to both processing and accessing personal data, compared to non-personal data.

In the European context, specific standards on 'data protection' have been laid down in the Council of Europe Convention for the Protection of Individuals with regard to Automatic

---

[11] Article 8 of the ECHR protects the right to respect for private and family life, the home and correspondence.

[12] General Comment No. 16, adopted 8 April 1988, para. 10.

[13] Key among these are the Organisation for Economic Co-operation and Development's 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data', adopted 23 September 1980: <http://www.oecd.org/>; two Resolutions of the Committee of Minister of the Council of Europe, namely (73)22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector, adopted 26 September 1973, and Resolution (74)29 on the protection of individuals vis-à-vis electronic data banks in the public sector, adopted 20 September 1974; and the Council of Europe Data Protection Convention, adopted 28 January 1981, E.T.S No. 108, in force 1 October 1985.

Processing of Personal Data[14] (the CoE Convention) and the European Union's Data Protection Directive[15] (the EU Directive). While Georgia is not at present a European Union Member State, it has repeatedly stated its desire to become one;[16] it follows that the EU Directive sets an aspirational standard for Georgia. Both instruments elaborate on the 'privacy' aspect of the right to have access to personal information. While the former applies only to data processing in automated systems, the EU Directive applies to all data processing, whether automated or not.[17] Both apply to data processing in the public as well as in the private sector.[18]

The CoE Convention and the EU Directive both state a number of basic 'data protection principles', requiring that data should be obtained and processed fairly and lawfully; be stored for specified and legitimate purposes and not used in a way incompatible with those purposes; be adequate, relevant and not excessive to those purposes; and be accurate.[19] Both instruments provide that the 'data subject' – the person whose information is being collected, held or processed – has the following rights:

- to be informed whether data relating to him or her is being processed and by whom;
- to be given information as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data is disclosed;
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source;
- rectification, erasure or blocking of inaccurate or incomplete data, and the notification of third parties to whom the data may have been communicated.[20]

It should be noted that the list of legitimate aims in pursuit of which access to personal data can be restricted is more limited under the data protection instruments than under the more generic access to information standards. The CoE Convention states that access may be restricted only,

> …when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:
>
> a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;
>
> b. protecting the data subject or the rights and freedoms of others.

[14] Note 13. This has been signed by Georgia, on 21 November 2001, but not yet ratified.
[15] Directive 95/46/EC, OJ L281, 23 November 1995, p. 31.
[16] For example, as reported by the BBC on 24 November 2003: <http://news.bbc.co.uk/1/hi/world/europe/3232158.stm>
[17] The only condition is that the data must "form part of a filing system or are intended to form part of a filing system". EU Directive, Article 3.
[18] For EU constitutional reasons the Directive does not apply to data processing operations relating to public security, defence, State security and the activities of the State in the field of criminal law (see Article 3 of the EU Directive) because in 1995, those areas fell outside the remit of the European Community bodies that adopted the Directive. The CoE Convention, signed by Georgia, contains no such exceptions.
[19] CoE Convention, Article 5 and EU Directive, Article 6.
[20] EU Directive, Articles 10, 11, 12 and CoE Convention, Article 8.

The right to have access to one's personal data also receives protection in the Georgian Constitution. Article 41 states:

> 1. Every citizen has the right, according to the law, to know information about himself which exists in state institutions as well as official records existing there, except for information containing state, professional or commercial secrets.
> 2. Information existing in official papers connected with health, finances or other private matters of an individual are not available to other individuals without the prior consent of the affected individual, except in cases determined by law, when it is necessary for the state and public security, defence of health, rights and freedoms of others.

It is important to note that the European Court of Human Rights has stressed that even if information falls within one of the above categories, any refusal constitutes a prima facie violation of the right of access which would need to be justified.[21] As is the case under the access to information regimes required under CoE Recommendation 2000(2), information can be withheld only when disclosure will actually 'harm' a protected interest and there is no overriding public interest that would justify disclosure.

Finally, the European Court of Human Rights has stated that independent systems have to be in place to oversee the implementation of the legal framework for access to information, and individuals must have access to an independent tribunal or court in order to challenge access refusals.[22] The EU Directive establishes a similar requirement[23] and within the framework of the CoE Convention, a special Protocol has been drawn up regarding this matter.[24] The latter has not yet entered into force.

III. Analysis of the draft Data Protection Law

III.1 Overview

The draft Law protects individuals' privacy in the processing of personal data by defining a number of "general principles of personal data processing", such as that personal data shall be processed lawfully and fairly, and that only relevant and accurate data shall be processed. The 'data subject' is given a number of rights, including, in principle, a right to be informed that data about him/her is being processed and a right to access that data. The draft Law applies to data processing by any person, legal entity or administrative organ, subject to the operation of the Law on State Secrets, as well as to general exceptions for data held in relation to criminal investigations or prosecutions.

Although the 'data protection principles' outlined in the international treaties discussed above find some recognition in the draft Law, there are a number of important oversights. In particular, the exceptions relating to State secrets and data processing in the context of

[21] *See* the Court's reasoning in *Gaskin v. the United Kingdom*, 7 July 1989, Application No. 10454/83, para. 49.
[22] *Ibid.*
[23] EU Directive, Article 28.
[24] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, CETS No. 181, opened for signature on 8 November 2001, not yet in force. This has not yet been signed by Georgia.

criminal investigations and proceedings would limit significantly the operational scope of the law. At the same time, an exception should be added to ensure that the media are not unduly fettered in their work by the data access provisions. The draft Law also fails to provide for a satisfactory supervisory body. The following sections elaborate these and other concerns in further detail.

III.2 Scope of the Draft Law

Article 2 of the draft Law provides that the law applies to "processing of personal data by any means including automatic means by a natural person, a legal entity or an administrative authority." Article 2(2) states three exceptions to this general principle:

1. the processing of personal data by a natural person for the purposes of personal, family or household affairs;
2. activities related to criminal prosecution of a person who has committed a crime, conducting criminal proceedings as well as operational investigation activities; and
3. matters regulated by the Law of Georgia "On State Secrets".

The first exception, relating to data processing for personal or household purposes, is uncontroversial. Exceptions such as this are found in all data protection laws and have the aim of exempting people's personal address books, for example, from being subject to data protection law.

The second and third exceptions, however, are more problematic. Both are framed as class exceptions, meaning that the draft Law will not apply to any data that falls in one of the relevant categories. No harm test is required and there is no provision for a public interest override. With regard to the second exception, protecting data processed in relation to criminal investigations, this would allow police or judicial authorities to shield serious wrong-doing within their departments. This is contrary not only to international standards, inasmuch as it fails to incorporate a harm test or public interest override. It also appears, on its face, to be contrary to the right to access personal information under Article 41 of the Constitution, which allows only for non-disclosure of "information containing state, professional or commercial secrets".[25]

The third exception effectively subjects the operation of the draft Law to the 1996 Law on State Secrets.[26] This Law defines as a 'state secret', "a kind of information that includes data containing a state secret in the areas of defense, economy, external relations, intelligence service, state security and protection of law and order disclosure or loss of which may inflict harm on the sovereignty, constitutional framework or political and economic interests of Georgia."[27] An exception is provided that restricts the classification as 'secret' of any information that "may prejudice or restrict basic human

[25] Article 41(2).
[26] 1996 Law of Georgia on State Secrets, as amended by Law No. 1276 of 4 March 1998 and Law No. 1853 of 19 March 1999.
[27] Article 1.

rights and freedoms or may cause harm to health and safety of population"[28] as well as information falling within one of the following categories:

a) information on natural disasters, catastrophes and other "extraordinary events" which have already occurred or may occur and which threaten the safety of citizens;
b) information on environmental conditions, health and living standards of the population, including information on medical services and social security, as well as social-demographic data and data on educational and cultural levels of the population.
c) information on corruption, unlawful action by officials and crime statistics;
d) information on privileges, compensations and benefits provided by the exception to citizens, officials, enterprises, institutions and organizations;
e) information on the exception monetary fund and national gold reserve; and
f) information relating to the health of "top officials of the state power".[29]

The regime established under the 1996 Law on State Secrets is problematic primarily because of the extremely broad range of material caught by the definition of 'state secret'. Despite the public interest exemptions provided in Article 8, the formulation as exception secret of any material relating to, for example, the economic situation of the country whose disclosure 'may' cause harm would capture a wide range of materials, and is contrary to international standard according to which disclosure may be refused only where there is a serious likelihood of real harm and the overall public interest is served by non-disclosure. By subjecting the draft Law on Personal Data to the Law on State Secrets, an unnecessarily broad range of material has been withdrawn from the scope of the draft Law.

Furthermore, this wholesale exception is not restricted to the question of access to information but means that all of the 'data protection principles' set out in Article 4 of the draft Law do not apply. For example, these principles provide that personal data should be obtained lawfully. The draft Law proposes that this would not be imposed where the information is collected as part of intelligence-gathering activities or criminal investigations. There is no apparent justification for this.

We also note that the draft Law does not specify its relationship with the existing regime for access to information held by public bodies, established under Chapter 3 of the General Administrative Code.[30] This means that individuals seeking to access personal data held by a government institution falling under that regime would have a choice of two procedures, which is likely to result in confusion. This should be addressed. It would be preferable to establish an integrated access procedure for all information held by public bodies. The operation of this regime should not be subject to the 1996 Law on State Secrets or any other more restrictive legal regime.

Recommendations:

[28] Article 8.
[29] *Ibid.*
[30] We shall not comment on the merits of that regime in this analysis.

- A unified access regime should be set up for all information held by public bodies.
- Exceptions to the principle of access to personal information should be allowed only in pursuit of those legitimate aims mentioned in the constitution and in international instruments.
- Exceptions should not be formulated as class exemptions, but should require the body seeking to deny disclosure to show that disclosure would cause harm to a legitimate protected interest and would not be in the overall public interest.

III.3 Data Protection and Freedom of Expression

Under Article 9 of the EU Directive, EU Member States are required to "provide for exemptions or derogations" from a number of the data protection principles to bring data protection law into line with the requirements posed by the right to freedom of expression. Article 9 makes it clear that such exceptions should apply to all data processing "for journalistic purposes or [for] the purpose of artistic or literary expression."[31] Without these exceptions, journalists would have to notify an individual as soon as they begin investigating a story relating to them and grant subjects of their stories access to any personal information held. Moreover, that person could object and block any subsequent publication. This would render investigative journalism impossible.

In a 2003 study, the European Commission found that although practical implementation of the principle stated in the EU Directive differed from country to country, all EU Member States recognised that special provisions are needed to reconcile data protection rights with the right to freedom of expression.[32] It found that Denmark, Finland and Sweden exempted the media from the data protection law altogether, with the Swedish Supreme Court stressing that the exception should apply not just to journalists but to all cases in which data is being processed in the exercise of the right to freedom of expression.[33] In other countries – for example, the United Kingdom, Netherlands and Portugal – the media have been exempted from specific provisions in the data protection law, such as those relating to the obligation to inform the data subject and to allow subject access.

The draft Law fails to provide this key exception for the media, or to reconcile data protection principles and the right to freedom of expression more generally. The only exception it does provides is: "In case of personal data processing for the scientific, statistical or artistic purposes, a person responsible for processing shall be free from the obligation of informing the data subject if informing of the data subject is impossible or causes unreasonably high expenses." This fails to recognise the need noted above in a number of ways. It is vague – what constitutes an "unreasonably high expense?" –, applies only to scientific, statistical or artistic expression and does not recognise that there are other interests than financial ones to be protected, namely freedom of

[31] The CoE Convention provides for a similar exception in Article 9(2)(b), as elaborated in the Council of Europe's 1991 Explanatory Report on Convention 108/81.
[32] *Analysis and impact study on the implementation of Directive EC 95/46 in Member States*, European Commission, 16 May 2003, pp. 17-19. Available at <http://europa.eu.int/>.
[33] Case B 293-00, Judgment of 12 June 2001.

expression. As such, it falls far short of the general exception called for under the EU Directive to reconcile freedom of expression and the right to privacy.

Recommendation:
- The draft Law should exempt all data processing that takes place incidental to the exercise of the right to freedom of expression.

III.4 Oversight and Supervision

The draft Law envisages that all supervisory functions should be exercised jointly by the Public Defender (the Georgian Ombudsman) and the State Department of Informatization. Article 25 of the draft Law provides: "The State Department of Informatization of Georgia shall … supervise the observance of the requirements of the present Law…" Article 28 provides: "The Public Defender of Georgia shall … supervise on the territory of Georgia the protection of inviolability of a natural person's private life while processing his personal data, reveal facts of violation of this right and promote restoration of the violated rights." Pursuant to Article 28(1)-(4), the Public Defender appears to have primary responsibility for the investigation of apparent violations of the draft Law, while the State Department of Informatization will be primarily responsible for the enforcement of the Public Defender's findings.

The EU Directive, as well as an additional Protocol to the CoE Convention, requires States to set up independent authorities to supervise the implementation of data protection law.[34] Article 28 of the EU Directive states: "Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive … These authorities shall act with complete independence in exercising the functions entrusted to them."

While the appointment of the Public Defender to conduct investigations into alleged violations of the law is uncontroversial, the role of the State Department of Informatization is highly problematic. As a government department, it cannot be said to be able to act "with complete independence", as required by the EU Directive, particularly with regard to personal data held by other government departments. As a recent report by the European Commission makes clear: "The establishment of independent supervisory authorities is an essential component of the protection of individuals with regard to the processing of personal data."[35] The report goes on to detail the status of the supervisory authorities in each of the EU Member States, finding that all except for one have established independent supervisory authorities separate from any organs of the executive arm of the exception. Only in Germany do State ministries exercise control over data processing, but their role is limited to supervision of data processing by private controllers: public authorities all fall under the control of an independent supervisory authority.[36]

[34] EU Directive, note 15, Article 28; Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, note 24.
[35] Commission report, note 32, p. 37.
[36] *Ibid*.

Recommendation:

- All supervisory functions must be established in an independent supervisory authority, such as the Public Defender.

III.5 Registration of Data Controllers

The draft Law requires everyone who intends to process information that falls within the scope of the draft Law to obtain government authorisation. Article 16 of the draft Law states: "Before processing of personal data, a person responsible for processing shall apply to the State Department of Informatization of Georgia for obtaining a permit to the processing." In order to obtain a permit, prospective data processors should lodge an application with the Department detailing the kind of information they intend to process, upon receipt of which the Department will make a decision within three days. Permits may be refused if the application does not comply with the formal requirements set out in the draft Law or if a previous permit for that same applicant has been annulled and the grounds for annulment have not been addressed by the applicant. Refusals to provide a permit may be appealed to a court.

The system envisaged by the draft Law cannot be considered to be in compliance with the standard set by the EU Data Protection Directive or the CoE Convention. The EU Directive only requires data processors to 'notify' an independent supervisory authority of data processing activities; no prior approval is necessary.[37] The regime by the draft Law would subject all data processing to State approval, which could have serious implications for political organisations, for example, who would hold a database of their membership or supporters. Despite the relatively strict criteria for refusals, this would still impose an unacceptable degree of government control. It should be noted that the EU Directive exempts certain bodies, such as human rights organisations who only run a membership database, from the notification requirement.[38]

We are also concerned about Article 26 of the draft Law, which authorises the State Department of Informatization to "create and keep national banks of personal data in accordance with the rules established by a decree of the President of Georgia." We assume that this relates to a national register of data controllers, a file showing all the organisations in Georgia who have notified the relevant supervisory body of data processing and detailing the kind of data processed by them.[39] If so, the wording of the draft Law must be amended to make this clear. However, if Article 26 of the draft Law is to be understood as allowing the Department to run a kind of amalgamated database of all the data being processed nationwide that falls within the ambit of draft Law, or if it allows the Department to set up some sort of open-ended national database of personal information, then it would be a potentially serious violation of the right to respect for private life protected under Article 8 of the ECHR. The European Court of Human Rights has made it clear that personal data processing by public authorities is lawful only when

[37] EU Directive, note 15, Article 18.
[38] *Ibid*.
[39] Such registers are routinely kept by data protection supervisory authorities in Europe. For an example of such as register, see <http://forms.informationcommissioner.gov.uk/search.html>.

authorised specifically by law and where guarantees are in place to prevent abuse.[40] Article 26 of the draft Law, if understood to authorise generic and unlimited personal data processing by a public authority, signally fails to meet these conditions.

Recommendations:

- Data processors should not require prior approval in order to begin data processing operations. A requirement to notify, which should be limited to categories of data controllers whose actions would be likely adversely to affect the rights of their data subjects, is sufficient.
- Article 26 should be amended to clarify that it requires the independent supervisory authority to maintain a database of data controllers.

[40] See, for example, *Amann v. Switzerland*, 16 February 2000, Application No. 27798/95 (European Court of Human Rights).