RoAid
ROMANIA'S DEVELOPMENT COOPERATION PROGRAMME

MINISTRY OF FOREIGN AFFAIRS

CENTRUL ROMÂN DE POLITICI EUROPENE
CRPE
DEBATING EUROPE
PROVIDING EXPERTISE

OPEN SOCIETY GEORGIA FOUNDATION
ფონდი ღია საზოგადოება საქართველო

UNDP
Empowered lives.
Resilient nations.

Personal data protection in Georgia and the dialogue on Visa Liberalization with the EU

CRPE Policy Memo, April 2015
Author: Bogdan Manolea, Affiliated expert,
Romanian Center for European Policies

Table of Contents

1. General overview on privacy and personal data in Georgia

The subject of privacy and, consequently, of personal data protection is gaining more importance with the increase of use of technologies in everyday life and especially its extensive use for data processing – both by private and public sector.

The subject of the personal data protection1 in Georgia has received considerable public attention in the past 3 years, following internal and external-triggered events: the illegal wiretappings and video scandals following the 2012 parliamentary elections and, more recently, the data protection issues in the context of the perspective of the dialogue on visa liberalization between Georgia and the European Union (EU).

This situation has spurred a long series of debates in Georgia on the privacy regulation and its implementation in practice – both in media and in the political arena. That is in fact a very good basis for having a comprehensive data protection regime in place.

A lot of essential steps forward have been made within a rather short period of time– especially if we are comparing what exists today with the situation before 2012 –a much clearer legislation of wire tapping and a legal framework on personal data protection, including the creation of an independent authority for personal data protection (Office of the Personal Data Protection Inspector, called thereafter the Data Protection Authority or DPA).

However, there are still several major shortcomings in having a fully functional privacy and data protection regime in Georgia – with some of them unlikely to be solved in the next years. It seems doubtful that there is a real political will on taking into account the recommendations for improvements in regard to sensitive subjects, already made on several occasions. The public debates and legal changes that took part towards the end of November 2014[2] on the new wiretapping legal provisions are an example in this sense.

---

1. For more details on principles of privacy and data protection we suggest reading this handbook on European data protection law (04.2014)
http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf
2. See “Parliament Overrides Veto on Govt-Backed Surveillance Bill” (30.10.2014)
http://www.civil.ge/eng/article.php?id=27866

But the Georgian experience needs to be seen in a wider European and international privacy context, constantly challenged in the past years by revelations on major state level privacy intrusions and big Internet companies from the private sector using widespread personal data collection in conditions that are challenged by the EU data protection authorities[3]. The context is somehow complicated by the revisions of the EU data processing legal regime that is taking much longer than expected, with significant differences between EU Member States' positions.

Therefore the current report needs to be read in the specific context of our interviews from November 2014 and the legislation applicable in March 2015, especially on the possible new changes to the national and international legislation.

We would like to take this opportunity and thank all the representatives of public and private institutions that were kind enough to answer our interview questions during our study trip to Tbilisi in November 2014: I Office of the Personal Data Protection Inspector, Tamar Kordzaia, Member of the Parliament, Ministry of Justice and Public Service Development Agency., Identoba, Transparency International Georgia, Georgian Young Lawyers' Association, Open Society Georgia Foundation.

2. The current legislative, institutional and implementation situation in Georgia

2.1. Georgian Constitution

The Constitution of Georgia[4] includes several articles that affirm the right to privacy and to personal development:

- art 16 on the free development of personality[5]
- art. 20 on the private life[6]

3. See the recent report commissioned by the Belgian Data Protection Authority on Facebok's privacy policies - http://www.law.kuleuven.be/icri/en/news/item/icri-cir-advises-belgian-privacy-commission-in-facebook-investigation or Dutch Data protection authority incremental fines to Google https://cbpweb.nl/en/news/cbp-issues-sanction-google-infringements-privacy-policy
4. Text available in English at http://www.wipo.int/wipolex/en/text.jsp?file_id=194553 (all websites were last time visited on 2 April 2015)
5. Entire text of art 16: "Everyone has the right to free development of his/her personality."
6. Full text of Article 20 par 1: "Everyone's private life, place of personal activity, personal records,

– art 41 on the processing of personal data by the State institutions[7]

There is also some constitutional jurisprudence regarding the right to privacy, as foreseen in the articles 16, 20 and 41.

One specific ruling from 2008[8] shows that its constitutional jurisprudence is consistent with the European Court of Human Rights practice in acknowledging the essence of the right to privacy: "One of the essential aspects of the right to privacy is the interest of a person not to allow the disclosure of the information concerning private matters and to control the dissemination of such information." [9]

Other cases ruled by the Georgian Constitutional Court had a more detailed approach with regards to the sphere of private life in case of video-recordings in a public space[10] and the mandatory court approval for operative search activities[11]. In a recent case the Constitutional Court ruled that internet communication falls under Article 20.1. [12]

---

correspondence, communication by telephone or other technical means, as well as messages received through technical means shall be inviolable. Restriction of the aforementioned rights shall be permissible by a court decision or also without such decision in the case of the urgent necessity provided for by law. "

7. Full text of Art 41 1.Every citizen of Georgia shall have the right to become acquainted, in accordance with a procedure prescribed by law, with the information about him/her stored in state institutions as well as official documents existing there unless they contain state, professional or commercial secret. 2. The information existing on official papers pertaining to individual's health, his/her finances or other private matters, shall not be accessible to any one without the consent of the individual in question except in the cases determined by law, when it is necessary for ensuring the state security or public safety, for the protection of health, rights and freedoms of others.
8. Decision of the Constitutional Court of Georgia dated 30 October 2008, #2/3/406.408, in the case of the Public Defender of Georgia and the Georgian Young Lawyers' Association against the Parliament of Georgia
9. English translation of the quote available through the DPA Annual Report 1/2014 that covers the period August 2013 to March 2014, available at http://personaldata.ge/res/docs/anual%20report%28eng%29%20%284%29.pdf
10. Case Citizen of Georgia Levan Sirbiladze vs. Parliament of Georgia (Decision of the Constitutional Court of Georgia, 19 December 2008, #1/7/454)
11. Georgian Young Lawyers' Association and Citizen of Georgia Ekaterine Lomtatidze vs. Parliament of Georgia (Decision of the Constitutional Court of Georgia, 26 December 2007, #1/3/407)
12. Citizen of Georgia Tamar Chugoshvili vs. Parliament of Georgia (Decision of the Constitutional Court of Georgia, 24 October 2012, #1/2/519)

A new case lodged with the Constitutional Court by the Public Defender's Office on 30 January 2015[13] will rule on the new provisions for wiretapping: "The Public Defender believes that the right of state agencies to have uninterrupted capability to copy metadata and to receive content of communication in real time violates the right privacy, envisaged by the paragraph 1 of the article 20 of the Georgian Constitution."

13. See "Public Defender Takes Surveillance Regulation to Constitutional Court" news (3.02.2015) http://civil.ge/eng/article.php?id=28020

2.2. Aftermath of the major privacy scandal

The major privacy scandals[14] spurred in spring 2013 over secret eavesdropping and surveillance, when the Ministry of Internal Affairs publicized the information on thousands of secret audio and video recordings created in 2005-2012, the total volume of which was 260 678 megabits and the length of the recordings exceeded 1760 hours.[15]

We could identify three different areas where remedial measures were envisaged after the privacy scandals:

- On the practical level for destroying illegally tapped data and suggesting solutions for improvement, for which a Temporary Commission on Issues of Illegal Eavesdropping and Secret Recording was created and functioned [16]. While some materials were destroyed, others were sent to the Prosecutor's Office for investigation. The lack of a consensus on the final report and its conclusions[17] shows that it could be debatable if the Commission has fully met its purpose.
- On sanctions – based on administrative and/or criminal law – for investigating the people responsible for breaching the rights to privacy and personal data. However, in the end just one person was sent to court and was sentenced for 1 year suspension in prison. It is hard to believe that just one person could have been responsible for such a massive breach of privacy rights. In fact it seems there was a total lack of political will to investigate and punish (with criminal or

14. See page 21 of the GEORGIA IN TRANSITION Report on the human rights dimension: background, steps taken and remaining challenges - Thomas Hammarberg in his capacity as EU Special Adviser on Constitutional and Legal Reform and Human Rights in Georgia (Sept 2013)

    http://eeas.europa.eu/delegations/georgia/documents/virtual_library/cooperation_sectors/georgia_in_transition-hammarberg.pdf and
    Dealing with illegal surveillance material: Preliminary advice by Thomas Hammarberg (24.04.2013)
    http://transparency.ge/en/post/general-announcement/dealing-illegal-surveillance-material-preliminary-advice-thomas-hammarberg
15. DPA 2014 Annual report (fn. 9) – page 13
16. Details in DPA 2014 Annual report 2014 (fn. 9) – pag. 13
17. See Dissenting opinion of the members of temporary commission on illegal surveillance and wiretapping (14.02.2014) http://transparency.ge/en/post/general-announcement/dissenting-opinion-members-temporary-commission-illegal-surveillance

administrative sanctions) these cases. This also indicates a potential major political influence on the law enforcement process.

- On the legislative level [18]
    - in the Georgian Criminal Code, where there was a revision of articles 157-159 - Disclosure of Personal or Family Secrets (Article 157); Disclosure of Secret of Private Conversation (Article 158); Disclosure of Privacy of Personal Correspondence, Telephone Conversations or Other Messages (Article 159). It is unclear to what extent these articles were and/or will be used effectively. An analysis of the Georgian Young Lawyers Association (GYLA)[19] seems to highlight the opposite: GYLA asked the Tbilisi City Court for public information on cases of conviction under Art. 157, 158 and 159 of the Criminal Code of Georgia. Information obtained from the Tbilisi City Court shows as follows:

        a. Neither during previous nor current government (which came into power in 2012), no person was convicted under Art. 157, 158 and 159, since no charges were filed under these articles.

        b. The only exception (except for the above-mentioned case) is the 2011 verdict against a citizen (which was provided to GYLA by the Tbilisi City Court), which shows that the courts' ruling was imprisonment for 1 year and 6 months.

    - Several revisions of Data protection laws and other legislation that affected wiretapping and operational search activities were adopted in August 2014, but then changed again on 30 November 2014.[20] While it is clear that several good steps have been made forward, the changes from November 2014 show significant drawbacks in this process, by watering down important practical aspects, such as the direct access to

18. For a more detailed analysis see Chapter "Processing of Personal Data by Law Enforcement Agencies" in the DPA report published page 17 - DPA Annual Rapport made public on 17.03.2015 – available (only in Georgian) - http://personaldata.ge/res/docs/Angarishi_2014/Annual%20Reporta_2014.pdf
19. Information received during the meeting with GYLA. Website available at https://gyla.ge
20. GYLA Evaluates the State of Human Rights Protection in 2014 (10.12.2014), https://gyla.ge/eng/news?info=2371

telecommunication data for the Ministry of Interior or the Personal Data Protection Inspector capacity and attributions to control access to telecoms traffic data or Internet data. [21]

On these aspects, we may highlight that a very detailed report[22] was produced by Council of Europe's Directorate General Human Rights and Rule of Law Data Protection Unit on the draft laws of Georgia relating to surveillance activities of law enforcement authorities and national security agencies that provided significant advice on the way forward for a proper regulation that fully respects data protection in the area of law enforcement and secret services, even before the laws were considered by the Georgian Parliament. Another follow-up report was drafted in September 2014.[23]

Unfortunately, most of the key recommendations that called for a comprehensive analysis of the data protection in the field of law enforcement and secret services, as well as for specific data protection rules for these categories were ignored so far. Some of the practical and specific amendments highlighted in the report were included in the new changes of the legislation.

It is also interesting to note that while Georgia was still debating the lessons learned from the privacy scandals and how to ensure that these will not happen again, the Parliament also suggested an expansion of surveillance activities through mandatory data retention provisions for all electronic communications providers. Despite the fact that the EU data retention directive was considered invalid

21. See for info at "This Affects You – They Are Still Listening: Beselia-Popkhadze-Sesiashvili's draft is a step backwards for protection of civil liberties" (24.11.2014) https://gyla.ge/eng/news?info=2356 and "Nine threats to your personal life stemming from the new legislation on secret wiretapping" (23.12.2014) http://transparency.ge/en/blog/nine-threats-your-personal-life-stemming-new-legislation-ons-secret-wiretapping
22. Council of Europe's Directorate General Human Rights and Rule of Law Data Protection Unit on the Draft laws of Georgia relating to Surveillance Activities of Law Enforcement Authorities and National Security Agencies - Provided on the basis of the expertise by Douwe KORFF (The Netherlands), Joseph A. CANNATACI (Malta) and Graham SUTTON (United Kingdom), 14.02.2014 available at http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Expertise%20Draft%20Laws%20on%20Surveillance%20Georgia_14%2002%202014.pdf
23. Report of the Council of Europe - Key Points Regarding Access to Personal Data by Law Enforcement and by National Security Agencies, 8 September 201, Authors: Joseph A. CANNATACI and Graham SUTTON – available at http://www.civil.ge/files/files/2014/KeyPointsRegardingAccessToPersonalDataBySecurityAgencies.pdf

by the European Court of Justice in 2014[24] and that several Constitutional Courts from European countries have declared the national laws implementing the Directive as breaching the rights to privacy, the Georgian Parliament has not given up on its plans on data retention and they were delayed to be discussed at the end of February 2015.[25]

Also the Romanian Constitutional Court has declared two times two different data retention laws as breaching the fundamental rights. The first decision [26], has been used also by other constitutional courts in Europe for its arguments. The judges explained that a system of widespread surveillance if problematic in relation with human rights:

> *"This operation [retaining the communication data"- our note] equally addresses all the law subjects, regardless of whether they have committed penal crimes or not or whether they are the subject of a penal investigation or not, which is likely to overturn the presumption of innocence and to transform a priori all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes. Law 298/2008, even though it uses notions and procedures specific to the penal law, has a large applicability – practically to all physical and legal persons users of electronic communication services or public communication networks - so, it can't be considered to be in agreement with the provisions in the Constitution and Convention for the defence of human rights and fundamental freedoms regarding the guaranteeing of the rights to private life, secrecy of the correspondence and freedom of expression.*
>
> *(...)*

24. Judgment in Joined Cases C -293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, 8 April 2014 available at http://curia.europa.eu/juris/documents.jsf?num=C-293/12
25. "With this decision Parliament has also delayed till February 28, 2015 to adopt data retention regulations. Regulations should define where data – it involves records which can identify a caller and date, place, duration and the means of communication, but not the content of the communication itself – will be retained and for how long." - from news "President Vetoes Delaying Adoption of Key Part of Surveillance Regulation" (31.10.2014) http://civil.ge/eng/article.php?id=27762
26. See the first decision that is also translated in English - Constitutional Court Decision no 1258 from 8 October 2009
available here http://www.legi-internet.ro/en/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html

The retaining of these data, in a continuous way, in relation to every user of electronic communication services or public communication networks (...) is sufficient to generate in the mind of the persons the legitimate suspicion regarding the respect of their privacy and the perpetration of abuses. "

2.3. Personal Data Legislation

The Georgian Law on Personal Data Protection (PDP) entered into force in May 2012. The provisions on administrative responsibility entered into force in January 2013, but were actually applied only in the second half of 2013, after the DPA was created. Furthermore, the application of the law to the private sector has entered into force only on 1 November 2014, following several new changes to the law that were adopted in August 2014.

This offers a limited period for the law's enforcement in order to identify its shortcomings in practice, but a few of them could be identified, based on a comparative approach with other best practices of the European data protection legislation and especially the Romanian and Republic of Moldova legislation.

It's worth noting that the DPA itself identified a number of limitations of the current law on data protection in its first annual report.[27] Also the civil society has issued a number of practical suggestions for the improvement of the legislation.[28] Other specific recommendations were made by the Council of Europe in its specific report[29] to the Georgian Parliament from February 2014. Some of these were implemented in the changes of the data protection law adopted on the 1st of August 2014.

We do need to emphasize that the overall impression when reading the law is that it fulfils the major aspects of the Council of Europe Convention 108 and EU data protection directive. Our comments are focusing only on some debatable issues regarding the law in force on 20 March 201530, while other aspects on the shortcomings of the institutional design are included in the next chapter:

27. DPA 2014 Annual Report (fn. 9) – page 22
28 See GYLA report – Personal Data Protection Inspector – Practice in Georgia and International Experience (2014) https://gyla.ge/uploads/publications/personalurmonacemTadacvisinspeqtori_en.pdf
29. See fn. 22
30. The report is based on the English translation of the law available here http://personaldata.ge/res/docs/Kanoni/PDP%20Law.pdf

- The lack of prior authorisation for the collection of special categories of data and/or other cases when such a collection could be sensitive to privacy rights might be considered as a limitation of the current law. In the case of Romania, the authority has used several times the prior authorisation regime not to allow certain data collection to take place until all legal restrictions have been met;
- The inflexible amount of a fine for each specific violation (chapter 7) could be considered as a limitation to the DPA in assessing each case and establishing a relevant penalty.[31] For example the Romanian law foresees a fine[32] starting with 500 RON (approx 110 Euro) and ending up to 10 000 RON (approx. 2220 Euro) for lack of notification, improper notification and notification with false information, so it leaves a lot of room for manoeuvre. Based on recent discussions for the draft EU Data Protection Regulation and taking into account the low level of fines for big companies, the DPA should consider if a fine based on a percentage of the turnover is not a suitable solution – for cases of major data breaches or repeated offences.
- Protecting personal data of a deceased person (art 8). This is sometimes a controversial subject and it is not included in the general EU legislation on data protection and also not covered by the major part of data protection regimes in Europe. There is also an ongoing discussion if the privacy and the personal data rights are inherently related to the persons, and, as such, if they should be irrelevant when that person dies.[33] But as a practical matter if the person is not alive any more, its personal data is less relevant, especially for the private sector – but it could become more used in other contexts (such as archives or libraries, research or statistics) where the issues of conflict with other fundamental rights (such as the freedom of expression) may

31. See also GYLA Report 2014 – Page 20 - "Administrative violations relating to the personal data and the amounts of the relevant fines. On the average, the amount of the fine varies from 500 GEL to 3'000 GEL depending on the gravity and the frequency of the violation. The law imperatively provides the amounts of the fines for each specific violation, therefore, the Personal Data Protection Inspector is deprived of the possibility to exercise discretional authority and to establish the reasonable amount of the fine according to the circumstances of each specific case"
32. Art. 31 – Romanian Law 677/2001 on personal data – Text in English available at http://dataprotection.ro/servlet/ViewDocument?id=174
33. For more details on this topic and other points of view see E Harbinja, "Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be The Potential Alternatives?", (2013) 10:1 *SCRIPTed* 19 http://script-ed.org/?p=843

arise more often. For example after the data protection law with similar provisions in this field was adopted in Republic of Moldova, they realised that the law actually made on obstacle for historians to research the recent history, so they had to issue a new specific law that would allow the transfer of the names of deceased people from 1943-1945 to the Holocaust Museum in United States of America for research purposes.[34]

– The limitation of the right of a data subject to request rectification, update, addition, blocking, erasure and destruction of data provided by art 22 of the law in "cases when the submission of such information is impossible due to the multiplicity of data recipients and disproportionately huge costs" seems excessive and could be misused by the data controllers.

2.4. Sector-specific legislation on personal data

Some of the sector specific regulations of data protection issues existed even before the data protection law was first adopted. However, these seem to be exceptional cases with a limited application in legal acts such as[35] Tax Code of Georgia, Law of Georgia on Commercial Banks, Decree of National Commission of Communications of Georgia on Provision of Services and Protection of Consumers' Rights in the Sphere of Electronic Communications or General Administrative Code of Georgia. The latter one was probably the most detailed on data protection issues, including a definition of personal data and more clear rules for personal data protection and privacy issues in relation to administrative agencies and ensures the lawfulness of their actions as a direct interpretation of Art 21 of the Georgian Constitution.

There seems to be a lot of room for improvement in the field of sector specific regulation of data protection issues, but this can be done in the next years. There are a lot of areas where such secondary legislation or even improving the primary legislation is needed such as:

34. See Law 38/2011 from Republic of Moldova and the situation quoted on page 27 in CRPE Report on personal data protection in the context of VLAP process in Republic of Moldova – Author: Bogdan Manolea, May 2011(only in Romanian) – available here http://www.crpe.ro/wp-content/uploads/2011/05/aici.pdf
35. See Regulatory Framework for Personal Data Protection in Georgia and its accordance with EU regulations (2013) – pag 25 https://www.duo.uio.no/bitstream/handle/10852/39045/Masters-Thesis.pdf?sequence=1

- the sector of electronic communications in regards to issues like: traffic data, subscribers directories or unsolicited communications (with a functional opt-in system);
- sector of health data and its related services;
- labour relations, where a Recommendation of the DPA is already available[36]
- open data and data anonymisation practices[37]
- data protection as the specific purpose for data security and information security requirements.

2.5. Institutional framework and design for data protection

The EU Directive on data protection 95/46/EC38 foresees in Article 2839 the minimal requirements

36. Available at http://personaldata.ge/res/docs/recommendation/Labour%20Rec.pdf
37. Especially in the context and activities internationally assumed by Georgia as part of their OGP plan – see details from the former plan Independent assessment of Georgia's 2012 open government action plan http://transparency.ge/en/node/4293
38. 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 Official Journal L 281 , 23/11/1995 P. 0031 – 0050 available at http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046
39. Article 28 Supervisory authority

1. 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.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to

that a DPA should be meeting in order to be fully functional and independent.

A report of the Fundamental Rights Agency40 suggests an interesting classification and comparative presentation on the way that EU member states' authorities are fulfilling these requirements and what are the national best practices, with a starting point in above-mentioned Article 28 of the EU Directive. We would also use a similar classification for an analysis of the Georgian DPA:

- **Full Independence**41 is one of the essential criteria which need to be interpreted in a wider sense42 The DPA has a relative independence in the current normative framework. The current law stipulates in art 30 (3) b) that the current inspector would be automatically terminated for being "unable to perform his/her obligations for 4 consecutive months". As there is no specificity on who would see if the Inspector was able or not to perform his/her obligation, this provision leaves room for potential abuses – which we have seen happening in Romania done in the past both for presidents of the the Data Protection Authority, but also for the Electronic Communications Authority. Also, a lot of details of practical importance43 that could significally affect the independence of the authority are left to be regulated by a Statute enacted by the Executive Government which could be another tool to change or minimize the current

---

national parliaments or other political institutions,

- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

40. See entire document - European Union Agency for Fundamental Rights Data Protection in the European Union: the role of National Data Protection Authorities Luxembourg: Publications office of the European Union, 2010, available at http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf
41. For a detailed interpretation see the European Court of Justice case Case C-518/07 European Commission vs. Federal Republic of Germany available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?isOldUri=true&uri=CELEX:62007CJ0518
42. "That independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data. " see fn 40
43. Such as "The structure of the office, rules of activities and of division of powers among the employees" or "terms of activities of an Inspector and of exercising his/her powers" - see Art. 27 (6) and Art 32 (2) of the Georgian data protection law - fn30

role of the DPA.

- **Resources.** The Georgian DPA seems to be adequately provided with human and financial resources at this point. The current legislation however cannot impede a potential drastic restriction of its budget, if the authority that approves the state budget decides to do so.
- **Powers of investigation.** The Georgian legal framework seems to give the DPA enough powers to supervise the application of the law. It remains to be seen though to what extent this will work in practice when the DPA would like to enforce them to public or private bodies.
- **Powers of intervention.** So far the DPA has functioned more like a mediator, so it is not tested yet if these attributions are functional or not. Also, it seems unclear at least if the DPA has actually any direct instrument to analyse a data processing before it starts, especially if it is likely to present specific risks – the current text of art 20 (but also article 10 that regards biometric data) only specify a notification procedure, which is less powerful than a prior authorization regime.[44]
- **Powers to hear claims and engage in legal proceedings** The Georgian DPA has these powers in the current legal framework, but it has used them to a limited extent, considering the reduced number of complaints. We have to point out that **t**he only fine issued by the Georgian DPA in 2014 that was contested in court, was upheld by the Tbilisi Court.[45]
- **Advisory powers.** The art 36 of the Georgian Personal Data law foresees that the DPA is authorized to submit proposals to the Parliament of Georgia and other public institutions for the purpose of improvements in the legislation and prepare conclusions on the laws and other normative acts related to the processing of data, on its own initiative. The best practices from

44. GYLA Report page 11 (see fn. 24) provides more context to this issue: "The law of Georgia on the "Personal Data Protection" does not directly provide the obligation of examining the environment prior to the data processing, but because the the data processors have the obligation to inform the inspecting authority in writing (or electronically) of the law-prescribed information prior to the creation of the personal data Filing System and prior to adding the new category of information to the system, it may be implied that if the doubts arise prior to the processing of the data, the Inspector has an authority to conduct the inspection for establishing whether or not the existing environment complies with the requirements prescribed under the law."
45. See page 8 of the DPA Report 2015 (fn.18)

EU member states46 and from the European Data Protection Supervisor indicate that it is much better to have a mandatory consultation of the DPA for all draft governmental acts that have an effect on privacy or personal data and that the result of the consultation is made publicly available. In the absence of such publication, it would be impossible to assess the role of the DPA in the legislative process and the way the government answered to its arguments.

The area of privacy and personal data is, by its own nature, closely linked with the activity of NGOs dealing with human rights issues. With several NGOs in the country that have significant expertise on privacy and data protection, the Georgian DPA could really use this expertise in its favour. Where other data protection authorities in Europe have acknowledged this expertise, such a collaboration has proven to be very fruitful for both parties involved. The FRA report[47] provides two important arguments in this respect:

> *"Firstly, NGOs are in a position to signal systematic and/or flagrant violations of data protection laws to national authorities and civil society. Thus an additional, informal supervisory body is in place. In certain instances they effectively contribute to a comprehensive monitoring of the data protection field. Secondly, NGOs provide for a 'bottom-up' channel of communication, providing active citizens with the opportunity to propose amendments to the legal framework."*

In the end, we believe that the real test for the independence of the Georgian DPA would be the reaction of the government to possible DPA decisions which are unfavourable to its direct or indirect actions. For example it is unclear if and how the DPA was actively involved in providing its expertise on the new amendments adopted on 30 November 2014 by the Parliament.

2.6 Implementation of the current data protection regime

Due to the relative short period of time since the law has been in force, it would be difficult to have a

46. See FRA report (see fn 40) arguments on this "The absence of opinions issued by Data Protection Authorities prior to the enactment of legislation or guidelines that have a potentially negative impact on personal data protection, may signal that there is a failure to fully appreciate the importance of the protection of privacy when making political choices. As such, it may be recommended that Member States ensure a more consistent involvement of supervisory bodies in the policy-making process.
47. Page 49 of FRA report – see fn 40

comprehensive image of the results of its implementation.

However, the image depicted in the first report of the Georgian DPA[48] seems to be glum, but accurate:

> *"In Georgia even the large organizations fail to fully realize their responsibilities and obligations. (...) In everyday life people have to frequently deal with collection, storage, disclosure or dissemination of their data. A certain part of the citizens have the feeling that they are under constant scrutiny."*

Despite the efforts of the Georgian DPA from the past years – that have correctly focused on trainings and awareness to the data processors and data controllers - it appears that not a lot has changed in the meantime, based on the overall feedback from the interviews gathered.

While this is the big picture of the situation, then the present limited enforcement in specific cases[49] (through fines or stopping collection of illegal data) raises some question marks regarding the strategy for the next years and whether it should focus more on significant actions and publicly sanctioning blatant data protection breaches.

Even though the implementation of the law in the private sector is impossible to assess at this point[50], with only 5 months of implementation, it is worth noticing as a good practice the fact that several private companies (mainly banks), but also other state institutions, have appointed Data Protection Officers (DPOs) despite the fact that the current Georgian law has no specific requirement or even recommendation in this regard. On the other hand, a quick check of the DPA's Registry of Filling System[51] shows us that only 6 private companies have notified the DPA about their filing systems in the first five months of the law's implementation – which is a very low number.

Some specific issues related to the implementation of data protection rules by the Georgian public administration were raised during the interviews in November 2014 and are relevant for the current

48. See Page 21 of the DPA 2014 Report (fn. 9)
49. Only 3 public institutions were fined in 2014, according to page 7 of the DPA Annual Rapport made public on 17.03.2015 (fn.18)
50. There are several cases highlighted in the DPA 2015 report – page 22 – most of them where the reports notes that further consultations are on-going - fn18
51. Checked at http://catalog.pdp.ge/SearchCatalogue on 2 April 2015

status of implementation. While we were positively surprised by a number of IT and e-government systems deployed by the Georgian state, it was quickly confirmed that they were implemented without a fully proper consideration of data protection principles (*privacy by design*). Therefore a number of these systems could raise significant data protection issues that need to be addressed as soon as possible. In fact, also the DPA report issued in 2015[52] investigated some practices, such as the legality of disclosing personal data on the web-page by the National Agency of Public Registry and the Central Election Commission.

For example[53] the Georgian Public Service Development Agency (PSDA)[54] is a public institution operating under the management of the Georgian Ministry of Justice. The functions of the Public Service Development Agency include maintaining and constantly improving the registry of citizens and issuing related documents, but also performing various functions of the civil registry, such as: maintaining a common population registry, registering civil acts, issuing identity documents, carrying out procedures related to citizenship, working on migration issues, authenticating documents by Apostille and legalization.

PSDA processes the personal data for the electronic ID card(which is mandatory for all citizens over 14 years old) and for passports (which are now only biometric passports).

According to an answer received from PSDA[55], there are "currently approximately 70 entities[56] receiving PSDA data. Approximately 20 of them are commercial banks, 20 are other private sector companies and 30 are from the public sector, which is composed of ministries and legal entities of public law. It must be noted that no entity has access to biometric data from the PSDA." According to our understanding, these entities have direct access to the PSDA database – of course, with various access rights – which is granted through an agreement procedure between these entities and PSDA.

52. Page 10 DPA 2015 report – fn 18
53. To be precise, we need to highlight that we are not pointing out to this state institution example as the most important or prominent one – but just one that we directly encountered in our analysis and interviews that started after a personal incident. We actually need to thank PSDA for their openness in answering our questions on these issues.
54. More detailed about PSDA at http://sda.gov.ge/en/home/
55 Source: Email received by the Author on 17.11.2014, Subject: Answers concerning Personal and Biometric data Public Service Development Agency, Georgia.
56. 73 institutions according to the page 16 DPA 2015 report (fn. 18)

The PSDA confirms that when a citizen obtains an ID card or a passport, he/she is not informed in detail on how or with whom that data will be shared. The authority underlines that the consent is at the basis of this data processing[57] of his/her data for a specific purpose.

Whereas the system could have real benefits for the citizens and work really well in practice, from an outside perspective a few data protection questions could to be raised, such as:

- consent for data processing – is it a voluntary consent if the user cannot object to having an ID card under these conditions imposed by PSDA, while having an ID card is mandatory?
- purpose of data processing – is the purpose of data collection to get an ID card or to give data to 70 entities? For what purposes are those entities processing the data? Is it the same purpose or for different purposes?
- May a user object to access to its data from one or several private entities? Or by public entities? May he/she knows when his/hers data have been accessed and for what purposes?
- Shouldn't the user give its consent on the specific access from other entities than those specifically prescribed by law? Is a memorandum a powerful enough legal basis for the access?

Moreover, the PSDA gives a clear – and not clear at the same time – answer to the question of how long the personal data is being kept:

> *"There is no specification of the duration of data storage. Therefore, it is reasonable to assume that data is stored indefinitely. However, it is noteworthy that ID cards are valid for 10 years. "*

Whereas the answer should raise immediate questions on issues such as the necessity to keep the data longer than the period of validity of the ID cards, this actually seems to highlight a practice already identified by the DPA in their report from 2014[58]:

> *Mostly the data processors themselves acknowledge that the storage of data is performed with a term inadequate to the purpose or without any term whatsoever. Throughout the years data*

57. Defined by the Georgian data protection law as the "voluntary consent of a data subject to the processing of data regarding him/her for a specific purpose, expressed orally, by means of telecommunication or other relevant means, which can clearly indicate the will of a data subject, after receiving relevant information by him/her."
58. Page 6 of the 2014 Report of the DPA (fn.9)

processors have been observing the principle: "we keep everything that can be collected and stored." In practice the term of data storage depends not on the purpose of data collection, rather on the technical conditions such as server capacity or archiving capability.

Another question on the practices of biometric passport issuing regards similar unclear data protection practices that should have respected data minimization[59] principles:

"The biometric data is stored in the database of the Public Service Development Agency (PSDA) at the time the document's issuance. The data includes a biometric photo and four fingerprints."

Why are the authorities asking for 4 fingerprints and not only 2 (which is the norm)? Has it ever considered not to have a common database for biometric identifiers (especially fingerprints) and to be only store them on the chip device?[60]

The lack of precise answers to all these questions might show that the data protection principles are not respected in practice, although the institution has a DPO and it has received training from the DPA in the past years.

The Georgian DPA investigated[61] some of the issues related access of other authorities to PSDA in 2014 and it is no surprise that they found both access to a disproportionate amount of data and/or access to the data without a legal basis:

"it was found that the data was transmitted to several organizations without identifying the legal basis (often times contracts/memoranda concluded between the Agency and other organizations did not include the reference and the Agency did not possess the verified

59. In collecting data, the Government should adopt a principle of data minimisation: it should collect only what is essential, to be stored only for as long as is necessary. See details in "In the Service of the States Dilemmas of Privacy and Technology Enabled Surveillance," Walter Frisch, University of Vienna, 2008 available la http://staatswissenschaft.univie.ac.at/fileadmin/user_upload/inst_staatswissenschaften/Frisch/210116_ps/InTheSereviceoftheState-WFrisch-1.pdf
60. The common database for fingerprints in biometric passports could be considered illegal in the EU if we interpret correctly the ECJ decision Case C-291/12 from 17.10.2013 - http://curia.europa.eu/juris/document/document.jsf?docid=143189&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=585394
61. See original text in page 16 of the DPA 2015 report (fn 18)

information which legal obligation necessitated receiving information from the Agency's database), and the need for receiving the data was not substantiated. "

According to the same report four public institutions ceased to have access to the PSDA database.

Some of the interviews with private organizations confirmed the fears that these excessive data collection practices, as such the one highlighted above, are being misused in some cases. This was also highlighted in the report of the DPA[62] published in 2015. We believe that these cases, together with the ones related to surveillance and wiretapping discussed in chapter 2.2, are the main cause of the Georgian people's "*feeling that they are under constant scrutiny."*

Therefore, we would recommend that a detailed Privacy Impact Assessment of the government regarding the IT systems that process a large number of personal data is a necessity from the DPA, at least at this stage – because of the low level of data protection awareness in these institutions that could just lead to implementation of strictly formal measures (e.g. a new consent form) for much more complicated issues.

3. Relation with the EU and the Visa Liberalisation Action Plan (VLAP)

3.1 Visa Liberalisation Action Plan (VLAP) and data protection

Following the 2012 launch of the EU-Georgia Visa Liberalisation Dialogue and the implementation of the VLAP in 2013, the European Commission adopted on 29 October 2014[63] its second progress report on the implementation by Georgia of the VLAP that concludes that Georgia meets the first-phase requirements of the visa dialogue.

The second phase, where the Commission will be checking the implementation of all these benchmarks, has been launched and it includes the following steps in the field of data protection:

- Implementation of the legislation on the protection of personal data both in the public and private sectors;

62. See page 20 of the DPA 2015 report – fn. 18
63. Georgia: one step closer to EU visa liberalisation (29.10.2014) http://europa.eu/rapid/press-release_IP-14-1206_en.htm

- Ensuring efficient functioning of the independent data protection supervisory authority both in the public and private sectors also through the allocation of the necessary human and financial resources;
- Conducting training programmes (including on anti-corruption) and raising awareness on data protection, including establishment of guidelines and ethical codes for officials and authorities concerned.

While Georgia is still very early in the process of implementing these steps, it's worth noting that the second one seems to be close to achievement, if the level of staffing and funding would remain satisfactory after the new attributions related to surveillance activities will start. As regards the first item, our estimation is that the implementation is still in early stages and an ambitious and pro-active attitude is needed for a quick success.

Also, the recent Georgian report on "Implementation of the European Neighbourhood Policy in Georgia - Progress in 2014 and recommendations for actions" acknowledges the steps forward in the field of data protection and surveillance activities, but also remains cautious on the quality of the new surveillance law by recommending that "An assessment of the new surveillance law by the Venice Commission of the Council of Europe would be necessary. "[64]

3.2. Impact of the EU acquis communautaire

It's obvious that the VLAP process has been instrumental on developing and encouraging a personal data protection legal and institutional framework. The EU data protection rules are probably one of the highest world standards on data protection, but this is the result of a lengthy and complicated process that started in some member countries almost 40 years ago. As a direct consequence, we should not expect major results over night, as it happened in other countries where data protection domain was introduced mainly as a result of the EU integration. For example the data protection law was adopted in 2001 in Romania, but until 2006 when the new authority was created, nothing important happened in terms of implementation

64. Page 14 of the Implementation of the European Neighborhood Policy in Georgia Progress in 2014 and recommendations for actions (25.03.2015) http://eeas.europa.eu/enp/pdf/2015/georgia-enp-report-2015_en.pdf

In the context of Georgia's Association Agreement with the EU and its inherent process to implement the European *acquis communautaire*, it's worth underlining that there are several normative acts[65] that directly or indirectly regard the processing of personal data.

Consequently, we may identify, from a theoretical point of view, three stages for data protection objectives in the following years:

A) Fulfilment of the minimal data protection standards as part of the visa liberalisation process;

B) Reaching the adequate level of data protection recognized by the European Union[66];

C) Implementing the entire *aquis communautaire* in this specific field.

It's important to note in this context that these stages can be identified only in the process of adapting to EU standards and not necessarily as steps that Georgia has internally established as a path to a functioning privacy protection framework.

Although we understand the specific interest from Georgia on the elements of the action plan (already seen in other states that have followed the similar route), we need to underline the risk that the interest in fulfilling these elements can replace the natural interest of having an efficient protection of personal data in the country on the medium and long term. Learning also from the Romanian experience, this moment should also be used by the interested stakeholders to push for a functional data protection system to be put in place before the VLAP process is finalized.

Thus, we would like to point out the following ideas:

- meeting the EU standards may sometimes represent a subjective standard and not necessarily solve all the problems in the privacy and data protection field;
- the analysis made by foreign experts (the current one included) need to be read in the specific national context of Georgia that is much better known by the local experts who can identify better ways of implementation. Also, nothing should stop Georgia from implementing a lot of the best practices from EU member states that go beyond the minimum agreed EU criteria;

65. See Report on Privacy and Personal Data Protection in the European Union – AEDH &EDRi, December 2009, http://www.ldh-france.org/IMG/pdf/legislation_Europeenne.pdf, p. 11-36
66. More information at http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

- the EU standards are in place after a lengthy process of implementing the personal data protection provisions and in a somehow different economic context;
- The EU regularly holds tense debates and sometimes with opposite opinions on a lot of the subjects that may be presented afterwards as "the norm in the EU" - especially in the conflict between data protection on one side and justice, law enforcement, security or visa and immigration, on the other side.67 For example see the tense situation on the adoption, implementation and then invalidation of the EU Data Retention Directive68 or the current debates on the draft EU Data Protection Regulation.

67. See various opinions of the European Data Protection Supervisor on various EU normative acts - https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Papers
68. For a detailed analysis see "Data Retention after the Judgment of the Court of Justice of the European Union by Prof. Dr. Franziska Boehm and Prof.Dr.Mark D.Cole (30.06.2014) available at http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf

4. Conclusions and Recommendations

4.1. Conclusions

On data protection and privacy Georgia has come a long way in just three years - from a country where privacy was breached daily to one where finding the right protection for personal data and privacy is a hot subject for public debates. Some of these debates have been transformed in real benefits for protection of personal data – a functional law, a data protection authority on regulating the private and public sector, including law enforcement.

Other debates are still not producing the necessary result for a real privacy protection – and the new surveillance law seems to be the most obvious bottleneck these months[69], that will probably be solved only through the intervention of the Constitutional Court.

While several important problems have been addressed, it would be difficult to say at this point that all the mechanisms of prevention from potential systemic violations of privacy are in place. A large number of valid concerns[70] of NGOs on the new surveillance laws are left unanswered on a very sensitive subject in almost all EU countries and beyond – the balance between security and privacy in the current digital world.

The current low level of awareness on data protection and the lack of an efficient mechanism of protection for many years have led not just to many cases of personal data breaches, but also to cases of excessive collection and storing of personal data.

Thus all the activities in Georgia for the protection of personal data and privacy, despite the efforts of Georgian Data Protection Authority in this field, are just an indication that this is just the beginning of a long process, that needs to be supported daily for the country to reach the level where human rights are

69. See "This Affects You Too Campaign responds to the Prime Minister "(21.11.2014) http://transparency.ge/en/post/general-announcement/affects-you-too-campaign-responds-prime-minister
70. See "Nine threats to your personal life stemming from the new legislation on secret wiretapping" (23.12.2014) http://transparency.ge/en/blog/nine-threats-your-personal-life-stemming-new-legislation-ons-secret-wiretapping

respected.

The Visa Liberalisation process and the Association Agreement are focusing also on the issue of personal data protection. This opportunity will give Georgian authorities the opportunity to adapt the normative framework to the highest world standards on data protection. Even though these are great times to get the political support for such a process, **it's important to stress the final goal: of a legal, institutional and practical framework of privacy protection in Georgia.** Establishing this clear goal may allow tackling fundamental problems and not just checking criteria on a short term for the current geopolitical/economical objective.

The current framework on personal data protection in Georgia is good from a legal framework perspective, but unsatisfactory at the implementation level. Also as regards the VLAP, the process needs a better planning not only from the DPA, but also a real involvement from other public bodies that could have a role in data protection or are significant public data controllers.

As regards the data protection framework on a medium and long term, we suggest an exhaustive evaluation from the DPA of the major e-government systems focusing on respecting data protection principles and more specifically on the necessity of data collection and data storage. Unless this is done now, when the pressure of the EU integration process is higher, we doubt that it could be done later as an exhaustive process.

A major step in the right direction on a real privacy right could be considered achieved when the DPA report would acknowledge not that "*Certain part of the citizens has the feeling that they are under constant scrutiny",* but rather *" Now, a major part of the citizens feel free from surveillance".*

4.2. Recommendations

4.2.1 Legal and institutional recommendations

a) Following the decision of the Constitutional Court on the surveillance law, initiate a real and inclusive debate with public entities, civil society and private sector on a text that will respect the highest standards of privacy protections;

b) Implement the recommendations of the Council of Europe's reports from February and

September 2014[71] for a comprehensive analysis of the data protection framework in the field of law enforcement and secret services, as well as for specific data protection rules for these categories before the new law is adopted and include these results in the public debate;

c) Have a review of the final draft law on surveillance by the Venice Commission of the Council of Europe;

d) Give up on the current data retention plans;

e) Include an authorization procedure for processing special categories of personal data, if this is likely to raise privacy risks (e.g. for example in the case of biometric data or genetic data);

f) Establish minimum and maximum fines for each infringement of personal data legislation. Consider if a fine based on a percentage of the turnover of private companies is not a suitable solution – for cases of major data breaches or repeated offences;

g) Adopt other sector-based legislation or recommendations on data protection, where there is a need for further guidance or specificity of the data protection rules;

h) Include the obligation of a DPA opinion on all normative acts and e-government projects that may affect privacy or data protection. Include the publication of this opinion in an official publication and on the DPA website

i) Annul or clarify the text that may revoke the Inspector if "unable to perform his/her obligations for 4 consecutive months"

j) Create a method (e.g. a Consultative Council) to involve NGOs in the decision making process of the DPA

k) After a couple of years of implementation, commission an independent study to assess if the right to the protection of personal data of a deceased person is creating more problems than benefits;

4.2.2. Recommendations for implementation

(a) Elaborate detailed Privacy Impact Assessment evaluations especially for the current e-

71 Op. cit. See fn. 22 and 23

government projects or other state owned IT projects that process a high number of personal data;

(b) Analyse the major privacy breaches before the year 2012 and make complaints to relevant investigation bodies, in order to show that the responsible people are brought to justice. Publicize these actions in order to get support from media and the public;

(c) Encourage the current practice of establishing a Data Protection Officer in public and private sector and offer benefits to companies or institutions that do so;

(d) Establish annual priorities for the DPA in regard to the most common type of personal data processing, with emphasis on the special categories of data;

(e) Raise awareness within the legal professions (judges, prosecutors, lawyers, legal advisers, etc.) on personal data protection;

(f) Consider promoting actions in court for the significant cases of data breaches and for cases of strategic litigation;

(g) Establish minimum security rules for data processing in cooperation with all interested parties.

4.2.3. Specific recommendations for the VLAP process

- Create and publicize an Action Plan for the fulfilment of the 2nd phase of the VLAP, through a transparent and inclusive process;
- Consider including in the action plan:
    - Development by the DPA of a training plan for at least 3 years for all its current personnel and include it in the yearly budget. Plan at least 2-3 persons to participate to international Masters programmes on data protection, in order to create national expertise in the DPA;
    - Development by the DPA of a 3 year budget plan, that should include awareness activities in Georgia and approval of this plan by the Ministry of Finance.
- Conduct Training of Trainers activities for DPOs and provide them with training materials they may use themselves;

- Coordinate the DPOs in more formal actions and gather feedback from them on various problems and solutions;
- Publish the action plan and the monthly reports of the responsible authorities.

This Policy Brief was published by the Romanian Center for European Policies within the project *"Supporting the Visa Liberalization Process in Georgia through assistance in the field of anti-discrimination and personal data protection", supported by the Romanian Ministry of Foreign Affairs, through its Official Development Assistance Policy.* The project has been implemented with the support of Open Society Georgia Foundation between July 2014 and April 2015.

The Official Development Assistance Policy of Romania has been established in 2007, following its accession to the European Union. The overall objective of this policy is to support the beneficiary countries' efforts to implement their own national development strategies.
As a donor, Romania is focused on sharing its experience and lessons learned in the transition to a democratic political system and society, as well as the Euro-Atlantic integration process, with a thematic focus on:

- Good governance
- Strengthening democracy and the rule of law
- Economic development
- Education, vocational training and employment
- Health
- Development of infrastructure and environment protection

The opinions presented in this report do not necessarily represent the position of CRPE or of the financing institution.

Romanian Center for European Policies www.crpe.ro

Ştirbei Vodă street no. 29, Bucharest

Contact: office@crpe.ro

Tel. +4 0371.083.577

Fax. +4 0372.875.089

www.crpe.ro