E-Government in Greece: Serving State's Economic Needs – Respecting the Fundamental Right to Data Protection

Zoe Kardasiadou, Evi Chatziliasi, and Konstantinos Limniotis

Hellenic Data Protection Authority,
Kifisias 1-3, 11523, Athens, Greece
{kardasiadou,exatziliasi,klimniotis}@dpa.gr

Abstract. Due to the recent economic crisis Greece is facing, the government has developed several initiatives using information and communication technologies (ICT) in order to foster the economic growth, enhance trust and transparency in the operation of public administration, streamline the public expenditure and combat corruption and tax evasion. Such initiatives include: a) the "transparency project", b) the electronic prescription, c) the publication of tax data on the internet, d) the use of a tax card and finally e) the eGovernment Law. As data protection is a fundamental right according to Greek and EU law, this paper aims at analyzing whether such initiatives pass the proportionality test and may justify "legitimate" restrictions of the aforementioned right and which particular data security and other measures may alleviate the restrictions occurred.

Keywords: e-Government, personal data protection.

1 Introduction

E-government services are being characterized as a "guiding vision towards modern administration and democracy" [1]. Notably, the appropriate use of ICT technologies for interactions with the public sector results in several benefits, including transparency, openness, convenience, revenue growth and cost reductions. On this direction, the European Commission launched in 2010 the Europe 2020 Strategy[1] which sets objectives for the growth of the European Union by 2020, including better exploitation of ICT in order to foster innovation, economic growth and progress.

In light of the recent financial crisis which exceeds the Greek borders, it becomes evident that the aforementioned goal is of major importance. Moreover, in this highly evolving environment, reconciling public interests and fundamental rights, such as the right to data protection, is crucial. As it is explicitly pointed out in the Digital Agenda (one of the seven pillars of the Europe 2020 Strategy), the right to privacy and the

[1] The Europe 2020 strategy was proposed by the Commission on 3 March 2010 [COM/2010/2020] and adopted by the European Council on 26 March 2010.

H. Jahankhani et al. (Eds.): ICGS3/e-Democracy 2011, LNICST 99, pp. 179–185, 2012.

protection of personal data are fundamental rights which should be effectively enforced using the widest range of means: from the wide application of the principle of "Privacy by Design" in the relevant ICT technologies to dissuasive sanctions, wherever necessary.

The Greek government in the era of economic crisis but also as an addressee of the Europe 2020 Strategy is developing several initiatives based on ICT, aiming at fostering economic growth and transparency, increasing accountability, strengthening control mechanisms and a tax compliance culture, and streamlining public expenditure.

This paper studies e-government services in Greece and how these affect the right to data protection. The question whether they pass the proportionality test is addressed, mainly based on the relevant Opinions of the Hellenic Data Protection Authority (HDPA)[2]. More precisely, the paper is organized as follows: Section 2 discusses the legitimate limitations of fundamental rights. Recent ICT initiatives in Greece are studied in Section 3, where relating data protection issues are highlighted. Concluding remarks are given in Section 4.

2 Limitations of Fundamental Rights in the CJEU Case Law

Given that the operation of e-government services may impose limitations on the exercise of the fundamental right to the protection of personal data[3] the relevant case law of the Court of Justice of the European Union should be considered. Accordingly, limitations imposed on fundamental rights should be provided for by law, meet objectives of general interest recognised by the European Union (e.g. transparency and accountability regarding the use of public funds) or the need to protect the rights and freedoms of others and be subject to the principle of proportionality in the sense that they are necessary in order to meet the aforementioned objectives.

A prominent example of how to strike the proper balance between legitimate public interests and the right to the protection of personal data is the recent decision of the Court of Justice regarding the publication on a website of identifying (personal) information relating to the beneficiaries of agricultural funds within the Common Agricultural Policy (CAP) of the EU[4]. In this case the Court first accepted that such a publication is provided for by law and is appropriate to enhance transparency, which constitutes a legitimate interest as being established in the EU Treaties (it enables citizens to participate in the decision making process, guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen in a democratic system). It continued that the right to data protection is not an absolute right,

[2] The Hellenic Data Protection Authority, established by the Data Protection Law 2472/1997, is a constitutionally entrenched independent authority (art. 9A of the Hellenic Constitution).

[3] The right to the protection of personal data is laid down in article 8 of the European Convention on Human Rights and more explicitly in article 8 of the Charter of Fundamental Rights of the European Union. The Charter has binding legal effect, equal to the Treaties, after the entry into force of the Lisbon Treaty.

[4] See Court of Justice of the EU, joined cases C-92/09, C-93/09 Volker und Markus Schecke GbR / Hartmut Eifert vs Land Hessen.

but must be considered in relation to its function in the society. Having said that, the Court found that the lack of any criteria for publishing personal data (e.g. the periods for which the beneficiaries received aid, the frequency, nature and amount of aid received) exceeds the limits imposed by the proportionality principle and renders the processing illegal.

From the aforementioned decision it can be concluded that the proportionality principle shall be respected in a way that at least the core of the fundamental right in question is not affected. To achieve this, differentiating criteria as well as data security measures shall be established. Otherwise the endeavour may be rendered illegal. In the following section this rule will be applied to some eGov initiatives in Greece.

3 E-Government Initiatives in Greece

3.1 The Transparency Project

The transparency project (Law 3861/2010) is aiming at enhancing the accountability of the public administration. To this end, it provides for the publication on the Internet of all legislative and a series of categories of administrative acts, including the appointment of civil servants, the issuance of building permits and public expenses. In addition, easy search capability for documents is supported by using keywords and/or thematic meta-data. The uploaded documents (.pdf format) are digitally signed and automatically provided with a unique number.

The HDPA has been consulted prior to the adoption of the law and issued the Opinion 1/2010[5] on the draft law, imposing restrictions in the publication:

1. Sensitive data should not be uploaded unless the HDPA issues a prior permit. As a response to this, the Law 3861/2010 excluded sensitive data from its scope.
2. Further use of the published data shall be allowed only for the purpose of free access to public information and not for other purposes, such as commercial ones. To this end, the central web site http://et.diavgeia.gov.gr/ of the transparency project states explicitly, in its “Terms of Use”, that illegal processing (by third parties) is prohibited; however, it is not further explained which purpose is considered legal.
3. Appropriate technical measures should be adopted, to avoid unlawful processing of personal data (e.g. creation of individuals “profiles”). After the initiation of the project, the HPDA specified several measures towards this direction. These include: i) measures to prohibit the processing by external search engines (since transparency may be adequately served via the dedicated web sites of the authorities), such as appropriate lock of uploaded .pdf files, as well as the use of the Robots Exclusion Protocol, b) measures to prevent massive downloads, such as usage of appropriate challenge/response tools (e.g. Captcha) and c) proper administration of tracking cookies with the use of friendly techniques for opt-out

[5] All the Opinions referred in this paper are available (in Greek) at the HDPA's site `http://www.dpa.gr`

instead of forcing users to change their browser settings. Up to the cookies the aforementioned measures are not yet implemented[6].

4. A time limitation for the publication should be in place; such a limitation is not in conflict with the need for transparency, since each file's meta-data may be available for longer in order to facilitate citizens' requests for access directly to the competent authorities. This condition is not yet implemented.

As a result, the project still lacks of some essential safeguards for an efficient protection of personal data.

3.2 The Electronic Prescription

Law 3892/2010 provides for an integrated electronic prescription system which shall support the effective control of insurance funds' expenditures, amongst others by limiting unnecessary prescriptions. The system is currently focusing on some insurance funds in the process of completing the pilot site.

The HDPA has been prior consulted and issued a permit approving the data processing upon specific conditions, namely:

1. A single entity (i.e. the General Secretariat for Social Security) should be appointed as data controller in terms of the Data Protection Act to ensure legal responsibility.
2. Authentication of the system's users should be put in place.
3. The access to data should be in accordance to the need-to-know principle (where the cases of the data controller, social insurance organisations, pharmacists and doctors are treated separately). Doctors' access to patient information produced by others is subject to patients' prior consent.
4. Any access should be logged.
5. Data should be kept for 20 years from the last treatment.
6. The HDPA shall be consulted prior to the issuance of the ministerial decision concerning the procedure and the technical requirements for the registration and the identification of the system's users.

3.3 Publication of Taxpayers' Data on the Internet

Towards combating tax evasion and enhancing compliance, the Ministry of Economy suggested as an exception to tax secrecy, the publication on the Internet of the annual income and the tax due by the taxpayers. Accordingly, a) access is limited to identified users, b) searches may be performed by specific criteria, that is the unique tax number or address and part of the name or business name, c) a limitation on the number of requests (up to 20 retrievals per month) will be in place, d) storage of data in editable form shall not be enabled.

[6] A new web site `http://yperdiavgeia.gr/`, maintained in the meanwhile by a computer expert, provides for more powerful searches due to the lack of the aforementioned measures.

The HDPA with the Opinion 1/2011 ruled that the aforementioned processing of personal data is not compliant with the proportionality principle, since there is no evidence that such publication is really necessary to combat tax evasion. On the contrary, one shall first consider the improvement of control mechanisms and powers of the competent authorities.

3.4 Tax Card

According to the Greek taxation law receipts for the purchase of goods or services may be deducted up to a certain amount from the taxable income and are also used for the establishment of the minimum of income, exempted from taxation. The Ministry of Economy introduced an optional system for the collection of such data, based on a magnetic card and the existing bank payment infrastructure (POS) at the suppliers' site. The system has a double purpose: it enables the automatic storage of the necessary data in the IT system of the Ministry while at the same time is used for the control of issuance of receipts by the suppliers. The data are transferred in real time through the banks to the tax authority without revealing purchasers'/taxpayers' identity. The supplier's name, the amount paid, and the unique identifier of the card are only transferred. After the data are received by the tax authority, this may link the information to a specific taxpayer on the basis of card's unique identifier. By the end of the calendar year the total amount spent by each taxpayer is calculated for the taxation, whereas the taxpayer may access at any time the information related to him/her via a secure web service.

The HDPA in the Opinion 4/2010 stressed that there was no sufficient legal basis for the processing of personal data in this system. Even if the use of the card should be optional, i.e. upon consent of the taxpayer, this shall be provided for by law. The HDPA also raised the concern that, although banks receive anonymous data, there is a possibility to identify data subjects if a credit card is used for the said payment. Thus there is the risk to create "consumer profiles". In our opinion, there is also the risk of creating suppliers' profiles, especially regarding their revenues. In addition, the HDPA pointed out that there is no need, even for the tax authority, to identify the taxpayers in real time, but at the end of the calendar year. In order to address these risks, the HDPA suggested the use of two different infrastructures to meet the two different purposes (a smart card for the taxpayers for the first purpose/connection of suppliers' cash registers with the system of the tax authority for the second purpose). Nevertheless, the tax card shall be introduced in October 2011 without implementing HDPA's remarks.

3.5 The eGovernment Law

Recently, the eGovernment Law 3979/2011 was adopted. The main objectives of this law are described as following: a) provide for the right of citizens and businesses to communicate with the public sector via ICT, b) user friendly services also for disabled people, c) reinforcement of trust between citizens, businesses and the public sector.

The law addresses several key issues, such as the protection of personal data, the identification/authentication of users, the validity of electronic documents and the shared use of telecommunication systems, computational resources, ICT infrastructure and data amongst public sector bodies (which may understood as the first attempt to introduce cloud computing and grids). In order to fully deploy legal effects however the law provides for the prior adoption of 24 implementing acts!

Regarding personal data protection, the law explicitly establishes the privacy-by-design and the data minimisation principle, the conduct of privacy impact assessments and the appointment of a Data Protection Officer in each public body. Moreover, it states that that the right to access should be exercised upon users' authentication and appropriate security measures. The future use of one's personal data is allowed only on the basis of consent. As a remark, these high-level principles need to be further specified in order to effectively enhance personal data protection.

Development of a Greek e-ID Card. The eGov Law 3979/2011 constitutes a first step towards the e-ID card. In this context, electronic identification and authentication schemes are prerequisites for proving one's identity, whereas electronic signature schemes are also necessary to create legally binding documents; hence, these three levels of protection (which have been also pointed out in the seminal paper [2]), constitute the main building block for any e-ID card.

Despite though the common underlying goals, a strong diversity exists regarding the adopted design approaches for the e-ID cards within the European Union; more precisely, while security of online public services is the primary aim, privacy seems to be a rather implicit goal [3]. Indeed, linkage of personal data for profiling purposes is not adequately treated in the current e-ID solutions - exceptions being Austria and Germany, which have taken some important steps towards unlinkability and selective disclosure [4]. The linkability problem mainly stems from unique identifiers, although decentralized data storage as well as context separation are also important factors to resolve this threat [3].

We subsequently briefly describe the Austrian case [5] which, according to some relevant publications (e.g. [6]), seems to have influenced the greek legislator. All individuals are registered in one of the national registers, whereas a unique 12-digit identifier (PIN) is assigned to each individual. PIN though is not used for identification and is not even stored in the card; instead, a unique source personal identification number (sourcePIN), derived by strong encryption from the citizen’s PIN, is stored in the e-ID card (as a separate XML-based data structure, containing the individual's public key which is associated with a certificate). The sourcePIN Register Authority is the Data Protection Commission. Moreover, each public service provider is assigned a specific sector’s code and a personal sector-specific identifier (ssPIN) is generated by applying a one-way hash function to the sPIN and the sector code; for each sector, identification is based on ssPIN, stored by the public service provider. Hence, an individual (with a unique sPIN) has a different ssPIN per service, whereas it is not possible, from a given ssPIN to derive either the sPIN or other ssPIN.

In the Greek case, many important questions need still to be answered: for instance, the law does not specify how the level of required security is determined, as well as whether identifiers are stored by the public entities. Moreover, although there is a reference for “per-service" generation of identifiers and credentials, it is not clear whether unlinkability (to ensure that a user may make multiple uses of services without others being able to link these uses together) is a design objective. From the perspective of the fundamental right to personal data protection unique identifiers, although technically convenient, should be avoided since they violate unlinkability and the principles of data minimization and purpose limitation.

4 Conclusions

Current economic crisis put at risk fundamental rights, especially because economic constraints may influence the criteria for striking the right balance, i.e. when applying the proportionality test. The boundaries of the margin of appreciation are set where the balance of public interests, such as transparency, accountability, combating tax evasion etc. on the one side, and the right to personal data protection on the other side, renders the latter invalid. A win-win situation may benefit the most through the serious consideration of privacy by design measures and an early consultation with the Data Protection Authorities.

References

1. Wimmer, M., Traunmuller, R.: Trends in electronic government: Managing distributed knowledge. In: Database and Expert System Applications, pp. 340–345 (2000)
2. Fiat, A., Shamir, A.: How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987)
3. Strauß, S.: The Limits of Control – (Governmental) Identity Management from a Privacy Perspective. In: Fischer-Hübner, S., Duquenoy, P., Hansen, M., Leenes, R., Zhang, G. (eds.) Privacy and Identity Management for Life. IFIP AICT, vol. 352, pp. 206–218. Springer, Heidelberg (2011)
4. Naumann, I., Hobgen, G., et al.: Privacy features of European eID card specifications. In: European Network and Information Society Agency, ENISA (2009)
5. Aichholzer, G., Strauß, S.: The Austrian case: multi-card concept and the relationship between citizen ID and social security cards. In: Identity in the Information Society. LNCS, vol. 3, pp. 65–85. Springer, Heidelberg (2010)
6. Drogkaris, P., Geneiatakis, D., Gritzalis, S., Lambrinoudakis, C., Mitrou, L.: Towards an Enhanced Authentication Framework for eGovernment Services: The Greek case. In: EGOV 2008 7th Int. Conf. on Electronic Government, pp. 189–196 (2008)