Future Internet **2015**, *7*, 500-515; doi:10.3390/fi7040500

OPEN ACCESS

future internet

ISSN 1999-5903

www.mdpi.com/journal/futureinternet

Article

A Hierarchical Multitier Approach for Privacy Policies in e-Government Environments

Prokopios Drogkaris [1,*], Stefanos Gritzalis [1], Christos Kalloniatis [2] and Costas Lambrinoudakis [3]

[1] Laboratory of Information and Communication Systems Security, Department of Information and Communication Systems Engineering, University of the Aegean, GR-83200 Samos, Greece; E-Mail: sgritz@aegean.gr

[2] Cultural Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, GR-81100 Mytilene, Greece; E-Mail: chkallon@aegean.gr

[3] Department of Digital Systems, University of Piraeus, GR-18534 Piraeus, Greece; E-Mail: clam@unipi.gr

* Author to whom correspondence should be addressed; E-Mail: pdrogk@aegean.gr; Tel.: +30-22730-820-00; Fax: +30-22730-820-09.

Academic Editor: Steven Furnell

Received: 11 August 2015 / Accepted: 9 December 2015 / Published: 21 December 2015

Abstract: The appeal of e-Government users to retain control over their personal information, while making use of advanced governmental electronic services through interconnected and interoperable deployments, can be assisted by the incorporation of privacy policy and Preferences documents. This paper addresses the formulation of light-weight and accurate privacy policies, while preserving compliance with underlying legal and regulatory framework. Through the exploitation of existing governmental hierarchies, a multitier approach is proposed able to support diverge data needs and processing requests imposed by service providers. The incorporation of this approach into e-Government environments will reduce the administrative workload, imposed by the inclusion of privacy policy documents, and promote the implementation and provision of user-centric and data privacy aware electronic services.

Keywords: e-Government; privacy policy; hierarchy; privacy preferences

1. Introduction

The broad expansion of Information and Communications Technologies (ICT) and the pervasive deployment of interconnected networks, along with service-oriented architectures, that enable the composition and provision of interactive and personalized services, have introduced overarching challenges related to security, dependability, privacy, and trust. Not only should they have built-in privacy and security, but they should also enable and empower users to comprehend and make informed decisions on trustworthiness of information, services, and levels of security. As governments are moving away from inter-organizational modalities and put emphasis on a collaborative and service-oriented model, issues concerning data privacy, protection against misuse, consent, accountability, and assurance to (re)gain attention. Hence, it is essential for them to strike the right balance between the needs for privacy and openness.

The deployment of privacy aware e-Government environments that allow for the provision of interoperable user-centric electronic services, while empowering users to retain control over their personal data, is largely acknowledged as a challenge in [1–4]. The incorporation of privacy policy and privacy preferences documents, through well-defined XML schemas, is an approach that can assist towards establishing certain level of assurance on data privacy for both users and service providers (SP) [5–7]. Such deployment advances and simplifies the provision of electronic services, while allowing users to preserve, control, and modify their personal data privacy characteristics based on their inclinations and needs. Based on such an architecture, e-Government environments could expand their capabilities towards implementing services that meet citizen needs, promote further exploitation of electronic services to different user groups and, finally, (re)establish confidence in applications of e-Governments involving sensitive personal information.

This paper addresses the formulation of coherent and accurate privacy policy documents, from service providers' perspective, while preserving compliance with underlying legal and regulatory framework. Through the exploitation of existing governmental hierarchies, a multitier approach is proposed able to support differ data needs and processing requests imposed by them. The inclusion of specific rules and referencing XML elements enables the formulation of light-weight documents that adhere to the imposed requirements.

The rest of the paper is structured as follows. Section 2 presents an architecture that promotes the employment of privacy policies and privacy preferences in modern e-Government environments while Section 3 presents the proposed hierarchical approach. Section 4 introduces a use case that provides evidence about its usability and functionality, while Section 5 discusses similar approaches on e-Health environments. Finally, Section 6 concludes the paper providing directions for future work.

2. Privacy Policies and Preferences in e-Government Environments

The concept of embodying privacy policy and privacy preference documents in modern e-Government environments has been explored in [8] towards advancing and simplifying the provision of electronic services while preserving user's privacy. Through privacy policy documents, each service provider provides a formal public engagement of the information required, the purpose of the request, as well as how the information will be used and to whom it will be disclosed. Data subjects consent to

the use of their personal data by specifying, for each data item or group, fine-grained privacy preferences that define how they can and must be used. Through this procedure, the data subject is empowered to revoke the right, upon decision, that has been previously granted to a data collector to use their personal data and/or can constitute certain data items or groups be no longer validly accessible.

The architecture's design is based on modern e-Government environment structures which embody a central portal; it most commonly operates as a one-stop shop, being the front-end for every service provider. Typically this portal implements the authentication and registration procedures or incorporates the federated identity management infrastructure for every service provider. Alongside to these authorities a new entity is introduced, named Privacy Controller Agent (PCA). It is responsible of storing and comparing service providers' privacy policies and user privacy preferences documents. An overview of an agents' architecture can be seen in Figure 1 below.

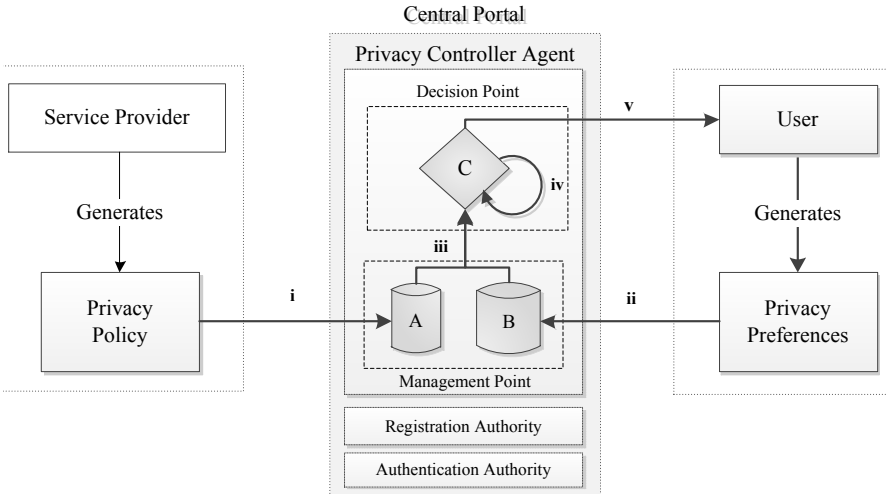

Figure 1. Privacy Controller Agent (PCA).

Privacy Controller Agent consists of two main units: a management point and decision point. The management point consists of two storage repositories which are in charge of retaining the privacy policy of each service (A) and the privacy preferences of each user (B). When a SP enrolls an electronic service to the central portal (CP), apart from the other information that he is required to provide, depending on the underlying interoperability framework, he must obligatorily submit the corresponding privacy policy. Since a service provider will most commonly offer numerous different electronic services, a separate privacy policy must be submitted for each one of them. This document states explicitly which data is required for service's provision, for which purpose it is required, how it will be processed, if it will be stored, for how long it will be retained and if it will be communicated to another SP. After its submission (action i), PCA validates the policy's origins and stores it at policy repository (A).

Similarly, when a user registers to the central portal, they are also required to submit their privacy preferences. Since privacy preferences regard a user's personal data, there is not a direct relation to the service they will be utilized by. Therefore, users will have to submit only one document which will apply to every electronic service. Apart from the categorization in data types (personal data and personal identifiers) and their scope of usage and processing, we propose the inclusion of characterization regarding the service provider that will process it. Thus, users will have to specify what type of data will be included in their privacy preferences, for what purpose can they be used, and by which service

provider. After their submission, the Privacy Controller Agent validates the preference's origins and stores them at the preferences repository (action ii).

Following a successful user authentication and request of an electronic service, the central portal forwards the request to Privacy Controller Agent. The PCA then retrieves the preferences and the corresponding policy and forwards them to the decision point (action iii). At this point the comparison procedure evolves and the policy is checked against the user's preferences. If preferences assent on the usage of data through the operations and for the purpose described in the policy, the agent informs the user through the portal of the concurrence and forwards the service's request to the applicable service provider. Through this comparison and notification the user is now confident that their personal data will be accessed, processed, and transmitted according to their preferences. In case these preferences do not match the policy of the service provider, the Privacy Controller Agent informs the user, again through central portal, of the conflict and its details. In typical privacy policy model, the controller agent would initiate a negotiation between the user and service provider in an attempt to overcome the conflict. However, due to the legal basis of all governmental services (electronic or not), the requisite pretenses are not likely to change and only user is prompted to review their preferences.

3. Privacy Policies Multitier Approach

In this paper we propose the adoption of a hierarchy multitier scheme for the deployment and organization of governmental service providers' privacy policies in e-Government environments. Based on the concept of embodying privacy policy and privacy preference, towards advancing and simplifying the provision of electronic services, presented in [8,9], it was evident that due to the size and total length of the privacy policy documents, especially for composite or multi-entry electronic services, they could not be easily administered and updated. Through the exploitation of existing governmental hierarchies the proposed multitier approach enables the formulation of light-weight documents. Such adoption will facilitate the consistent deployment and re-configuration of e-Government services while preserving compliance with the underlying legal and regulatory framework.

3.1. Hierarching Privacy Policies

In e-Government environments, data is structured at different abstraction levels, and service providers have different data needs and processing requests when requested to provide an electronic service. These needs and requests may deviate from each other but they are also bound to the restrictions opposed by corresponding ministerial departments and subsequently by legal requirements. Thus, from a modeling prospective, a privacy policy document, for a given electronic service, adheres and complies to the following hierarchy, where each arrow indicates a further level of generalization; Electronic Service → Service Provider → Ministerial Department → Central Government. A similar generalization level for e-Health environments has also been proposed at [10].

To make the above statement more formal, let us denote P_{CG} as the privacy policy elements of the central government, P_{MD} as the privacy policy elements of ministerial department, P_{SP} as the privacy policy elements of the service provider, and P_{ES} as the privacy policy elements of electronic service. Therefore, P_{ES} can be regarded as proper subset of P_{SP}, P_{SP} as a proper subset of P_{MD}, and P_{MD} as a proper subset of P_{CG}, as depicted in Equation (1), below:

$$P_{ES} \subsetneq P_{SP} \subsetneq P_{MD} \subsetneq P_{CG} \quad (1)$$

The expected inclusion of the aforementioned sets would be that P_{ES} is a subset of P_{SP}, P_{SP} a subset of P_{MD}, and P_{MD} a subset of P_{CG}. However, as we move towards supersets, the specification of elements regards different levels of abstraction. For example, P_{CG} will contain an element regarding Social Security Number (SSN); based on the underlying legal and regulatory framework SSN falls under the category of personal identifiers (PId) and, consequently, should be treated as confidential data. Thus, P_{CG} states that SSN should be treated as confidential data during processing and storage. At the next level of abstraction, P_{MD} assents to the classification of SSN as PId and only specifies that, for the purposes of the specific ministerial department, it can be retained for a specific amount of time (days). Moving along to lower superset levels, P_{SP} specifies if it will be processed and how by the specific service provider and, finally, P_{ES} specifies only the purposes for collecting this PId. Depending on the e-Government environment and the structure of the central government (unitary, federal, or con-federal) we consider, the number of sets and subsets could vary; however, the organization and the representation is always viable.

3.2. Privacy Policies Formation

Based on the architecture of the Privacy Controller Agent (PCA), presented at Section 2 above, when the PCA receives a user's request for an electronic service, two documents must be retrieved and compared against each other; (i) the user's privacy preferences; and (ii) the electronic service privacy policy. The first is submitted by user and stored at the preferences repository and the second is submitted by the service provider, specifically for each electronic service, and is stored at the policy repository. Taking into account the hierarchy scheme discussed in Section 3.1 and the identified proper subsets, the central government issues a generic privacy policy document that describes, in a broad level, how specific data types can be accessed, processed, and stored, based on the underlying legal and regulatory framework at level *(1)*. As we move down on the hierarchy, privacy policy documents are issued from specific ministerial departments, level *(2)*, and further down from specific electronic services, level *(k)*. At each one of these levels, an acknowledgement of previously-made acceptations, through reference, is included along to a more explicit expression of data access, process, storage, and retention period, if required. A schematic representation of privacy policy documents creation is depicted in Figure 2 below:

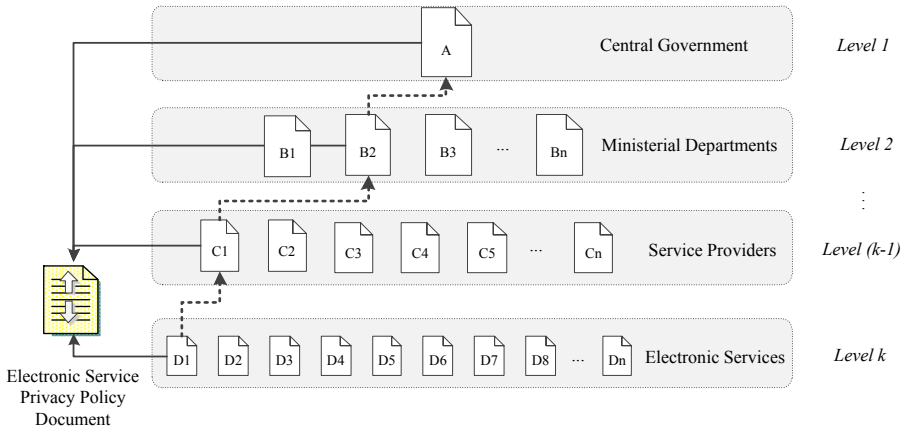

Figure 2. Electronic Service Privacy Policy Formation.

The number of references to previous levels may vary on each document depending on the provider of the electronic service and the structure of government. In every case, all documents should obligatorily contain a reference to the higher level *(1)* since it comprises a representation of the underlying legal and regulatory framework. To ensure a seamless transition of privacy requirements to lower levels we define the following mandatory rules which accompany the proposed approach.

Rule 1: Each one of the {*Level(k), Level (k−1), ⋯ , Level 3, Level 2*} privacy policy documents must comply to Level 1 document.

Privacy policy document compliance is defined as the absence of negation or generalization from the stipulations and clauses it imposes.

Rule 2: Each one of the {*Level(k), Level (k−1), ⋯ , Level 3, Level 2*} privacy policy documents must include direct or indirect reference to *Level 1* document.

Rule 3: Each one of the {*Level(k), Level (k−1), ⋯ , Level 3, Level 2*} privacy policy documents can introduce new stipulations and clauses, provided that they contradict to the existing ones.

Rule 4: Each one of the {*Level(k), Level (k−1), ⋯ , Level 3, Level 2*} privacy policy documents can only particularize stipulations and clauses imposed by higher level documents.

Particularization of stipulations (S) and clauses (C) is valid only if the introduced stipulation (S') or clause (C') are subsets of S or C respectively.

$$S' \subset S \mid C' \subset C \tag{2}$$

3.3. Approach Evaluation

The deployment of the proposed approach promotes the interoperability of electronic services along to the compliance with underlying legal and regulatory framework. This can be regarded not only as a control but also as an enforce mechanism for any alterations that may occur. A newly-introduced legislative amendment does not normally propagate seamlessly into the corresponding e-Government services; each service provider has to perform the appropriate modifications which take time and effort to be completed efficiently. Regardless if such a change occurs, ministerial departments and service providers cannot deviate from upper level stipulations and clauses, ensuring an overall comprehensive compliance. Moreover, the produced policy documents have significantly reduced length compared to the traditional approach which improves their manageability. Finally, it could be deployed in federated environments where data protection and privacy requirements are imposed by multiple providers or in cross border electronic service delivery. Within EU, such federated environments could enable the pan-European e-Government services provision, as described in the Interoperable Delivery of Pan-European e-Government Services to Public Administrations, Business, and Citizens (IDABC) (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens) and the Interoperability Solutions for European Public Administrations (ISA) (Interoperability Solutions for European Public Administrations) Programs of the European Commission.

From a security perspective, privacy policy documents do not contain any restricted information on the service provider and they are meant to be publicly available. Thus, the preservation of their integrity can be ensured by central portals' underlying public key infrastructure through digital signatures. An important issue that must be addressed during deployment of the proposed approach is the XML

schema to be utilized, as well as the creation and administration of the XML documents that will support the hierarchy scheme. Selecting the appropriate schema can be a complicated task. Existing schemas have not been designed taking into consideration specific needs and requirements of e-government environments. Thus, several aspects have been left uncovered and post-design modifications may be necessary. The proposal of a new schema oriented to e-government environments seems to be a promising path. Yet, the deployment of newly proposed schemas introduces the challenges of compatibility, up keeping, evaluating and updating procedures. In addition to that, depending on the environment, additional data interchange formats could also be explored, especially since XML is regarded to have significant consequences on data transmission rates and performance compared to JSON [11].

One drawback of the approach is the workload and computational cost introduced to the central portal since for every electronic service request, the PCA is obliged to perform a root back retrieval of all referenced policy documents. Similarly to X.509-based PKIs as discussed in [12–16], which are generally hierarchical and centralized, it can be resolved if actual policy documents are retained at the PCA for certain time periods, based on service request. In the event of a change in a higher level privacy policy document, PCA will be informed to rescind all related documents. Similarly, in the event of a central government organizational restructure, the PCA will also have to retract all affected documents. However, this would also be the case is the non-hierarchical approach presented in [8].

4. Case Study

In order to demonstrate the applicability of the proposed approach in modern e-Government environments, a case study, where privacy policy hierarchy is incorporated into the Greek e-Government environment, is presented. The Greek e-government interoperability framework (Greek e-GIF) was first proposed in 2007 [17,18], based on worldwide best practices along with the specific needs and restrictions set by the underlying legal and regulatory framework. The main objective of this framework is the support of common authentication and registration mechanisms for accessing all the electronic services offered. This is realized through a central portal, named "Ermis" (http://www.ermis.gov.gr/), which operates as a one-stop shop and provides to Greek citizens a common interface for all electronic services offered by SPs of the public sector. The framework's main characteristics are uniform registration and authentication procedures for every service provider, implemented by the Ermis Portal, and classification of services to levels of trust depending on the required level of identity assurance and data protection.

4.1. Annual Vehicle Tax Electronic Service

Each car owner is required to pay an *Annual Vehicle Tax* (AVT) for every vehicle registered under his ownership. Overall tax amount is calculated based on vehicle's CO_2 emissions, engine size, and production date and is paid separately from annual income tax. Electronic service is provided by the General Secretary of Information Systems (GSIS) which operates under the authority of the Ministerial Department of Finance. The applicable hierarchy is presented below in Figure 3. For the successful completion of the electronic service user is required to submit her National Taxation Number along with a vehicle's license plate. GSIS validates data accuracy and generates a receipt which contains owners'

first and last name, vehicle's license plate, and the tax amount to be paid along to a unique payment identifier, which will be utilized by the bank institution, where payment will be made.

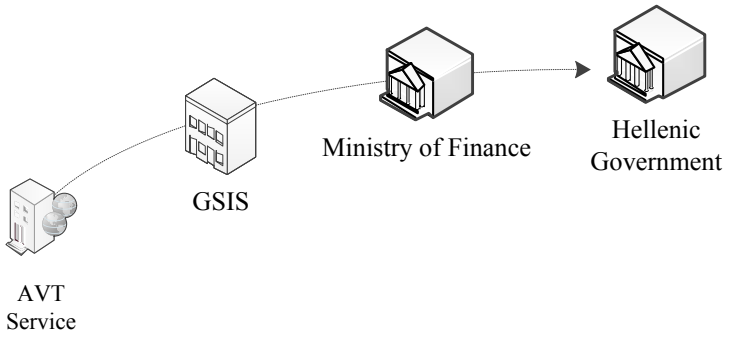

Figure 3. Case Study Privacy Policies Hierarchy.

4.2. Privacy Policies

For the purposes of this case study, the necessary privacy policy documents have been prepared in a simple XML schema, based on the attributes and elements introduced in [8] (removed for review). This schema consists of simple elements along with some attributes, in an attempt to describe a strict privacy policy in a structured yet easy way. Documents presented at this section contain information only for the personal identifiers and data required for the successful completion of AVT electronic service. Each document consists of a root *Privacy_Policy* element, a *Policy_ID* element, which includes a unique policy document identifier, based on which the referencing from lower levels is achieved, along to a *Data* element. The latter is divided into two sub-elements, *Personal_Identifiers* and *Personal_Data*, based on data type.

The Hellenic Government Privacy Policy, presented at Table 1 below, states that *National Taxation Identifier (line A.7)*, *License Plate* information *(line A.14)*, and *First and Last name (line A.19)* must be processed as confidential data and can be stored by service providers. There is no reference to how long SPs are allowed to store this data and therefore this is subject to be specified by lower level policy documents. However abstract this policy may seem, these are the fundamental obligations that are imposed and must be endorsed by all underlying ministerial departments and SPs.

Table 2 below presents the privacy policy of the Ministry of Finance. For all data types contained within the document there is a clear reference to a policy document with *P_Ref_ID = "001" (lines B.7, B.13,* and *B.17)* with regards to the Hellenic Government Privacy Policy. Statements regarding data processing remain the same and three new specifications are introduced; At line *B.8* it is stated that National Taxation Identifier can processed for Identification purposes, at lines *B.9* and *B.15* the corresponding data can be retained for 365 days and at *B.19* first and last names can be retained for 90 days. The lack of <*Transmitted*> elements means that what imposed by referenced document is still in effect.

Table 1. Hellenic Government Privacy Policy.

Line	Privacy Policy Content
A.1	<Privacy_Policy>
A.2	<Policy_ID="001">
A.3	<Description> Hellenic Government Privacy Policy </Description>
A.4	</Policy_ID>
A.5	<Data>
A.6	<Personal_Identifiers>
A.7	<Identifier_ID="26"> National Taxation Identifier (AFM)
A.8	<Processed="Confidential"> </Processed>
A.9	<Storage="Yes"> </Storage>
A.10	<Transmitted="Yes" </Transmitted>
A.11	</Identifier_ID>
A.12	</Personal_Identifiers>
A.13	<Personal_Data>
A.14	<Data_ID="873"> License Plate
A.15	<Processed="Confidential"> </Processed>
A.16	<Storage="Yes"> </Storage>
A.17	<Transmitted="Yes" </Transmitted>
A.18	</Data_ID>
A.19	<Data_ID="32"> First and Last Name
A.20	<Processed="Confidential"> </Processed>
A.21	<Storage="Yes"> </Storage>
A.22	<Transmitted="Yes" </Transmitted>
A.23	</Data_ID>
A.24	</Personal_Data>
A.25	</Data>
A.26	</Privacy_Policy>

Table 2. Ministry of Finance Privacy Policy.

Line	Privacy Policy Content
B.1	<Privacy_Policy>
B.2	<Policy_ID="024">
B.3	<Description> Ministry of Finance Privacy Policy </Description>
B.4	</Policy_ID>
B.5	<Data>
B.6	<Personal_Identifiers>
B.7	<Identifier_ID="26" P_Ref_ID="001"> National Taxation Identifier (AFM)
B.8	<Processed="Confidential"> Identification </Processed>
B.9	<Storage="Yes" Retention="365"> </Storage>
B.10	</Identifier_ID>
B.11	</Personal_Identifiers>
B.12	<Personal_Data>
B.13	<Data_ID="873" P_Ref_ID ="001"> License Plate
B.14	<Processed="Confidential"> </Processed>
B.15	<Storage="Yes" Retention ="365"> </Storage>

Table 2. *Cont.*

Line	Privacy Policy Content
B.16	</Data_ID>
B.17	<Data_ID="32" p_Ref_ID="001"> First and Last Name
B.18	<Processed="Confidential"> </Processed>
B.19	<Storage="Yes" Retention="90"> </Storage>
B.20	</Data_ID>
B.21	</Personal_Data>
B.22	</Data>
B.23	</Privacy_Policy>

The privacy policy document presented at Table 3 below is issued by General Secretary of Information Systems (GSIS). Again, there is a clear reference to a policy document with *P_Ref_ID = "024" (lines C.7, C.12,* and *C.13)* which regards Ministry of Finance Privacy Policy. The only addition identified at this document regards the retention time for National Taxation Identifier is reduced to 180 days (*line C.8)*.

Table 3. GSIS Privacy Policy.

Line	Privacy Policy Content
C.1	<Privacy_Policy>
C.2	<Policy_ID="587">
C.3	<Description> GSIS Privacy Policy </Description>
C.4	</Policy_ID>
C.5	<Data>
C.6	<Personal_Identifiers>
C.7	<Identifier_ID="26" P_Ref_ID="024"> National Taxation Identifier (AFM)
C.8	<Storage="Yes" Retention="180"></Storage>
C.9	</Identifier_ID>
C.10	</Personal_Identifiers>
C.11	<Personal_Data>
C.12	<Data_ID="873" P_Ref_ID ="024"> License Plate </Data_ID>
C.13	<Data_ID="32" p_Ref_ID="024"> First and Last Name </Data_ID>
C.14	</Personal_Data>
C.15	</Data>
C.16	</Privacy_Policy>

The privacy policy document presented below at Table 4 refers at Annual Vehicle Tax electronic service. Compared to previously discussed documents, two newly introduced elements, <*Service_Provider*> and <*Electronic_Service*> can be identified (*lines D.3* and *D.5*). Since this document regards an electronic service and not a ministerial department, their inclusion is required to make apparent its scope and the SP that offers it. Within this document, the National Taxation Identifier (AFM) is prohibited from being transmitted (*line D.12),* License plate information is processed for identification purposes (*line D.17*) and will be retained for 90 days *(line D.18*), while name will be also used for identification purposes *(line D.22)* and will not be stored and retained *(line D.23)*.

Table 4. AVT Service Privacy Policy.

Line	Privacy Policy Content
D.1	<Privacy_Policy>
D.2	<Policy_ID="1038">
D.3	<Service_Provider> General Secretary of Information Systems (GSIS)
D.4	</Service_Provider>
D.5	<Electronic_Service> Annual Vehicle Tax </Electronic_Service>
D.6	<Description> Privacy Policy for Annual Vehicle Tax Electronic Service
D.7	</Description>
D.8	</Policy_ID>
D.9	<Data>
D.10	<Personal_Identifiers>
D.11	<Identifier_ID="26" P_Ref_ID="587"> National Taxation Identifier (AFM)
D.12	<Transmitted="No" </Transmitted>
D.13	</Identifier_ID>
D.14	</Personal_Identifiers>
D.15	<Personal_Data>
D.16	<Data_ID="873" P_Ref_ID ="587"> License Plate
D.17	<Processed="Confidential"> Identification </Processed>
D.18	<Storage="Yes" Retention="90"> </Storage>
D.19	</Data_ID>
D.20	<Transmitted="Yes" </Transmitted>
D.21	<Data_ID="32" p_Ref_ID="587"> First and Last Name
D.22	<Processed="Confidential"> Identification </Processed>
D.23	<Storage="No" Retention="0"> </Storage>
D.24	</Data_ID>
D.25	</Personal_Data>
D.26	</Data>
D.27	</Privacy_Policy>

Table 5. Composition of AVT Service Privacy Policy Document.

Identifier	***AVT***					***GSIS***					***Ministry of Finance***					***Central Government***				
	Storage	***Process***	***Purpose***	***Retention***	***Transmit***	***Storage***	***Process***	***Purpose***	***Retention***	***Transmit***	***Storage***	***Process***	***Purpose***	***Retention***	***Transmit***	***Storage***	***Process***	***Purpose***	***Retention***	***Transmit***
AFM	►	►	►	►	No	►	►	►	180	►	►	►	*I*	365	►	Yes	*C*	◄	◄	Yes
License Plate	►	►	*I*	90	►	►	►	◄	►	►	►	►	◄	365	►	Yes	*C*	◄	◄	Yes
Name	No	►	*I*	►	►	►	►	◄	►	►	►	►	◄	90	►	Yes	*C*	◄	◄	Yes

I : Identification; C: Confidential; ►: Policy refers to a higher level Policy; ◄: Policy refers to a lower level Policy.

Table 5 below summarizes the specifications imposed by each policy document and presents the composition of AVT electronic service privacy policy document. From the inclusion of arrow indicators, it is apparent where each element and attribute is specified, (re)specified, and referenced. Such a representation could be easily implemented in uniform interface operated by PCA that would allow for

easier and effective compliance control. The Compliance Support Tool (CST) accesses privacy policy storage repository, retrieves the XML documents, creates a schematic representation of the aforementioned information and is able not only to audit compliance but also to inform the operator of the results through appropriate messages and color-coding, similar to [9].

4.3. Non-Hierarchical Privacy Policies

An identified benefit from the deployment of the hierarchy approach, mentioned at Section 3.3, regarded the length reduction of the derived privacy policy documents, apart from ensuring compliance with the underlying legal and regulatory framework. Within the context of the case study and without applying the hierarchy scheme, AVT electronic would comprise of additional three lines and 100 ASCII characters, as depicted in Table 6 below. However insignificant this reduction may seem in one document, when applied to all respective documents, from electronic services, service providers, and ministerial departments, it is expected to produce more impressive results in terms of absolute numbers and workload.

Table 6. AVT Service Non-Hierarchical Privacy Policy.

Line	Privacy Policy Content
D.1	<Privacy_Policy>
D.2	<Policy_ID="1038">
D.3	<Service_Provider> General Secretary of Information Systems (GSIS)
D.4	</Service_Provider>
D.5	<Electronic_Service> Annual Vehicle Tax </Electronic_Service>
D.6	<Description> Privacy Policy for Annual Vehicle Tax Electronic
D.7	Service </Description>
D.8	</Policy_ID>
D.9	<Data>
D.10	<Personal_Identifiers>
D.11	<Identifier_ID="26"> National Taxation Identifier (AFM)
D.12	<Processed="Confidential"> Identification </Processed>
D.13	<Storage="Yes" Retention="90"> </Storage>
D.14	<Transmitted="Yes" </Transmitted>
D.15	</Identifier_ID>
D.16	</Personal_Identifiers>
D.17	<Personal_Data>
D.18	<Data_ID="873"> License Plate
D.19	<Processed="Confidential"> Identification </Processed>
D.20	<Storage="Yes" Retention="90"> </Storage>
D.21	<Transmitted="Yes" </Transmitted>
D.22	</Data_ID>
D.23	<Transmitted="Yes" </Transmitted>
D.24	<Data_ID="32"> First and Last Name
D.25	<Processed="Confidential"> Identification </Processed>
D.26	<Storage="No" Retention="0"> </Storage>
D.27	</Data_ID>

Table 6. *Cont.*

Line	Privacy Policy Content
D.28	</Personal_Data>
D.29	</Data>
D.30	</Privacy_Policy>

5. Related Works

XML schemas have been widely adopted by e-Government environments and their corresponding interoperability frameworks (e-GIFs) as key components in exchanging information and offering improved user oriented electronic services [19]. Even if the notion of hierarchy in XML documents for modeling privacy policies or privacy preferences has been explored in certain contexts, to the best of our knowledge it has not yet been considered for privacy preservation in e-Government environments. In [20] a user's preferences model was proposed based on the assumption that each element of personal data could be represented by a hierarchical taxonomy of values and categories. These hierarchies were tree-shaped and they could be represented using a directed acyclic graph. Graph nodes represent values or categories and an edge from one node *(a)* to another *(b)* represents that *(b)* is contained within category *(a)*. A similar approach was proposed by [10] and pertained a hierarchical approach to the specification of privacy preferences in e-Health environments. The defined hierarchies are inherent to each dimension of privacy preferences are introduced alongside methods that simplify users' tasks in specifying their privacy preferences. Additionally, guidelines for resolving potential conflicts are also introduced based on meta-policies, and representation and implementation of hierarchical authorizations, using privacy metadata of Hippocratic databases are also presented. Regarding the implementation, a snowflake metadata schema is deployed to record the authorizations which are capable of substituting existing metadata when necessary. Even from the limited relevant publications, it is apparent that the notion of hierarchy can be applied in contexts where representation of subordinate and superordinate levels can be made.

6. Conclusions

The success of e-Government initiatives depends not only on the modernization of front office but also on the streamlining, (re)organizing, and support of the back-office processes. Acceptance and further evolvement are affected by the gap and inconsistencies that exist between the perspective of policy makers and public administrations' managers on the one hand and the technical realization of e-Government on the other hand [21,22]. In this paper, a simple, yet effective, approach for the formulation of coherent and accurate privacy policies has been proposed, while preserving compliance with underlying legal and regulatory framework. Through the exploitation of existing governmental hierarchies, the proposed multitier approach is able to support diverge data needs and processing requests imposed by service providers. A case study has also been presented, as a testbed of the hierarchical scheme along to a notion of a Compliance Support Tool that will be able to support documents auditing and diagrammatic compliance representation. The incorporation of this approach into e-Government environments will reduce the administrative workload, imposed by the inclusion of privacy policy documents, promote the implementation and provision of user-centric and data privacy aware electronic services.

Author Contributions

P.D. and S.G. conceived the formulation of privacy policy documents through the exploitation of existing governmental hierarchies. C.K. and C.L. conceived the inclusion of specific rules and referencing XML elements which enable the formulation of light-weight documents.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Belanger, F.; Hiller, J. A Framework for e-Government: Privacy Implications. *Bus. Process Manag. J.* **2006**, *12*, 48–60.
2. McRobb, S.; Stahl, B. Privacy as a shared feature of the e-phenomenon: A comparison of privacy policies in e-government, e-commerce and e-teaching. *Int. J. Inf. Technol. Manag.* **2007**, *6*, 232–249.
3. Carter, L.; McBride, A. Information Privacy Concerns and e-Government: A Research Agenda. *Transform. Gov. People Process Policy* **2010**, *4*, 10–13.
4. Vrakas, N.; Kalloniations, C.; Tsohou, A.; Lambrinoudakis, C. Privacy Requirements Engineering for Trustworthy e-Government Services. In Proceedings of the 3rd International Conference on Trust and Trustworthy Computing, Berlin, Germany, 21–23 June 2010; Springer Verlang: Berlin, Germany, 2010; pp. 298–307.
5. Bussard, L.; Pinsdorf, U. Abstract Privacy Policy Framework: Addressing Privacy Problems in SOA. In Proceeingds of the IFIP WG 11.4 International Workshop, iNetSec, Lucerne, Switzerland, 9 June 2011; Springer LNCS: Berlin, Germany, 2012; pp. 104–118.
6. Oyomno, W.; Jäppinen, P.; Kerttula, E. Privacy Policy Enforcement for Ambient Ubiquitous Services. In Proceedings of the First International Joint Conference on Ambient Intelligence (AML 2010), Malaga, Spain, 10–12 November 2010; Springer LNCS: Berlin, Germany, 2010; pp. 265–269.
7. Lee, K.; Lee, J.; Chun, M. Incorporating Privacy Policy into an Anonymity-Based Privacy-Preserving ID-Based Service Platform. In Proceedings of the 9th International Conference in Knowledge-Based Intelligent Information and Engineering Systems (KES 2005), Melbourne, Australia, 14–16 September 2005; Springer LNCS: Berlin, Germany, 2005; pp.1028–1035.
8. Drogkaris, P.; Gritzalis, S.; Lambrinoudakis, C. Employing Privacy Policies and Preferences in Modern e-Government Environments. *Int. J. Electron. Gov.* **2013**, *6*, 101–116.
9. Drogkaris, P.; Gritzalis, A.; Lambrinoudakis, C. Empowering Users to Specify and Manage their Privacy Preferences in e-Government Environment. In Proceedings of the 3rd International Conference on Electronic Government and the Information Systems Perspective (EGOVIS 2014), Munich, Germany,1-3 September 2014; Springer LNCS: Cham, Switzerland, 2014; pp. 237–245.
10. Hong, Y.; Lu, S.; Liu, Q.; Wang, L.; Dssouli, R. A hierarchical approach to the specification of privacy preferences. In Proceedings of the 4th International Conference on Innovations in Information Technology (IIT'07), Dubai, United Arab Emirates, 18–20 November 2007.

11. Nurseitov, N.; Paulson, M.; Reynolds, R.; XIzurieta, C. Comparison of JSON and XML Data Interchange Formats: A Case Study. In Proceedings of the ISCA 22nd International Conference on Computer Applications in Industry and Engineering, San Francisco, CA, UFA, 4–6 November 2009.
12. Zhiwei, G.; Yingxin, H.; Kai, L. CPTIAS: A new fast PKI authentication scheme based on certificate path trust index. *J. Ambient Intell. Humaniz. Comput.* **2015**, *6*, 1–11.
13. Zhao, S.; Aggarwal, A.; Kent, R. PKI-Based Authentication Mechanisms in Grid Systems. In Proceedings of the International Conference on Networking, Architecture, and Storage (NAS 2007), Guilin, China, 29–31 July 2007; pp. 83–90.
14. Satizábal, C.; Forné, J.; Hernández-Serrano, J.; Pegueroles, J. Building Hierarchical Public Key Infrastructures in Mobile Ad-Hoc Networks. In Proceedings of the Second International Conference on Mobile Ad-hoc and Sensor Networks (MSN 2006), Hong Kong, China, 13–15 December 2006; Springer LNCS: Berlin, Germany, 2006; pp. 485–496.
15. Zhao, M.; Smith, S. Modeling and Evaluation of Certification Path Discovery in the Emerging Global PKI. In Proceedings of the Third European PKI Workshop: Theory and Practice, EuroPKI 2006, Turin, Italy, 19–20 June 2006; Springer LNCS: Berlin, Germany, 2006; pp.16–30.
16. Lambrinoudakis, C.; Gritzalis, S.; Dridi, F.; Pernul, G. Security requirements for e-government services: A methodological approach for developing a common PKI-based security policy. *Comput. Commun.* **2003**, *26*, 1873–1883.
17. Charalabidis, Y.; Lampathaki, F.; Sarantis, D.; Mouzakitis, S.; Gionis, G.; Koussouris, S.; Ntanos, C.; Tsiakaliaris, C.; Tountopoulos, V.; Askounis, D.; *et al*. The Greek electronic government interoperability framework: Standards and infrastructures for one stop service provision. In Proceedings of the Panhellenic Conference on Informatics (PCI'08), Samos, Greece, 28–30 August 2008; pp. 66–70.
18. Drogkaris, P.; Geneiatakis, D.; Gritzalis, S.; Lambrinoudakis, C.; Mitrou, L. Towards an Enhanced Authentication Framework for eGovernment Services: The Greek Case. In Proceedings of the 7th International Conference on Electronic Government (EGOV'08), Torino, Italy, 1–5 September 2008; Trauner Verlag: Linz, Austria, 2008; pp. 189–196.
19. Janssen, M.; Charalabibis, Y.; Kuk, G.; Cresswell, T. E-government Interoperability, Infrastructure and Architecture: State-of-the-art and Challenges. *J. Theor. Appl. Electron. Commer. Res.* **2001**, *6*, 1–8.
20. Irwin, K.; Yu, T. Determining user privacy preferences by asking the right questions: An automated approach. In Proceedings of the ACM Workshop on Privacy in the Electronic Society, Alexandria, USA, 7–10 November 2005; pp. 47–50.
21. Apostolou, D.; Stojanovic, L.; Lobo, T.; Miró, J.; Papadakis, A. Configuring e-government service using ontologies. In Proceedings of the 5th IFIP Conference e-Commerce, e-Business, and e-Government (I3E'2005), Poznan, Poland, 28–30 October 2005; pp. 141–155.

22. Magoutas, B.; Halaris, C.; Mentzas, G. An ontology for the multi-perspective evaluation of quality in e-government services. In Proceedings of the 6th International Conference on e-Government, EGOV 2007, Regensburg, Germany, 3–7 September 2007; pp. 318–329.