Compliant and secure websites for the Greek Libraries Network of the National Library of Greece and each library-member of this Network in consideration of internet security and GDPR

Konstantinos Vavousis,[1] Marinos Papadopoulos,[2] Michalis Gerolimos[3] & Christos Xenakis[4]

[1]PhD cand, IT Security Professional in the private sector (TRUST-IT Ltd.); secnews.gr Editor-in-Chief
2Phd, Attorney-at-Law, Legal Counsel of the National Library of Greece
[3]PhD, e-Resources & Systems Librarian at the National Library of Greece
[4]Professor, University of Piraeus, Department of Digital Systems; System Security Laboratory

Abstract: The application of the General Data Protection Regulation (GDPR) regarding the operation of websites is considered of vital importance, especially to organizations within the European Union. GDPR is a useful tool, which, among other requirements, mandates the adoption of privacy-by-design and advanced IT security mechanisms in place. Considering its requirements, this paper analyses their implementation with regard to applied Internet Security solutions for the websites of the Greek Libraries Network of the National Library of Greece. While the GDPR offers a minimum set of technical Internet Security means to be taken into consideration by companies and organizations Europe-wide to achieve GDPR compliance, hereby we aim to highlight the adaptation of strong and proper security mechanisms that will not only set libraries-members of the Greek Libraries Network of the National Library of Greece compliant with GDPR, but also maintain them strong and secure against most threats targeting websites to both internal and external cyber security threats.

Keywords: IT security, website security, security mechanism, GDPR, privacy by design, privacy by default, appropriate technical and organizational measures, National Library of Greece

1. Security by design and by default for the Greek Libraries Network of NLG

The General Data Protection Regulation 2016/679/EU (hereinafter, GDPR) offers a digital environment for companies and organizations where they can better trace, secure and handle data within the IT infrastructure and beyond. In this context, GDPR requires strong security mechanisms to be in place in order

Received: 6.8.2020 Accepted: 8.9.2020 ISSN 2241-1925

to safeguard the data under consideration. All libraries, public and private need to comply with GDPR requirements for personal data protection. Hence, powerful security mechanisms should be adopted for the adequate protection of personal data and/or special categories of data processed through their IT infrastructure. The latest trends in cyber security have embedded technologies with enhanced mechanisms for better results, including machine learning and big data analytics on network security solutions (Kantarcioglu, M., et al, 2016). In this paper, we analyze the basic components that the Greek Libraries Network that the National Library of Greece supports and coordinates (hereinafter, NLG Network), should implement and properly configure, in order for its websites to become compliant with the relevant legislation and resilient to cyber-attacks.

The Greek Libraries Network of the National Library of Greece has been established to help Academic, Research, Public, Municipal, and School libraries to develop and evolve the services they offer to their public. It aspires to be the means of exchanging information, knowledge and professional communication between libraries, to undertake training program initiatives for library staff, to plan and organize national and international activities, such as campaigns or conferences, to aspire its members in the use of professional tools and standards, and to provide ongoing support to libraries which are members of the Greek Libraries Network of NLG. It provides leadership and consultant services to all its member (e.g. applying standards and implementing new). In the organizational field, the Greek Libraries Network of NLG offers library support by creating a union catalog, providing Integrated Library Systems (ILS) and defending the political, economic and social positions of libraries so that in the future libraries will be social hubs for every community they serve. It aims to conduct research and surveys to serve its purpose (e.g. level of development of library services in the country, benchmarking based on other countries data and metrics). Also, the Greek Libraries Network of NLG has a key-role in the preparation of integrated funded programs either national or international that aim at the development of libraries in the Network.[1] NLG and all member-libraries of the Greek Libraries Network set up their collaboration through the Greek Libraries Network of NLG with the aim to apply Network-wide innovative methods of developing services and programs, such as Information Literacy, that each library could not implement on its own and jointly and radically comply to the requirements of Library Science in the modern landscape in Greece today, which of course includes the application of GDPR requirements in the operation of libraries. For all the above reasons, the Greek Libraries Network, has a pivot role to map and organize the Greek libraries eco-system and establish an annual survey documenting resources, services, and developments.

[1] Dr. Philippos Tsimpoglou, General Director of the National Library of Greece, in Network of the Greek Libraries of the National Library of Greece, available at URL: https://network.nlg.gr/liga-logia/ [last check, Aug.12, 2020].

Under GDPR, following a data breach, the data controller has the legal obligation to notify the supervisory authority in 72 hours maximum.[2] This way, apart from any actual data losses, organizations run the risk of harming their reputation and even face the financial burden of GDPR fines. Due to the high costs of data breaches (IBM Security, 2017; IBM Security, 2019), *security by design* and *security by default* are highly recommended to for-profit and non-profit organizations such as most libraries of the Greek Libraries Network of NLG to assist them in minimizing investments for their IT security infrastructure and protecting their data. Once these strong security mechanisms are in place to cover a potentially wide range of data protection measures and to ensure data minimization and confidentiality the level of security of an IT infrastructure which is used for the processing of personal data will be enhanced and the organization will minimize the required response to a security breach.

Therefore, in order for the Greek Libraries Network of NLG to enhance the security of its websites and comply with the GDPR requirement for processing of data in a manner *that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures*[3] it needs to maximize its Information Technology security posture through proper "*technical or organizational measures*". By the term "*technical or organizational measures*", mentioned in Regulation 2016/679/EU, the legislator refers to the functions, processes, controls, systems, procedures and policies that are in place, to protect and safeguard the critical data and private information that an organization holds.

GDPR's article 25[4] mandates the requirement for data protection *by design* and *by default*, leveraging on *technical and organizational measures* taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing. The controller is mandated both at the time of the determination of the means for processing and at the time of the processing itself, to implement *appropriate technical and organizational measures*, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of GDPR and protect the rights of

[2] Art.33(1) of GDPR, according to which *In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.*

[3] Art.5(1)(f) of GDPR.

[4] See art.25(1) & (2) of GDPR.

data subjects. The controller is obliged to implement *appropriate technical and organizational measures* for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. *Appropriate technical and organizational measures* must ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Clarification upon the notion of *appropriate technical and organizational measures* is provided through Recital 78 of GDPR, according to which *such measures could consist, inter alia, of minimizing the processing of personal data, pseudonymizing personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.* Technical and organizational measures must be taken *to ensure that the requirements of this Regulation* [a.k.a. GDPR] *are met;* technical and organizational measures consist of policies and measures which *meet in particular the principles of data protection by design and data protection by default.* The principles of data protection *by design* and *by default* must be taken into consideration in the context of public tenders, too.[5] Therefore, any attempt of Greek Libraries Network of NLG to apply for integrated funded programs either national or international that aim at the compliance of libraries in the Network to the requirements of GDPR must consider data protection *by design* and *by default.*

In consideration of the principles of data protection by design and by default *when developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.*

Recital 46 of the Data Protection Directive 95/46/EC (hereinafter, DPD) mentioned the need to take *appropriate technical and organizational measures* for the protection of data-subjects' rights and freedoms *both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing.* Since the application of DPD in personal data protection the notion of *appropriate technical and organizational measures* is aligned with measures that can ensure an appropriate level of security, taking

[5] See Recital 78 of GDPR.

into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected. The Court of Justice of the European Union (hereinafter, CJEU) has yet to rule on the subject matter of article 25 of GDPR. However, it has strongly ruled through joined cases C-293/12 and C-594/12 that the adoption of *technical and organizational measures* ensures that personal data are given effective protection against the risk of abuse and against any unlawful access and use.[6] Thus, CJEU is in line with the application of article 25 of GDPR and article 25 is in line with the rulings of the CJEU even before the pass of GDPR; the CJEU has, also, ruled indirectly in line with the requirements of article 25 of GDPR in some of its decisions dealing with internet mechanisms, such as the decision in Case C-131/12 in which the CJEU ruled that Google and other search engine operators must reconfigure their systems so that they are more privacy friendly.[7]

The purpose of article 25 of GDPR is to impose a qualified duty on controllers to put in place technical and organizational measures that are designed to implement effectively the data protection principles of GDPR. Article 25 of GDPR prevents controllers from using technologies that collect more personal data than are strictly necessary for technological functionality or that leak personal data to outsiders. The wording of GDPR expressly applies its ruling not just at the time of the processing but also beforehand when the controller determines the means for the processing. The measures referred to in article 25 of GDPR are not just *technical* but also *organizational*, which means that they embrace not simply the design and operation of software and hardware, but they extend to business strategies and other organizational measures which contribute to the application of the GDPR principles listed in article 5 of GDPR regarding data processing and privacy protection (Kuner, C., et al, 2020).

Article 25 addresses the notions of *privacy by design* and *privacy by default*, as well. Both, *privacy by design* and *privacy by default* are to be taken by controllers which are the entities to determine the purposes and the means of processing of personal data.[8] *Privacy by design* is addressed in article 25(1) of GDPR while *privacy by default* is addressed in article 25(2) of GDPR. Article

[6] See joined cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*, Judgement of the Court, paras.5, 7, 40, 66, 67, available at URL: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=10218830 [last check, Aug.12, 2020].

[7] See Case C-131/12, *Google Spain and Google*, available at URL: http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&lgrec=el&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-131%252F12&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=en&avg=&cid=10219757 [last check, Aug.12, 2020].

[8] See art.4(7) of GDPR.

25(1) of GDPR formulates the design stage in terms of when the controller assumes its status by the time of determination of the means for processing.

Both *privacy by design* and *privacy by default* impose on library-members of the Greek Libraries Network of NLG the obligation to meticulously select *technical* and *organizational* measures that are privacy-friendly and can ensure effective protection against the risk of abuse and against any unlawful access and use of personal data. Having that in mind, where does this selection start from?

One way to begin would be to conduct vulnerability scans and penetration tests on the website and its components, including hosting servers and service providers checks. Endpoint risk assessments could assist further to discover loopholes in all processing activities, identify high risks regarding personal data and the effective reparative measures.

Regardless of possible future changes in the IT support system of the Greek Libraries Network of NLG, a resilient IT security infrastructure for the websites of the Network-members should consider the security and regulatory requirements described in the current article for coping with most common website cyber security threats, to which we will now turn to refer.

2. Common website Cyber Security Threats

In order to understand the needs of an organization and conduct the websites of the Greek Libraries Network of NLG compliant and resilient to cyber security threats, we need to thoroughly understand the online threats that might affect the web infrastructure, including the website of an organization. As described on the OWASP Top Ten security risks to web applications of The Open Web Application Security Project[9], the most common threats that must be taken under consideration include but may not be limited to the following: Injections, Broken Authentication, Sensitive Data Exposure, XML External Entities (XXE), Broken Access Control, Security Misconfiguration, Cross-Site Scripting XSS, Insecure Deserialization, Using Components with Known Vulnerabilities and Insufficient Logging & Monitoring.

Regarding these Cyber Security Threats:
Injection. Injection flaws are a class of security vulnerability such as SQL, NoSQL, OS, and LDAP injection that allows a user to "*break out*" of the web application context. These vulnerabilities may exist in the case of uncontrolled data enter an interpreter as part of a query or command. In the case of a website or a web application that take user input into a back-end database, shell command, or operating system call, the application may be susceptible to an injection vulnerability (Abdul Bashah Mat, A. et al, 2011).

[9] See the OWASP Top Ten about the most critical security risks to web applications of the Open Web Application Security Project at URL: https://owasp.org/www-project-top-ten/ [last check, Aug.12, 2020].

Broken Authentication. Regarding web applications, the authentication procedure is considered as "*broken*" when a potential malicious user is able to compromise passwords, keys or session tokens, user data and further information that my provide more details about the users' identity. Broken authentication attacks aim to achieve unauthorized access to active accounts giving the malicious user the same privileges as the legitimate user by manipulating the improper implementation of application functions related to authentication and session management (Maruf, H., et al, 2018).

Sensitive Data Exposure. This kind of cyber threat may occur in a case of a web application which does not properly secure sensitive data that may include passwords, session tokens, financial data and even private health data and more. The administrators and developers of web applications should protect properly all sensitive data, including the aforementioned categories, in order to prevent unauthorized accesses and data losses from malicious users. (Sue, X., et al, 2015)

XML External Entities (XXE). XML external entity injection (hereinafter, XXE) is a flaw targeting web applications, which permits malicious users to manipulate with a web application processing of XML data. By XXE, a potential malicious user is able to disclose internal files of the web application and to interact with any backend or external systems that the web application itself is able to access. Furthermore, an attacker may be able to view internal file shares, conduct internal port scanning, conduct remote code execution, perform Server-Side Request Forgery (SSRF) attacks and perform denial of service attacks (Osincev, A., et al, 2019).

Broken Access Control is another common vulnerability that occurs when testing the security of a web application, which in most cases results to unauthorized access, information disclosure of sensitive files and data, modification of access rights, and changing or corruption of information and data. Broken Access Control, is a security flaw that may occur due to lack of proper security methodology adopted by developers in the procedure of creating a web application during coding or insecure implementation of authentication and authorization mechanisms (Hassan, M., et al, 2018).

Security misconfiguration threats are the most common problems regarding the security of web applications. They occur when a web application has not proper configuration regarding its source code or the infrastructure that is hosted and may exist in software components or subsystems; it may lead to the exploitation of other vulnerabilities that target any part of the application stack. For the avoidance of any security misconfiguration it is strongly recommended to harden all the components of a web application including operating systems, frameworks and libraries, upgrading each part especially with security patches whenever is needed (Eshete, B., et al, 2011).

Cross-site scripting (hereinafter, XSS) is one of the most common web application security vulnerabilities that is found during website security tests. XSS vulnerabilities provide the ability to a malicious user to inject untrusted content or client-side scripts into web pages without proper data validation techniques or escaping. The manipulation of an XSS vulnerability enables a malicious user to run unauthorized scripts in a victim's web browser leading in user session hijacking, website deface or redirection to malicious websites. XSS flaws impact may differ according to the sensitivity of the data handled by the vulnerable application and the nature of any security mitigation implemented by the administrator of the web application (Gupta, S, et al, 2015).

Insecure deserialization is a security flaw where malicious content often leads to remote code execution, denial of service attacks (DoS attack), replay attacks, injection attacks, privilege escalation attacks, authentication bypass or manipulation of the logic the web application operates (Dehalwar, V., at al, 2017).

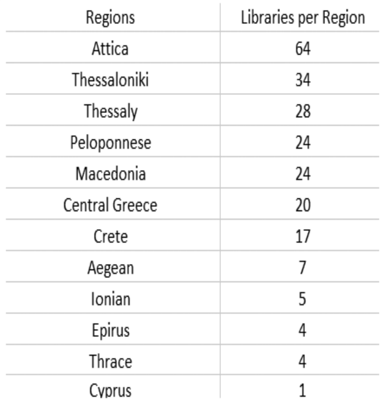
The use of application components that include known vulnerabilities is another common security flaw of a web application. It should be underlined that libraries, frameworks, and other software modules, have the same permissions as the web application runs. In case of exploitation of a component with known security flaws, this may lead to further information leakage or even manipulation of the web server where the web application is hosted. Web applications and APIs that include components with known security flaws may be targeted by malicious users and lead to serious security incidents.

Insufficient Logging & Monitoring. One of the major flaws of a web application is the lack of sufficient logging and monitoring. In a case of an effective security incident, without proper logging and monitoring, the web applications' administrator will not be alerted, allowing the malicious user to continue the attack uninterrupted apart from the web application, to the whole infrastructure hosting the application. Typically, for a security incident to be identified, it takes approximately 200 days based on 2019 Cost of a Data Breach Study conducted by IBM (IBM, 2019) and it is detected by external parties rather than inside procedures or internal security teams (Leite G. S., et al, 2019).

3. The situation currently of websites of library-members of the Greek Libraries Network of NLG

In order to depict the current situation of the websites of library-members of the Greek Libraries Network of NLG, we have analyzed for every library-member of said Network the existence of its website—if any, its social media presence, the existence—if any—of an updated Privacy Policy with regard to GDPR and the use of a Secure Socket Layer (SSL) certificate, regarding the security of the communication between a user and the library's website. The Greek Libraries

Network of NLG consists of 234 library-members in total, of which 233 libraries are based in Greece and 1 is based in Cyprus.



Regions	Libraries per Region
Attica	64
Thessaloniki	34
Thessaly	28
Peloponnese	24
Macedonia	24
Central Greece	20
Crete	17
Aegean	7
Ionian	5
Epirus	4
Thrace	4
Cyprus	1

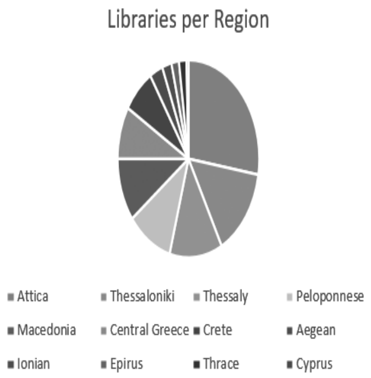
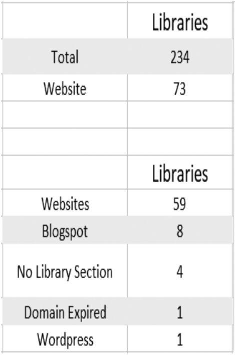


Table 1. The Greek Libraries Network of the National Library of Greece consists of 234 Libraries. Separation per region.

The distribution of the Greek Libraries Network of NLG as shown in table 1, includes 7 libraries in the region of Aegean, 4 libraries in the region of Epirus, 28 libraries in the region of Thessaly, 34 libraries in the region of Thessaloniki, 17 libraries in the region of Crete, 24 libraries in the region of Peloponnese, 64 libraries in the region of Attica, 4 libraries in the region of Thrace, 5 libraries in the region of the Ionian sea, 20 libraries in Central Greece, 1 in Cyprus and 26 in the region of Macedonia.



	Libraries
Total	234
Website	73
	Libraries
Websites	59
Blogspot	8
No Library Section	4
Domain Expired	1
Wordpress	1

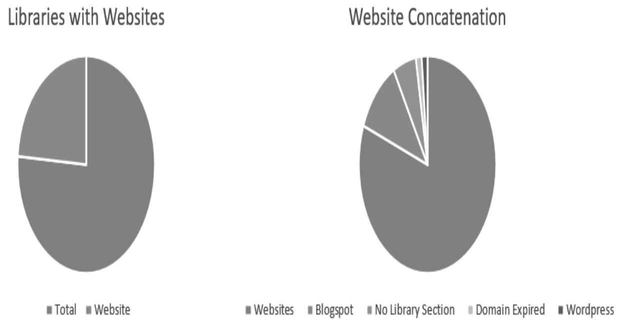
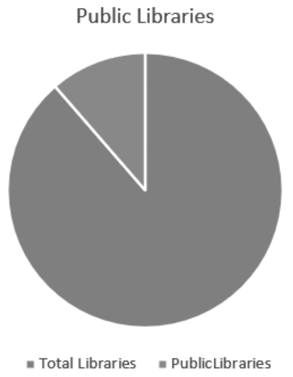
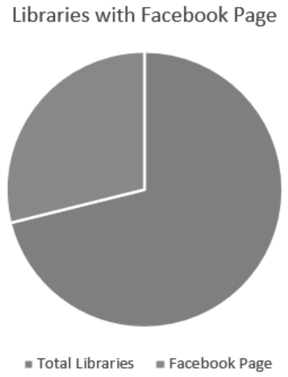


Table 2. The Greek Libraries Network of the National Library of Greece includes 73 libraries with a website.

From the total of 234 libraries, 30 are public libraries, 73 have a website and 95 have a Facebook page.

Out of the 73 libraries that have a website, there is either a separate website for the library (e.g. http://vivl-atalant.fth.sch.gr/) or the library is mentioned as a sub-category on a municipal website (e.g. https://mykonos.gr/the-island/culture/). There are also eight libraries that instead of a website they use a BlogSpot page, four libraries that are not even mentioned on the municipal website, one example of a library with a WordPress page and one example that the domain has expired.





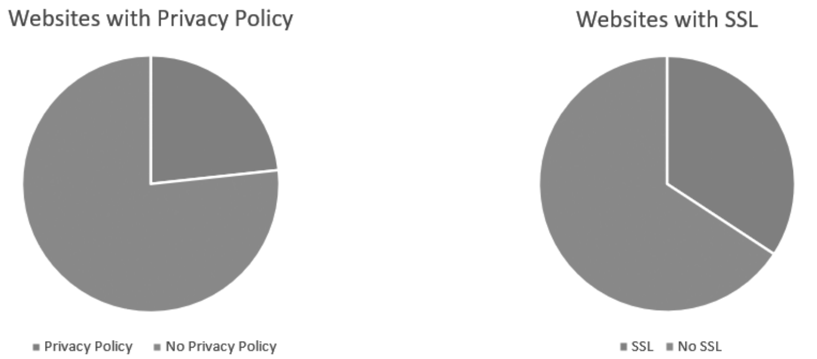
	Libraries
Total Libraries	234
PublicLibraries	30

	Libraries
Total Libraries	234
Facebook Page	95

***Table 3.* The Greek Libraries Network of the National Library of Greece includes 30 libraries that are Public and 95 have a Facebook Page.**

An important factor regarding website security is the use of Secure Sockets Layer (hereinafter, SSL) certificates. SSL certificates play a crucial role in website security, enabling web applications to adopt the more secure protocol Hypertext Transfer Protocol Secure (hereinafter, HTTPS), which is used for secure communications in the online world, rather than Hypertext Transfer Protocol (HTTP) which is less secure due to lack of proper encryption. An SSL certificate is a data file hosted in a website's origin server. With the use of SSL certificates, the encryption SSL/TLS occurs. The SSL certificates include the public key of the website a users' browser is trying to connect with and further relevant information for the website's identity. Users that try to initiate communication with a specific web server will reference the exact file containing the above information in order to obtain the public key and verify the server's identity. The private key is not transmitted but is kept secret and secure. SSL, more commonly called Transport Layer Security (TLS), is a protocol for the encryption of internet traffic and the verification of a servers' identity. Any website with an HTTPS web address uses the protocol SSL/TLS. Previous studies have shown that the state of non-browser SSL code is catastrophic across web applications, leaving users vulnerable to Man-in-the-Middle attacks (MITMAs) (Fahl, S., et al, 2013; Conti, M., et al, 2016). SSL certificates are used to encrypt data in transit between the host, either the server or the firewall, and the user, through the internet browser. With the use of SSL certificates, it is ensured that the information transmitted, are delivered from/to the appropriate server without interceptions. Some types of SSL certificates such as organization SSL or extended validation SSL add an additional layer of credibility since the visitor of a website may see the organization's information knowing that is a genuine entity (Bhiogade, M.S., 2002).

From the total of 73 libraries that have a website, as shown in Table 4, we have identified that only 25 use SSL in order to secure the transmitted data.



	Libraries
Privacy Policy	17
No Privacy Policy	56

	Libraries
SSL	25
No SSL	48

Table 4. ***The Greek Libraries Network of the National Library of Greece includes 73 libraries that have website.***
From a total of 73, 17 libraries have updated Privacy Policies and 25 use SSL in order to secure the transmitted data.

Despite that the Greek Libraries Network of NLG was created with the aim to assist academic, research, public, civil and school libraries to develop and evolve—among others—their online services provided to all interested parties, the usability and security of these services is weak—if not embryonic—at least. In order for the Greek Libraries Network of NLG to participate in national and/or in international financial programs, it must previously invest in both security and data protection, especially after the application of GDPR. Following the requirements of international laws and standards, GDPR has come to set new rules regarding how to manage personal data on websites, giving explicit choice to each user whether to allow or not the use of their data. An investment in website-security and data protection for the Greek Libraries Network of NLG and each library-member of this network could consider the deployment of elements of a GDPR-compliant website, the minimum number of which is referred below hereto.

4. Elements of GDPR-compliant websites

An interesting factor regarding GDPR is the enforcement of fines to the organizations that appear to be non-compliant. GDPR Enforcement Tracker[10] is a website which contains a list and overview of fines and penalties which data protection authorities within the EU have imposed under GDPR the past couple of years. No library appears to have been fined, so far. Since some fines are not made public, this list is not exhaustive, and thus the GDPR Enforcement Tracker cannot guarantee that libraries Europe-wide have escaped fining for non-compliance with GDPR.

Drawing on the available data and by searching for keywords '*web*' and '*email*', we have found that until June 2020, 27 cases relate to non-compliance regarding websites and 8 cases have to do with marketing email campaigns. While this may not be a large number of fined entities, combined with the current risk incurred by the growth of personal data processing, more fines are expected to emanate in the future should the requirements of GDPR will not be fully respected.

In order to consider how the GDPR impacts a website, it should be determined how the website under consideration interacts with organizational activities in the online world such as email campaigns, digital marketing and social media strategies and further actions that might include personal data. GDPR makes clear that each user should firstly provide consent regarding the use of his/her personal data, thus more transparency should be applied regarding the handling of personal data. This consent must be cumulatively (1) freely given, (2) be specific, (3) be informed and (4) be unambiguous.[11] All these four traits of consent must be explicitly clarified in the content of a Terms and Conditions of Use text in the website of the Greek Libraries Network of NLG as well as in the websites of the library-members of the Greek Libraries Network of NLG. The Data Subject Consent Form and the Data Subject Consent Withdrawal could be linked documents/forms to the Terms and Conditions of Use text. In the event of underaged users of the library-website and/or applications used through it, the Parental Consent Form and the Parental Consent Withdrawal Form could be also linked to the Terms and Conditions of Use text. An Access Control Policy may also be linked to the Terms and Conditions of Use text informing users of the library and/or users of the Greek Libraries Network of NLG upon the basic

[10] See GDPR Enforcement Tracker available at URL: https://www.enforcementtracker.com/[last check, Aug.12, 2020].

[11] See art.4(11) of GDPR.

principles for accessing all available information systems, networks and services and the user-registration process for accessing said means. In the event of allowance to use user's own devices within the premises of a library, the Terms and Conditions of Use text could also include a link to the Bring Your Own Device Policy that applies in the library.

Additionally, and in consideration of GDPR, the websites of the library-members of the Greek Libraries Network of NLG should contain an analytic and unique Privacy Policy section, analyzing the types of information that are stored, the way they are collected and the purposes of the collection. Also, linked to the Privacy Policy could be the Data Retention Policy, as well as the Cross Border Personal Data Transfer Procedure if applicable. The website of the Greek Libraries Network of NLG and/or the websites of the library-members of said Network may elaborate upon Standard Contractual Clauses for the Transfer to Controllers of personal data and/or upon Standard Contractual Clauses for the Transfer to Processors of personal data in the event they are making use of them—Controllers and/or Processors—for the processing of personal data through their operation. The Data Subject Access Request Form could be linked to Privacy Policy, too.

An analytic and unique Privacy Policy section is a sine-qua-non element of a website that is compliant to the GDPR-requirements (Degeling, M., et al, 2019). In addition to elements linked to the Privacy Policy of a website as reported above hereto, the following elements could be contained in the Privacy Policy: 1) basic information regarding the library and the types of information that are stored and the way they are collected; 2) apart from GDPR, there should be a reference to applicable national laws like data protection laws and regulations that remain in effect in Greece; 3) if any third-party providers are leveraged upon, they should be mentioned in the Privacy Policy including all services that might track end user data e.g. Google Analytics, Facebook Analytics even plugins and applications that use or store such data. etc.; 4) the Privacy Policy should include detailed information regarding the personal data gathered by the website and/or the applications offered to users through it as well as the purpose for each personal data process; 5) a detailed action plan in an event of a data breach or a successful hacking attack. If any data is in danger, the data-subject should be notified following a concrete communication strategy of which the core elements may be reported in the Privacy Policy; 6) the Privacy Policy should include detailed information about the data controller and the data protection officer, including contact details of both of them (Lindèn, T., et al, 2020; Zuiderveen Borgesius, F., et al, 2017).

Furthermore, all websites should contain a Cookies Policy which includes an analytic list of the cookies that are collected by each website including the data of the visitors. Following the principles of the GDPR, both the Greek Libraries Network of NLG's website as well as each library-member's website should contain an analytic list of the cookies that are collected by each website including data of their visitors. Also, there should be included a notification banner or page regarding the cookies, in order for the user to choose the cookies that he/she wants to provide in any case (Sanchez-Rola, I., et al, 2019; Dabrowski, A., 2019).

A Privacy Notice composed in lay-terms should be provided in the index page of websites of both the Greek Libraries Network of NLG as well as in the websites of the library-members of the Greek Libraries Network of NLG.

Regarding plugins and further application that may be implemented on the website of any library-member and/or the website of the Greek Libraries Network of NLG, they should be compliant under GDPR. If the application or plugin is created by a third-party, then the website owner (library or the Greek Libraries Network of NLG) should check whether the third party is GDPR compliant or not. In any case that any plugin or application is not compliant to the requirements of GDPR, then an alternative plugin or application should be found and used.

All checkout pages should follow GDPR's principles. In order to do so, checkboxes should be included for the consent of the user and link directly to the website's Privacy Policy during checkout.

The Privacy Policy and the Terms and Conditions of Use text, at least, should include among other information specific reference to user's rights furnished through the GDPR and also include a link to the Data Subject's Rights Form through which a user may apply his/her rights.

Regarding email marketing campaigns and newsletters, the website of any library-member and/or the Greek Libraries Network of NLG, should include an option for the user to unsubscribe from the mailing list and another option to opt-in the user and check if he/she gave the consent to store the personal data. Moreover, after a series of marketing email campaigns sent, the administrator of the website should proceed with deletion of the low bounces email accounts. In any case of a user request regarding personal data, a reply should be sent within two days. In addition, in any case of a user request regarding deletion or update of data, the library-member or the Greek Libraries Network of NLG should reply and act accordingly within 30 days after the submission of the user's request.

There are other documents and procedures which need not be linked to the texts described in the websites of the Greek Libraries Network of NLG as well as in the websites of the library-members of the Greek Libraries Network of NLG, such as an Appendix Inventory of the Processing Activities, the Employee Privacy Policy, the Data Breach Response and Notification Procedure, the Anonymization and Pseudonymization Policy, the Policy on the Use of Encryption, the Information Classification Policy—if any, necessary—, the

Mobile Device and Teleworking Policy, the Clear Desk and Clear Screen Policy, the Supplier Data Processing Agreement, the Employee Data Retention Policy, the Security Procedures for the IT Department, the IT Security Policy, the Data Breach Notification Form to the Supervisory Authority, the Data Breach Notification Form to Data Subject.

In the event of a hacking attempt, website backups are crucial. Although they should not be regarded as a substitute for having in place website security infrastructure, a back-up can always help restore damaged files, reassuring the fast recovery of the library' image to the online world. All library-members as well as the Greek Libraries Network of NLG should have a backup solution for their websites in order to be compliant under GDPR and also in order to ensure functionality and availability of their resources. Nevertheless, the administrator of each website should ensure that there are not more than three backups that may include personal data of users. A proper backup solution should be, firstly, off site. In case that the backup is stored in the same server where the website is hosted, then it is as vulnerable to attacks as the website itself, and this is a major security risk. The backups should be stored off-site in order to be immune to hacking attempts or a potential hardware failure. In addition, backups should be automated, taking advantage of the numerous backup solutions available. Backups should be checked periodically in order to ensure that they function in a proper way. Furthermore, the existing backup, should be encrypted with a strong encryption algorithm and only the administrator of the website should have the ability to download the backup. It is important to possess a local backup of the whole entity and an external backup not linked to the application in case of an equipment failure or of a malicious episode (Politou, E., et al, 2018).

Nowadays, more and more websites suffer from successful hacking attempts due to outdated or unpatched applications or Content Management Systems (CMS). It is of crucial importance to update each website whenever a new version is released either regarding the CMS or regarding the plugins that are installed. As we mentioned above, the majority of hacking attempts targeting websites are automated. Bots are scanning every site they can to discover any exploitation opportunities. It is not efficient to upgrade once a month or even once a week anymore, because bots are extremely likely to discover a vulnerability before it is patched.

A CMS is a software dedicated to creating and managing content for a website, on a particular platform. Nowadays, it is strongly recommended to use CMS such as WordPress (Lindèn, T., 2019) and Magento for security, compliance and functionality reasons. CMS platforms, have teams that implement and release functionality and security updates periodically (Patel, S., et al, 2011). A CMS like WordPress, has a strong community where anyone can share questions and find answers regarding how to further secure a website. While a CMS often provides frequent security updates, the use of third-party extensible components, such as themes or third-party plugins and applications, leads to vulnerabilities that cyber threats can easily target and exploit. The most common hacking attempts targeting websites are completely automated and most of these attacks rely on the default settings of a CMS. Thus, the vast majority of the attacks can be restrained by configuring the default settings by the website administrator. Nevertheless, despite the fact that a CMS may appear to be more vulnerable because it is based on an open source framework, a website based on a CMS can reach a satisfying level of security not only regarding compliance matters, but also regarding real hacking threats.

One of the most adequate technique in order to enhance the security of a website, is the use of a web application firewall (WAF). Even though a web application firewall may assist in order to fulfil Payment Card Industry Data Security Standards (PCI DSS) for a library's website, it can hardly provide protection with regard to every security incident that may occur online. There are also other aspects that may affect the security of a website such as the errors that may occur due to mistakes based on the human factor. Furthermore, the use of SSL certificates is not enough in order to prevent a malicious user to get unauthorized access to a library's website. A vulnerability that may exist on a library's website can enable a potential attacker to capture communications and receive personal or restricted data. Moreover, even if a library's website under consideration is completely patched with all the updates, a malicious user may focus the hacking attempt on distributed denial of service attacks (DDoS) with the aim to slow the websites' response to the legitimate users or even set it not available at all. Thus, a web application firewall is designed in order to prevent a library's website from such malicious activities.

5. Epilogue

As we have mentioned in past work (Vavousis, K., et al, 2020), the requirements of GDPR will affect not only the websites of the library-members of the Greek Libraries Network of NLG, but their day to day work as a whole. In parallel with the creation or re-built of a compliant and secure website, each member of the Greek Libraries Network of NLG will have to determine the level of compliance for its website and IT infrastructure regarding the processing of personal data; it should also comply with privacy by design and privacy by default principles by deploying technical and organizational means on how to process personal data and adopt privacy-enhancing techniques and policies capable of protecting personal data from malicious activities.

The security of an IT infrastructure of a library-member of the Greek Libraries Network of NLG is an ongoing procedure that requires constant research and changes according to the needs of the library based on international standards, regulations and new-found solutions. In a similar vein, a library's website security is a never-ending process that needs continuous assessment in order to achieve compliance with applicable laws and regulations such as GDPR and in order to reduce the risks that may occur, protecting the library's website under consideration from internal and external cyber threats. Thus, a library's website protection is certainly a procedure that evolves constantly and an important component for the management of a site (Johnson, G., et al, 2020).

Website security is essential for every organization, especially for the Greek Libraries Network of NLG and for each library-member's online presence. The absence of proper website security can lead to multiple unsolicited events such as traffic loses, website reputation loss and user-data leakages. The calamities that may occur due to improper website security such as user-data leakages, might lead to litigation enacted from negatively affected data-subjects, the imposition of fines by the Supervisory Authority in Greece for violation of GDPR and of relevant legislation, and to a tarnished library reputation.

In order to conduct an optimum solution with regard to security and compliance for the websites of the Greek Libraries Network of NLG and for each library-member's online presence, there should be protective mechanisms in place that will ensure high availability and security, not only for the visitors, but also for the IT infrastructure.

The Greek Libraries Network could expand beyond the Hellenic territory and include libraries abroad that serve as a center of Greek culture.

Following the project to provide an ILS to every library in Greece, a common identity management system (IDM) for users of all member-libraries (e.g. one ID card for all to unified services) is under consideration. Moreover, a documents exchange system is under development to organize and automate collection exchange among Greek libraries. In this context, the provision of legal services and consultancy to all member-libraries (e.g. intellectual property rights, collection donations, GDPR etc.) is also one of the core future developments of the Network.

References

¬ Abdul Bashah Mat, A., Ala' Yaseen Ibrahim, S., Mohd Syazwan, A., Jasem, A., 2011, *SQL-injection vulnerability scanning tool for automatic creation of SQL-injection attacks*, WCIT-2010, 1877-0509 © Elsevier, DOI: https://doi.org/10.1016/j.procs.2010.12.076, available at URL: https://www.sciencedirect.com/science/article/pii/S1877050910004515?via%3Dihub [last check, Aug.12, 2020].

¬ Bhiogade, M.S., 2002, *Secure Socket Layer*, in 2002 Informing Science & IT Education Conference proceedings, available at URL: https://proceedings.informingscience.org/IS2002Proceedings/papers/Bhiog058Secur.pdf [last check, Aug.12, 2020].

¬ Conti, M., Dragoni, N., Lesyk, V., 2016, *A Survey of Man in the Middle Attacks*, in IEEE Communications Surveys & Tutorials, Vol.8, Iss.3, pp.2027-2051, DOI: 10.1109/COMST.2016.2548426, IEEE, available at URL: https://ieeexplore.ieee.org/abstract/document/7442758 [last check, Aug.12, 2020].

¬ Dabrowski, A., Merzdovnik, G., Ullrich, J., Sandera, G., Weippl, E., 2019, *Measuring Cookies and Web Privacy in a Post-GDPR World*, In Choffnes D., Barcellos M. (eds), *Passive and Active Measurement*, PAM 2019, Lecture Notes in Computer Science, Vol 11419, Springer, Cham, DOI: https://doi.org/10.1007/978-3-030-15986-3_17, available at URL: https://link.springer.com/chapter/10.1007/978-3-030-15986-3_17 [last check, Aug.12, 2020].

¬ Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., Holz, T., 2019, *We Value Your Privacy… Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy*, NDSS 2019, DOI: 10.14722/ndss.2019.23378, available at URL: https://arxiv.org/abs/1808.05096 [last check, Aug.12, 2020].

¬ Dehalwar, V., Kalam, A., Lal Kolhe, M., Zayegh, A., 2017, *Review of web-based information security treats in smart grid*, in 7th International Conference on Power Systems, DOI: 10.1109/ICPES.2017.8387407, IEEE, available at URL: https://ieeexplore.ieee.org/abstract/document/8387407 [last check, Aug.12, 2020].

¬ Eshete, B., Villafiorita, A., Weldemariam, K., 2011, *Early Detection of Security Misconfiguration Vulnerabilities in Web Applications*, in Sixth International Conference on Availability, Reliability and Security, DOI: 10.1109/ARES.2011.31, IEEE, available at URL: https://ieeexplore.ieee.org/abstract/document/6045929 [last check, Aug.12, 2020].

¬ Fahl, S., Harbach, M., Perl, H., Koetter, M., Smith, M., 2013, *Rethinking SSL development in an appified world*, in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, pp.46-60, DOI: https://doi.org/10.1145/2508859.2516655, available at URL: https://dl.acm.org/doi/abs/10.1145/2508859.2516655 [last check, Aug.12, 2020].

¬ Gupta, S., Gupta, B., 2015, *Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art*, in International Journal of System Assurance Engineering and Management 8, pp.512-530 (2017), DOI: https://doi.org/10.1007/s13198-015-0376-0, available at URL: https://link.springer.com/article/10.1007/s13198-015-0376-0 [last check, Aug.12, 2020].

¬ Hassan, M., Shamina Sultana, N., Marjan, A., Rafita, H., Fabiha Nawar, D., Mostafijur, R., Asif, S., Hasan, S., 2018, *Broken Authentication and Session Management Vulnerability: A Case Study of Web Application*, DOI: 10.5013/IJSSST.a.19.02.06, available at URL: https://ijssst.info/Vol-19/No-2/paper6.pdf [last check, Aug.12, 2020].

¬ Hassan, M., Ali, M., Bhuiyan, T., Sharif, M., Biswas, S., 2018, *Quantitative Assessment on Broken Access Control Vulnerability in Web Applications*, in International Conference on Cyber Security and Computer Science 2018, available at URL: http://www.iconcs.org/papers/Paper_28.pdf [last check, Aug.12, 2020].

¬ IBM, *The 2019 Cost of a Data Breach Report*, available at URL: https://www.ibm.com/security/data-breach [last check, Aug.12, 2020].

¬ Johnson, G., Shriver, S., Goldberg, S., 2020, *Privacy & Market Concentration: Intended & Unintended Consequences for the GDPR*, SSRN, DOI: http://dx.doi.org/10.2139/ssrn.3477686, available at URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3477686 [last check, Aug.12, 2020].

¬ Kantarcioglu, M., Xi, B., 2016, *Adversarial Data Mining: Big Data Meets Cyber Security*, CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Pages 1866–1867, October 2016.

¬ Kuner, C., Bygrave, L., Docksey, C, 2020, *The General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press.

¬ Leite, G.S., Albuquerque, A.B., 2019, *An Approach for Reduce Vulnerabilities in Web Information Systems*, in Silhavy R., Silhavy P., Prokopova Z. (eds) *Intelligent Systems in Cybernetics and Automation Control Theory*, CoMeSySo 2018. Advances in Intelligent Systems and Computing, Vol.860. Springer, Cham, DOI: https://doi.org/10.1007/978-3-

030-00184-1_9, available at URL: https://link.springer.com/chapter/10.1007/978-3-030-00184-1_9 [last check, Aug.12, 2020].

¬ Lindèn, T., Khandelwal, R., Harkous, H., Fawaz, K., 2020, *The Privacy Policy Landscape after the GDPR*, in Proceedings on Privacy Enhancing Technologies, Vol.2020, Iss.1, DOI: https://doi.org/10.2478/popets-2020-0004, available at URL: https://content.sciendo.com/view/journals/popets/2020/1/article-p47.xml [last check, Aug.12, 2020].

¬ Lindèn, T., 2019, *Building a secure WordPress website with plugins*, Thesis, LAMK, available at URL: https://www.theseus.fi/bitstream/handle/10024/263175/Tuomas_Lind%c3%a9n.pdf?sequence=2&isAllowed=y [last check, Aug.12, 2020].

¬ Osincev, A., Laponina, O., 2019, *Vulnerability Testing in Web Applications External Entities XML*, International Journal of Open Information Technologies, Vol.7, No.10, available at URL: http://www.injoit.org/index.php/j1/article/view/808 [last check, Aug.12, 2020].

¬ Patel, S., Rathod, V.R., Parikh, S., 2011, *Joomla, Drupal and WordPress – a statistical comparison of open source CMS*, in 3rd International Conference on Trendz in Information Sciences & Computing, DOI: 10.1109/TISC.2011.6169111, available at URL: https://ieeexplore.ieee.org/abstract/document/6169111 [last check, Aug.12, 2020].

¬ Politou, E., Michota, A., Alepis, E., Pocs, M., Patsakis, C., 2018, *Backups and the right to be forgotten in the GDPR: An uneasy relationship*, in Computer Law & Security Review, Vol.34, Iss.6, pp.1247-1257, DOI: https://doi.org/10.1016/j.clsr.2018.08.006, available at URL: https://www.sciencedirect.com/science/article/abs/pii/S0267364918301389 [last check, Aug.12, 2020].

¬ Sanchez-Rola, I., Dell' Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vernier, P-A., Santos, I., 2019, *Can I Opt Out Yet?: GDPR and the Global Illusion of Cookie Control*, in Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, pp.340-351, DOI: https://doi.org/10.1145/3321705.3329806, available at URL: https://dl.acm.org/doi/abs/10.1145/3321705.3329806 [last check, Aug.12, 2020].

¬ Sue, X., Yao, D., Bertino, E., 2015, *Privacy-Preserving Detection of Sensitive Data Exposure*, in IEEE Transactions on Information Forensics and Security, Vol.10, No.5, pp.1092-1103, May 2015, DOI: 10.1109/TIFS.2015.2398363, available at URL: https://ieeexplore.ieee.org/abstract/document/7038200 [last check, Aug.12, 2020].

¬ Vavousis, K., Papadopoulos, M., Polley, J., Xenakis, C., 2020, *A compliant and secure IT infrastructure for the National Library of Greece in consideration of Internet security and GDPR*, [S.l.], Vol.9, No.2, pp.219-236, July 2020, ISSN 2241-1925, available at URL: http://www.qqml-journal.net/index.php/qqml/article/view/638 [last check, Aug.12, 2020].

¬ Zuiderveen Borgesius, F., Kruikemeier, S., Boerman, S., Helberger, N., 2017, *Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation*, 3 European Data Protection Law Review, p.353, available at URL: https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl3&div=63&id=&page= [last check, Aug.12, 2020].