Qualitative and Quantitative Methods in Libraries (QQML) 9,2: 219-236, 2020

A compliant and secure IT infrastructure for the National Library of Greece in consideration of internet security and GDPR

Konstantinos Vavousis[1], Dr. Marinos Papadopoulos[2], John Polley[3], Prof. Christos Xenakis[4]

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

Abstract. The application of the General Data Protection Regulation (GDPR) is considered an issue of vital importance for the smooth operation of IT infrastructures, especially for companies in EU Member States. GDPR is a useful tool, which, among other requirements, mandates the adoption of privacy-by-design and advanced security techniques. Taking into account its requirements, this article analyses their implementation with regard to applied Internet Security solutions. While the Regulation offers a minimum set of technical Internet Security means to be taken into consideration by companies and organizations to achieve GDPR compliance, the current paper aims to highlight the adaptation of strong security mechanisms that will not only set companies compliant with GDPR, but also maintain them strong and secure against most threats.
Keywords: IT security, optimal infrastructure, strong security mechanism, GDPR, security posture, policies

Enhanced Security Mechanisms for the National Library of Greece

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 a similar vein, GDPR requires strong security mechanisms to be in place in order to safeguard the data under consideration. All libraries, public and private including of course the National Library of Greece (hereinafter, NLG) need to comply with GDPR requirements for personal data protection. Hence, powerful security mechanisms should be adopted for the adequate protection of personal

Received: 19.5.2020 Accepted: 3.7.2020 ISSN 2241-1925

data and/or special categories data stored and in order to comply with GDPR requirements. 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., Xi, B., 2016). In this paper, we analyze the basic components that NLG should implement and properly configure, in order to become compliant with the relevant legislation and resilient to cyber-attacks.

Under GDPR, following a data breach, the data controller has the legal obligation to notify the supervisory authority in 72 hours maximum[1]. 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 is highly recommended to companies and organizations to assist them in minimizing investments for their IT security infrastructure and protecting their data. NLG is not an exception to the rule of this recommendation, of course. Strong security mechanisms should be implemented in order to not only be compliant with GDPR requirements, but also become secure against the continuously-evolving cyber security threats. Once these strong security mechanisms are in place, the level of security in an IT infrastructure will be enhanced and the company will minimize the required response to a security breach.

Thus, NLG has no alternative but to maximize it Information Technology security posture through technical measures with the aim to enhance the security of its IT infrastructure and comply with 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*[2]. By the term "*technical measures*", mentioned in the 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 a company holds.

The optimal way to begin, is to conduct vulnerability scans and penetration tests on the network and its components, including servers, routers, switches and endpoints risk assessments will assist further to discover loopholes in all

[1] 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.

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

processing activities, to identify the highest risks regarding personal data and the effective measures that should be taken under consideration.

Regardless of the possible future changes in the structure of NLG, a resilient IT security infrastructure for NLG should include a firewall solution with endpoint security, a DLP solution (Data Leakage Prevention) which will include an MDM (Mobile Device Management), an IDPS system (Intrusion Detection - Intrusion Prevention System), encryption regarding email communications, encryption and pseudonymization regarding the personal and sensitive data stored in the IT infrastructure. Regarding the authentication and authorization of the users in a web-based service, a strong access control solution should be adopted and be included as well in the arsenal of minimum IT security mechanisms.

The following image depicts a suggested topology regarding a compliant and secure IT infrastructure for NLG in consideration of its structure currently.

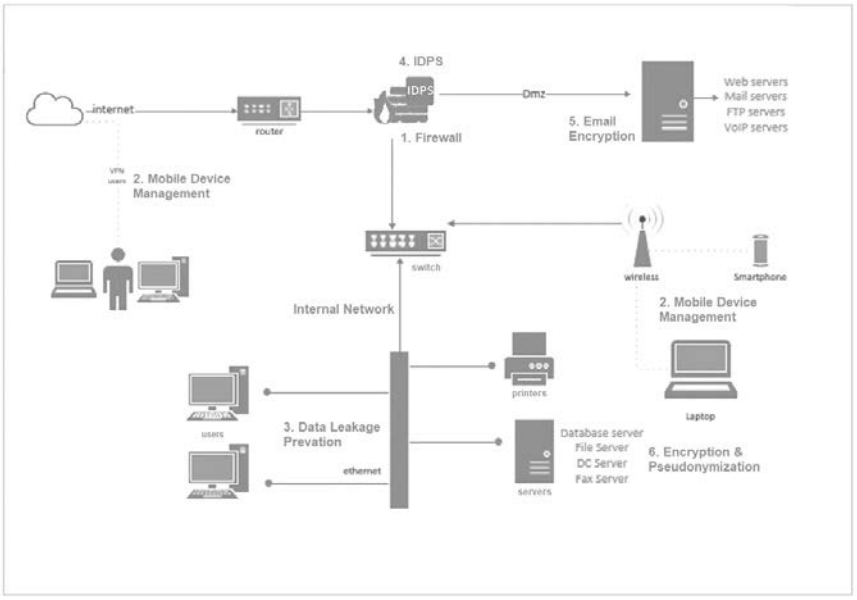

Figure 1. Suggested Topology Regarding a Compliant and Secure IT Infrastructure of NLG

1. Firewall

A firewall solution for NLG is an important component, able to safeguard its IT infrastructure, which not only monitors and manages all incoming and outgoing

network traffic, but additionally, is able to create a bulletproof environment against all types of malware threats. Numerous attacks have been seen in the wild that have to do mainly with poor configurations and lack of targeted rules enforced (Wool, A., 2010). While cyber intruders and malicious programs can bypass firewall solutions, these are the primary defense line against cyber-attacks coming from the outside of an IT infrastructure, as well as from insiders or malware attempting to transmit stolen data from the network's interior. Therefore, NLG's firewall is an essential ingredient of compliance with GDPR and other regulations.

A firewall can be implemented as hardware and software, or a combination of both according to the needs of the IT infrastructure. Typically, a firewall protects against malicious users and allows only legitimate users to access the network, based on the security strictly defined by the IT administrator and the applicable organization's policies. NLG's well configured firewall solution is able to determine potential malicious activities, monitor and alert on denial of service and distributed denial of service attacks when occurred, control access to all connected to its network computers if endpoint protection is enabled and allow access to information based on certain levels of trustworthiness that have been set by NLG's IT administrator and applicable IT security policies.

2. Data Leakage Detection and Prevention Systems

GDPR has introduced the concepts of "*Privacy by Design*"[3] and "*Privacy by Default*"[4,5]. "*Privacy by Design*" and "*Privacy by Default*" have been frequently-discussed topics related to data protection (Ved, A., 2017). The first

[3] See art.25(1) of GDPR.
[4] See art.25(2) of GDPR.
[5] Art.25 of GDPR, which is titled Data Protection by design and by default; according to art.25 of GDPR, 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 shall, both at the time of the determination of the means for processing and at the time of the processing itself, 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 this Regulation and protect the rights of data subjects.
The controller shall 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. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

thoughts of "*Privacy by Design*" were expressed in the 1970s and were incorporated in the 1990s into Data Protection Directive, i.e. Directive 95/46/EC[6]. According to Recital 46 in Data Protection Directive, Technical and Organizational Measures (TOM)[7] must be taken already at the time of planning a processing system to protect data safety. The term "*Privacy by Design*" means nothing more than data protection through technology design[8]. Behind this is the thought that data protection in data processing procedures is best adhered to when it is already integrated in the technology when created. The essence 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 the GDPR and to integrate necessary safeguards into the processing of personal data so that the processing will meet its requirements and otherwise ensure protection of data subject's rights. The wording of article 25 of GDPR expressly describes a duty for data-protection that applies not just at the time of processing but also beforehand when the controller determines the means for processing, i.e. at the time of designing an information system.

Nevertheless, there is still uncertainty about what "*Privacy by Design*" means, and how one can implement it. This is due, on the one hand, to incomplete implementation of the Data Protection Directive in some Member States; on the other hand, the principle of "*Privacy by Design*" which is addressed in the GDPR, requires persons responsible already to include definitions of the means

[6] See Recital 46 of Data Protection Directive according to which Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, 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; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking 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.

[7] See Recital 78 of GDPR titled Appropriate Technical and Organizational Measures. The definition of TOMs in GDPR includes indicatively internal policies and measures which meet in particular the principles of data protection by design and data protection by default, and 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, etc.

[8] See Recital 78 of GDPR according to which *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.*

for processing TOMs at the time that they are defined in order to fulfil the "*Privacy by Design*." Legislation leaves completely open which exact protective measures are to be taken. GDPR allows for the definition of TOMs through codes of conduct prepared by library industry bodies[9] or by proper certification schemes[10]. The "*Privacy by Design*" requirement is met through TOMs, i.e. through not just technical measures, but also through organizational measures. In other words, they embrace not simply the design and operation of software or hardware, but they also extend to business strategies and other organizational measures and practices such as rules determining which and under what circumstances NLG employees are authorized to access or otherwise process personal data or special categories data.

The "*Privacy by Design*" and "*Privacy by Default*" mandate of article 25 of GDPR is addressed to controllers. Thus, NLG acting as a controller must adhere to the requirements set by article 25 of GDPR. However, these requirements must also be met by third parties that NLG leverages upon for the provision of its services in consideration of Recital 78 of GDPR according to which *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.* '*Privacy by Design*' is an obligation set by GDPR that affects also NLG's processors since NLG is only permitted to use processors that provide *sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.*[11]

In addition to the named criteria, the type, scope, circumstances and purpose of the processing must be considered. This must be contrasted with the various probability of occurrence and the severity of the risks connected to the processing. The text of the law leads one to conclude that often several protective measures must be used with one another to satisfy statutory requirements. In practice, this consideration is already performed in an early development phase when setting technology decisions[12]. Recognized

[9] See art.40(2)(h) of GDPR, according to which Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation such as …

[10] See art.25(3) of GDPR, according to which An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

[11] See art.28(1) of GDPR; see, also, Recital 81 of GDPR.

[12] See Recital 78 of GDPR.

certification can serve as an indicator to authorities that NLG has complied with the statutory requirements of "*Privacy by Design*.[13]"

The outcome of these two concepts of "*Privacy by Design*" and "*Privacy by Default*" described in GDPR is that NLG is now legally accountable for any loss or unauthorized access and usage of the personal data it processes. NLG could further develop its understanding of "*Privacy by Design*" and "*Privacy by Default*" requirement set by article 25 of GDPR by delving into the requirements described in the Cybersecurity Act: Regulation 2019/881/EU of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)[14].

NLGs Data Leakage Detection and Prevention Systems solution can assist it to monitor, restrict and block the transferring of personal data. NLG's Data Leakage Detection and Prevention Systems solution provides information regarding the organization's data giving the ability to network administrators to enforce rules according to the defined level of sensitivity of the data in question. By adopting this kind of solutions, NLG's network administrator becomes able to mitigate data leaks coming from users' errors or internal malicious activities. NLG's Data Leakage Detection and Prevention Systems enhances NLG's GDPR compliance as it is leveraged in order to find, follow, delete, restrict access, prevent access and maintain personal data within NLG's IT infrastructure.

3. Special Categories Data Storage

GDPR requires data processors and data controllers to define where personal data and information is stored or processed[15]. By implementing NLG's Data Leakage Detection and Prevention Systems solution, NLG network administrator is able to scan the existing network infrastructure, including mobile devices and endpoints, for special categories data as defined by policies, compliance profiles, personally identifiable information, file extensions and other attributes that specify the nature of the data. By doing so, NLG has the

[13] See art.25(3) of GDPR.

[14] See Regulation 2019/881/EU available at URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj (last check, April 30, 2020); according to Recital 41 of this Cybersecurity Regulation ENISA should play a central role in accelerating end-user awareness of the security of devices and the secure use of services, and should promote security-by-design and privacy-by-design at Union level. In pursuing that objective, ENISA should make use of available best practices and experience, especially the best practices and experience of academic institutions and IT security researchers.

[15] Art.4 No.2 GDPR.

ability to know where special categories data exist and where they go throughout its network infrastructure. Furthermore, the application of NLG's Data Leakage Detection and Prevention Systems solution makes it is easier for the network administrator to provide extensive reports when requested by the Hellenic Data Protection Agency.

4. Deletion of Special Categories Data

One of GDPR's requirements is to collect data strictly for the necessary to the pre-defined specific, explicit and legitimate purposes and not further processed the data in a manner that is incompatible with those purposes[16]. Data must be stored only for the limited time that is need—the principle of data storage limitation (European Commission, 2018). In the framework of NLG's statutory goals and scope of activities, further processing of data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with article 89(1) of GDPR, not be considered to be incompatible with the initial purposes[17].

Data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. For NLG, the storage limitation principle of GDPR allows for data storage for longer periods *insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with article 89(*1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject[18].

By implementing NLG's Data Leakage Detection and Prevention Systems solution, NLG's network administrator becomes able to delete personal data or special categories data stored anywhere in NLG's network infrastructure even remotely, allowing for total control on the stored data within NLG's IT infrastructure, and at the same time making possible instant decisions on the maintenance of data on any devices connected to NLG's network (Prov International, 2017).

5. Restriction of Special Categories Data usage

Another GDPR requirement is to ensure that the controller or the processor will not process special categories data for any other purpose beside those strictly referred to[19]. Processing of special categories data by NLG is allowed provided that said *processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance*

[16]Art.5(1)(b) of GDPR.
[17] Art.5(1)(b) of GDPR.
[18] Art.5(1)(e) of GDPR.
[19] Art.9(1) of GDPR.

with article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject[20].

NLG does not upload or share data of special categories to any cloud service. By applying NLG's Data Leakage Detection and Prevention Systems solution, special categories data can be identified by NLG's network administrator, and by using rules, policies and specific filters NLG's network administrator restricts and totally denies any kind of data transfer within the network infrastructure or outside of it. Consequently, users of NLG's connected computers are restricted from uploading, downloading, coping or printing or otherwise using any special categories data.

6. Maintaining Security Standards

Following the enforcement of GDPR, NLG as data controller is required to be informed regarding the privacy and security standards that processors, which NLG may leverage upon, have adopted and implemented and whether or not they have been up to date[21]. Through the implementation of NLG's Data Leakage Detection and Prevention Systems solution, transferred or stored data can be scanned within the controller and processors' IT infrastructure; thus, NLG can inform, if necessary, the processors in order to take specific actions if a data breach occurred. NLG's Data Leakage Preventions system is an integral part of GDPR implementation by preventing losses of personal data and/or special categories data in NLG's network infrastructure, covering two of the most important components of GDPR, the integrity and confidentiality of protected data[22] (European Data Protection Supervisor, 2018).

7. Mobile Device Management system

Mobile device management (MDM) is a type of security software that can be used by NLG's IT department to monitor, manage and secure employees' mobile devices that are deployed across multiple mobile service providers and across multiple mobile operating systems being used in the organization (Blokdyk, G., 2019). GDPR has a strong impact on the way that NLG can handle its data within mobile devices.

A great change that came with GDPR, is the need-to-know basis of where the data exist at any given moment and a consent of the individual for storing and using the data. Another requirement, is to know the origin of specific data and the individual who shared these data, which is a challenge especially for mobile

[20] Art.9(2)(j) of GDPR.
[21] Art.32 of GDPR.
[22] Art.5(1)(f) of GDPR.

users, for example NLG's personnel who may collect data through its different premises.

One of the most important functionalities in order to meet a certain security level and also be compliant with GDPR, is to determine the devices that have access to specific data and services at all times. NLG's Mobile Device Management solution, allows to include some personal devices which need to be separate objects of a risk assessment before allowing their users to include protected data. NLGs' Mobile Device Management solution should come part and parcel with NLG's Bring Your Own Device policy that strictly describes the nature of the data and the access level through mobile devices policy applied in NLG (BYOD) (French A., et al, 2014). Gathering all the information and devices included in NLG's Mobile Device Management solution and Bring Your Own Device policy, NLG's IT administrator will have the ability to audit the logs and specify the actions that took place in an event of data breach.

It is of high importance to pinpoint that more often than not mobile devices are overlooked when it comes to security. However, they have become a great risk when it comes to security and compliance, if the appropriate security mechanisms are not in place. In any case, it is important to adopt strict security controls including proper configuration, policies and encryption techniques on every device, in order to safeguard the data included.

Of course, ensuring the security of business data is much easier when personal and business data are kept separate. Establishing clear boundaries between a user's personal data and NLG's business data on personnel's mobile devices is a very important, though a hard, step to take. Ideally, any user including NLG's personnel should not be able to gain access to any personal apps or personal email accounts on a business device and vice versa. This would help minimize security risks and it is a way for NLG to stay GDPR compliant regarding the integrity and confidentiality of protected data. However, this is not an easy step to take, and so instead NLG needs to focus on minimizing the overlap and establishing clear boundaries and policies for managing TOMs deployed for securing the integrity and confidentiality of protected data.

8. Intrusion Detection and Prevention system

Cyber-attacks are still one of the biggest reasons of personal data compromising. Verizon's 2017 Data Breach Investigations Report, mentions that more than half of the breaches occurred (51 per cent) can be traced back to malware, and this is just one type of network intrusion that can lead to data being compromised (Ward C., Pritam, N., 2017).

An Intrusion Detection and Prevention system is one of the most powerful ways to get properly protected from cyber threats acting in a different way from the other security components mentioned so far in this paper. NLG's firewall for example is able to filter potentially malicious traffic coming into NLG's

network, while NLG's Intrusion Detection and Prevention system is able to monitor all traffic inside NLG's network infrastructure and alert the NLG IT administrator if malicious acts have been detected.

NLG's Intrusion Detection and Prevention system is a device or software application that monitors NLG's network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to NLG's administrator or is collected centrally using a Security Information and Event Management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms (Blokdyk, G., 2020).

As is shown in the depicted above network topology and according to the needs of NLG's IT infrastructure, NLG's Intrusion Detection and Prevention system should be placed after its firewall, so only legitimate traffic will be inspected which will further reduce load on it as well. However, there are IT infrastructures, in which it is advisable to place the Intrusion Detection and Prevention system in front of the firewall to protect the firewall from cyber-attacks. Therefore, a strong customized to the needs of NLG Intrusion Detection and Prevention system solution, will enhance its protection from cyber-attacks.

9. Email encryption

Sending and receiving emails are considered as high-risk activities regarding information security because it is possible for a network administrator, the service provider or even a malicious user to capture this kind of communication. As a result, it is of high importance to use encryption techniques when transferring sensitive data via email communications and strongly recommended for GDPR compliance and the overall security[23]. Even though email encryption is considered an important component for security in general, it is not commonly implemented within IT security infrastructures for companies and organizations.

There are two basic techniques for email encryption, each one serving on a different level. The first method encrypts the emails while transmitted from one end to the other via an encrypted tunnel. Emails are encrypted before the actual transfer at the source and decrypted upon arrival to the destination, using network protocols such as TLS (Transport Layer Security) and its ancestor SSL (Secure Socket Layer). The second method for email encryption, encrypts the content of the email and doesn't interfere with any transferring protocols while transporting the email. Thus, even if the packets are captured by anyone in the middle of the communication, the content cannot be shown as it is encrypted (Desmedt, Y., 2005).

[23] Art.32 GDPR.

A known and widely used method regarding content encryption is S/MIME (Secure/Multipurpose Internet Mail Extensions) and Open PGP based on Pretty Good Privacy (PGP) (Internet Engineering Task Force - IETF, 2007). PGP is an encryption program that provides cryptographic privacy and authentication for data communication (Zimmermannn, P., 1995); regarding email encryption there are also numerous solutions nowadays by enterprise vendors like Microsoft (Microsoft Corp., 2019) and Symantec (Symantec Corp., 2019).

10. Encryption

In a similar vein with email encryption, data encryption converts clear text into a hashed code using ciphers, where the encrypted information is able to become readable again by the method of decryption. It needs numerous resources to decrypt a ciphertext without the knowledge of the encryption key, thus, it is highly unlikely for a third party to decrypt a captured ciphertext. Strong encryption is the best solution for NLG in order to safeguard the transmission of sensitive information and one of the best methods to protect personal data or special categories data by unauthorized access while stored.

11. Pseudonymization

Pseudonymization is a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. A single pseudonym for each replaced field or collection of replaced fields makes the data record less identifiable while remaining suitable for data analysis and data processing (ISO/TC, 2008). Regarding compliance to GDPR, the application of pseudonymization to personal data can reduce the risks to data subjects concerned and help controllers and processors to meet their data-protection obligations[24]. Pseudonymization is recommended as a means for securing data protection in NLG's network and IT infrastructure but should not be used as a way to separate identifiers from data subjects regarding personally identifiable information in order to circumvent other obligations (i-SCOOP, n/d).

12. Non-Technical Measures

Apart from strong technical implementations, NLG is in the need of effective Information Security Policy to be adopted as an essential part of its IT-security posture. This policy could include subsection such as Asset Management, Access Control, Passwords & Encryptions, Remote Access, Bring Your Own Device (BYOD), Clear Desk & Screen, Secure Disposal, Business Continuity Plan/Disaster Recovery. In addition, security awareness and training for all the NLG employees is required in order to avoid security breaches. Cyber criminals will mostly target the weakest link in the chain of security, which is the human factor (Evans, N. J., 2009). An employee unintentionally could click at a

[24] See Recital 28 of GDPR titled *Introduction of Pseudonymization*.

phishing email, share sensitive information over the telephone and could let a ransomware be installed in the computer connected to NLG's network, which could cause serious damage to the organization (Scheeres, J. W., 2012). For this reason, NLG's employees should become aware and be periodically trained on best practices in the usage of their systems and their obligations and responsibilities regarding the data they manage and are associated to. Trainings on a regular basis regarding strong password policies, best practices while surfing online, locking the screen when leaving the desk and the latest techniques used by hackers in order to evade a system, are some of the recommended practices that promote effectively throughout NLG the secure IT infrastructure and work as an add-on to a secure by design IT infrastructure within the organization.

13. Authentication and Authorization on a web service

Text and data mining have been already in use for security threat detection, and for discovering hidden information in unstructured log messages (Suh-Lee C., et al, 2017). Moreover, text and data mining has been used for security and crime detection (Paaβ, G., et al, 2014). While text and data mining may be used for security purposes, NLG's databases that contain and manage sensitive, confidential, and valuable data, should be properly protected from unauthorized access and data losses. A successful implementation for data security at NLG should not only provide accurate and timely data but also protect its confidentiality, integrity, availability, and security overall. While creating a database that is accessible online by registered users such as NLG's general catalogue[25], NLG's administrator must properly safeguard the catalogue's stored data. NLG's general catalogue and other NLG services available through the Web appear more vulnerable than other NLG infrastructures because they are accessible online, thus anyone can potentially access them; thus, the addition of a new set of requirements to the security landscape for all NLG services, moreover NLG's Web services is a necessity. NLG's properly configured Access Control policy is one of the most important components regarding security on Web services offered from the library and it works as a powerful tool to protect the stored data accessed by external users, as it filters who will have access and where exactly.

One of the major aspects regarding the security of NLG Web services is the authentication of each user trying to access the web service under consideration, verifying that the user is who he/she claims to be. Each user is identified through NLG's Single Sign On system by providing valid credentials, mostly his/her full name, email address, date of birth[26]. Users of NLG Web services are

[25] See NLG's catalogue available to registered users at https://www.nlg.gr/collection/catalogue/ (last check, April 30, 2020).

[26] See NLG's SSO system available at URL: https://register.nlg.gr (last check, April 30, 2020).

authenticated through SSO which is connected to Independent Authority for Public Revenue's system[27].

14. Epilogue

Throughout this paper, we focus on NLG's Internet Security solutions in consideration of compliance with the GDPR. While the Regulation offers a minimum set of technical Internet Security means to be taken into account by companies and organizations with the aim to achieve GDPR compliance, the current paper highlights on a set of TOMs deemed necessary for the application of strong security mechanisms at NLG. By adopting these TOMs described in this paper, NLG can enhance its ability to better protect the library's IT infrastructure from cyber threats, and also can improve the response to these kinds of threats and mitigate their impact. Even after more than two years since GDPR has been enforced, a large number of companies including most public libraries have not adopted a strong security strategy rendering them vulnerable to cyber security threats. GDPR is an opportunity for cyber security in practice, giving the chance to companies and organizations to implement effective security mechanisms. Apart from the fines enforced by Regulation 2016/679/EU, protecting personal data and data of special categories is foremostly a matter of NLG's IT infrastructure security.

NLG as well as all national libraries of EU Member States are organizations which operate as safe-keepers of cultural treasures; they are aimed to build a distributed and permanent collection of digital resources from the field of digital preservation development of a distributed network of safekept material with resource owners, or parties nominated by them, providing long-term access to their material. For this reason, Directive 2019/790/EU on copyright and related rights in the Digital Single Market, which amends Directives 96/9/EC and 2001/29/EC, paves the way for NLG and other EU Member States' national libraries to proceed with massive preservation of cultural heritage. Copyright law that negatively impacted on the reproduction of works protected by copyright is being amended through article 6 of Directive 2019/790/EU which caters for a mandatory exception *to the rights provided for Article 5(a) and Article 7(1) of Directive 96/9/EC, Article 2 of Directive 2001/29/EC, Article 4(1)(a) of Directive 2009/24/EC and Article 15(1) of this Directive, in order to allow cultural heritage institutions to make copies of any works or other subject matter that are permanently in their collections, in any format or medium, for purposes of preservation of such works or other subject matter and to the extent necessary for such preservation*. The digitization, maintenance, connectivity, and the making available to the public of digital resources kept in national libraries are becoming core features in an ever growing number of products and services offered by them and with the advent of the internet of Things (IoT) a high number of connected digital devices are expected to be deployed by

[27] See login through NLG's SSO system available at URL: https://sso.nlg.gr/login (last check, April 30, 2020).

national libraries across the European Union during the next decade. While an increasing number of cultural resources and treasures safe-kept in NLG and other national libraries are becoming available online, and while an increasing number of devices connected to the internet may be leveraged upon to access these cultural resources, security and resilience are not sufficiently built in by design in national libraries, leading to insufficient cybersecurity.

Cybersecurity is not only an issue related to technology, but one where human behavior is equally important. The so-called, "*cyber-hygiene*"[28], namely, simple, routine measures that, where implemented and carried out regularly by citizens, organizations and businesses, minimize their exposure to risks from cyber threats, should be strongly promoted in the environment of NLG and all national libraries of EU Member-States. National libraries, which most—if not all—of them are public organizations, are organizations which are involved in the design and development of ICT products, ICT services or ICT processes, thus they should be encouraged to implement TOMs at the earliest stages of design and development to protect the security of those products, services and processes to the highest possible degree, in such a way that the occurrence of cyberattacks is presumed and their impact is anticipated and minimized ('*security-by-design*')[29]. Security should be ensured throughout the lifetime of an ICT product, ICT service or ICT process deployed in a national library by design and development processes that constantly evolve to reduce the risk of harm from malicious exploitation. National libraries' ICT products or ICT services or ICT processes should be designed and be made available in such a way so that they ensure a higher level of security which *should enable the first user to receive a default configuration with the most secure settings possible* ('*security by default*'), *thereby reducing the burden on users of having to configure an ICT product, ICT service or ICT process appropriately*[30].

All EU Member States' national libraries including NLG, of course, have the daunting task of compliance with GDPR. This task can be seen in the wider spectrum of creating cyber-resilient organizations, i.e. national libraries that consider compliance with the requirements of Directive 2016/1148/EU concerning measures for a high common level of security of network and information systems across the European Union. Most of the cyber-security issues are common to all national libraries in the EU. The establishment of a European cybersecurity certification framework through Regulation 2019/881/EU[31] that lays down the main horizontal requirements for European

[28] See Recital 9 of Regulation 2019/881/EU on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
[29] See Recital 12 of Regulation 2019/881/EU.
[30] See Recital 13 of Regulation 2019/881/EU.
[31] See art.46 and art.49 of Regulation 2019/881/EU.

cybersecurity certification schemes to be developed and allows for European cybersecurity certificates and EU statements of conformity for ICT products, ICT services or ICT processes to be recognized and used in all Member States, could be leveraged in the industry of EU national libraries through a cybersecurity certification scheme customized to the relevant cyber-security special needs and requirements of national libraries, museums, and archives in the EU. We refer to a European certification scheme laying down the comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes used by libraries, museums, and archives throughout EU. The idea for a European cybersecurity certificate addressing cybersecurity needs of libraries, museums, and archiving organizations Europe-wide could be cultivated and further be developed through organizations such as the European Bureau of Library, Information and Documentation Associations (ELBIDA) or organizations with international poise such as the International Federation of Library Associations and Institutions (IFLA) which could furnish the European Cybersecurity Certification Group provisioned in article 62 of Regulation 2019/881/EU with information on the special needs and requirements for secure ICT products, ICT services, and ICT processes aimed to be used by organizations such as national libraries in the EU. A European cybersecurity certification for national libraries, museums and archiving organizations could be leveraged upon to prove compliance with GDPR requirements, in consideration of the provision of article 54(4) of Regulation 2019/881/EU according to which *a European cybersecurity certification scheme may be used for establishing the presumption of conformity with legal requirements*.

Bibliography

Blokdyk, G., 2019, *Mobile Device Management MDM – A Complete Guide*, 2019 Edition 5STARCooks.

Blokdyk, G., 2020, *Security Information and Event Management SIEM – A Complete Guide*, 2020 Edition 5STARCooks.

Desmedt, Y., 2005, *Man-in-the-Middle Attack*, In: van Tilborg H.C.A. (eds) Encyclopedia of Cryptography and Security, Springer, Boston, MA, 2005.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281, 23.11.1995, p. 31–50, available at URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 (last check, April 30, 2020); No longer in force, Date of end of validity: 24/05/2018; Repealed by Regulation (EU) 2016/679.

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 *on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC*, OJ L 130, 17.5.2019, p. 92–125, available at URL: https://eur-lex.europa.eu/eli/dir/2019/790/oj (last check, April 30, 2020)

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 *on the legal protection of databases*, OJ L 77, 27.3.1996, p. 20–28, available at URL: https://eur-lex.europa.eu/legal-

content/EN/TXT/?uri=celex%3A31996L0009 (last check, April 30, 2020); consolidated text of this Directive 96/9/EC can be found at URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:01996L0009-20190606 (last check, April 30, 2020)

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 *on the harmonization of certain aspects of copyright and related rights in the information society*, OJ L 167, 22.6.2001, p. 10–19, available at URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001L0029 (last check, April 30, 2020); consolidated text of this Directive 2001/29/EC can be found at URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02001L0029-20190606 (last check, April 30, 2020)

Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 *on the legal protection of computer programs* (Codified version), OJ L 111, 5.5.2009, p. 16–22, available at URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32009L0024 (last check, April 30, 2020)

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30, available at URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG (last check, April 30, 2020)

European Commission, 2018, *The GDPR: new opportunities, new obligations*, Luxembourg: Publications Office of the European Union, available at URL: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf (last check, April 30, 2020).

European Data Protection Supervisor, 2018, *Guidelines on the protection of personal data in IT governance and IT management of EU institutions*, available at URL: https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf (last check, April 30, 2020).

Evans, N. J., 2009, *Information technology social engineering: an academic definition and study of social engineering-analyzing the human firewall*, Graduate Theses and Dissertations, Iowa State University, 2009.

French A., et al, 2014, *Current Status, Issues, and Future of Bring Your Own Device (BYOD)*, Communications of the Association for Information Systems 35(10), November 2014.

IBM Security, 2017 Cost of Data Breach Study, Global Overview, Benchmark research sponsored by IBM Security, Study conducted by Ponemon Institute LLC, June 2017.

IBM Security, 2019 Cost of Data Breach Report, Global Overview, Benchmark research sponsored by IBM Security, Study conducted by Ponemon Institute LLC, July-August 2019.

International Organization for Standardization, Technical Committee, 2008, *Health Informatics: Pseudonymization*, ISO/TC 215, ISO.

Internet Engineering Task Force (IETF), 2007, *OpenPGP Message Format*, IETF Proposed Standard RFC 4880, November 2007.

i-Scoop, n/d, *Personal data pseudonymization: GDPR pseudonymization what and how*, available at URL: https://www.i-scoop.eu/gdpr/pseudonymization (last check, April 30, 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.

Microsoft Corp., 2019, *Email encryption in Office 365*, available at URL: https://docs.microsoft.com/en-us/microsoft-365/compliance/email-encryption (last check, April 30, 2020).

Paaβ, G., Reinhardt, W., Püping, S., Wrobel, S., 2014, *Data Mining for Security and Crime Detection*, NATO Science for Peace and Security Series, D: Information and Communication Security, p.56-70.

Prov International, 2017, *3 Phases of protection by a Data Leakage Prevention (DLP) plan*, available at URL: https://www.provintl.com/blog/3-phases-of-protection-by-a-data-leakage-prevention-dlp-plan, (last check, April 30, 2020)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88, available at URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (last check, April 30, 2020)

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 *on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013* (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15–69 available at URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj (last check, April 30, 2020)

Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 *concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004*, OJ L 165, 18.6.2013, p. 41–58, available at URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R0526 (last check, April 30, 2020)

Scheeres, J. W., 2012, *Establishing the Human Firewall: Reducing an Individual's Vulnerability to Social Engineering Attacks*, BiblioScholar.

Suh-Lee C., Jo, J-Y., Kim, Y., 2017, *Text mining for security threat detection discovering hidden information in unstructured log messages*, 2016 IEEE Conference on Communications and Network Security (CNS), February 2017.

Symantec Corp., 2019, *Encryption Solutions for Email Powered by PGP™ Technology*, 21276730-9 02/17, available at URL: https://www.symantec.com/content/dam/symantec/docs/data-sheets/encryption-solutions-for-email-en.pdf (last check, April 30, 2020).

Ved, A., 2017, *Privacy and Security by design is a crucial step for privacy protection*, Least Authority, July 2017, available at URL: https://leastauthority.com/blog/privacy-and-security-by-design-is-a-crucial-step-for-privacy-protection/ (last check, April 30, 2020)

Ward C., Pritam, N., 2017, *Cyberespionage and ransomware attacks are on the increase warns the Verizon 2017 Data Breach Investigations Report*, Verizon, available at URL: https://www.verizon.com/about/news/cyberespionage-and-ransomware-attacks-are-increase-warns-verizon-2017-data-breach (last check, April 30, 2020)

Wool, A., 2010, *Trends in Firewall Configuration Errors: Measuring the Holes in Swiss Cheese*, IEEE Internet and Computing, Volume: 14 Issue 4, p.58-65, March 2010.

Zimmermann, P., 1995, *The Official PGP User's Guide*, MIT Press.