A unified system for log management compliant with Italian requirement of "Minimal measures for ICT security" and General Data Protection Regulation

Francesco Ciclosi[a]

[a]*University of Macerata, Via Crescimbeni, 30/32, Macerata 62100, Italy*

Abstract: This paper describes and implements the University's log management system. In this scope, are also described, the collection, the archiving, the accessibility, the maintenance for availability, integrity and confidentiality, as well as the verification of the retention time of the information generated by all systems managed by University's IT systems. All the information are included in a ISMS's technical procedure, which applies to many entities, namely systems, hosts, critical processes, personal information and everything that, through the access to them, can generate some logs. Our approach is an integrated approach, which provides us the ability to manage with a unified strategy, different requirements provided by different laws and authorities. The work describes the analysis of the different requirements of Regulation (EU) 2016/679, as well as of the Standards ISO/IEC 27001:2013 and ISO/IEC 27002:2013, and the Italian legislation on ICT Minimum Measures for Public Administration (which is directly derived from the "CIS Critical Controls for Effective Cyber Defense" version 6 of the 2015). Therefore, it describes how to integrate these requirements in the University's Information Security Management System, to manage them, in a coherent and centralized way.

1. Introduction

In this paper, we describe the solution adopted by the University of Camerino about the log management system. The approach followed by the University is an integrated approach, who provides it the ability to manage in a unified strategy (within the Athenaeum's ISMS) different requirements provided by different laws and authorities. Specifically, these requirements are contained in the Regulation (EU) 2016/679, as well as in the Standards ISO/IEC 27001:2013 and ISO/IEC 27002:2013, as well as, in the Italian legislation on ICT Minimum Measures for Public Administration (which is directly derived from the "CIS Critical Controls for Effective Cyber Defense" version 6 of the 2015).

Nomenclature

GDPR	General Data protection Regulation
ISMS	Information Security Management System
CODAU	Conference of General Directors of Universities Administrations
CSC	Critical Security Controls
AGID	Italian Agency for Digital Italy
EU	European Union
CAD	Italian Code of the Digital Administration
EUNIS	European University Information Systems
WP29	Data Protection Working Party established by Article 29 of Directive 95/46/EC

2. The log management system as a tool to ensure compliance with GDPR requirements

The article 25 of Regulation (EU) 2016/679 establishes that "*the controller shall [...] implement appropriate technical and organisational measures*" (c.f. art. 25(1)) ((European Union), 2016). In addition, these measures "*are designed to implement data-protection principles*" (c.f. art. 25(1)) ((European Union), 2016), and also "*to integrate the necessary safeguards into the processing in order to meet the requirements of […] Regulation and protect the rights of data subjects*" (c.f. art. 25(1)) ((European Union), 2016). Recital 78 further clarifies these concepts, by specifying that "*such measures could consist, inter alia, of [...] enabling the data subject to monitor the data processing, enabling the controller to create and improve security features*" ((European Union), 2016).

The ICO's (which is the UK control authority) has stated that the implementation of solutions compliant with the concept of privacy by design, must involve a wide range of technical and organizational measures, among which there are "*security measures to prevent data misuse, such as access controls, audit logs and encryption*" ((Information Commissioner's Office), 2017).

The implementation of a log management system is useful to support the controller in achieving compliance with the GDPR accountability principle too. In fact, the article 33 of Regulation (EU) 2016/679 establishes that, "*in the case of a personal data breach, the controller shall without undue delay […], notify the personal data breach to the supervisory authority competent*" (c.f. art. 33(1)) ((European Union), 2016). In details, this notification must be provided, "*where feasible, not later than 72 hours*" (c.f. art. 33(1)) ((European Union), 2016) after the controller have become aware of data breach, "*unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons*" (c.f. art. 33(1)) ((European Union), 2016). Furthermore, according to the article 34 of Regulation (EU) 2016/679, "*the controller shall communicate the personal data breach to the data subject without undue delay*" (c.f. art. 34(1)) [1], in the case that "*the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons*" (c.f. art. 34(1)) ((European Union), 2016). This is a general requirement that could be avoided if "*the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects [...] is no longer likely to materialize*" (c.f. art. 34(2)) ((European Union), 2016).

Following this approach, the controller must have a support system that help it, both in the timely become aware of the data breach, and in the identification of what actually happened. Our log management system based on Graylog do both these functions. This statement is fully confirmed by the legal obligation of to "*document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken*" (c.f. art. 33(5)) ((European Union), 2016). Even in this case, our log management system is

very helpful to accomplishes with this requirements.
In paragraph 3 will be presented a detail analysis of the tracking of non-primary information as they are described (Diomede et al., 2017) by the Working Group of the "*Conference of General Directors of Universities Administrations*" (CODAU).

3. The tracking of non-primary information

In order to deal with the particular challenge of the application of minimum ICT measures in the complex academic world, the CODAU has provided some guidelines (Diomede et al., 2017) about Universities' main processing activities. In this document are analyzed processing related to system and network tracking, as well as to application tracking.
In fact, is not possible to conceive a processing activity that is applicable to events registration, without consider some aspects concerning the compliance with the General Data Protection Regulation. Sure enough, in these registrations are included personal data, namely "*any information relating to an identified or identifiable natural person («data subject»)*" (c.f. art. 4(1)) ((European Union), 2016).
In CODAU opinions' (Diomede et al., 2017), the ground of the purposes of these processing are related to:

- the fulfillment of a regulatory obligation;
- the "*systemic constraints (e.g. data that for technical reasons are strictly necessary for the provision of a service)*" (Diomede et al., 2017);
- the "*recording of events to guarantee the protection of data and/or information systems (e.g. to support proactive or reactive activities of cyber security or data protection)*" (Diomede et al., 2017);
- the recording of events to support;
- the "*recording the sequence of events generated by users as part of an administrative process in order to support reconstruction and verification activities*" (Diomede et al., 2017);
- the verification of the real use of a service;
- the internal reporting for administrative purposes.

It is important to underline that in WP29 Opinion, the meaning of word "employees" is related not only to people who have a contractualized position with employer, but instead to "*all situations where there is an employment relationship, regardless of whether this relationship is based on an employment contract*" (Falque-Pierrotin, 2017).
Taking into account the new recent technological developments, today the monitoring problems is not only related to email and Internet usage, but it involves also "*newer, potentially more intrusive and pervasive, ways of monitoring*" (Falque-Pierrotin, 2017). Among these new methods of monitoring, the WP29 (Falque-Pierrotin, 2017) specifies some, which are also implemented at the University of Camerino; namely:

- **next-Generation Firewalls**, which can provide both a variety of monitoring technologies (e.g. deep packet inspection, TLS interception, website filtering, content filtering, on-appliance reporting, user identity information) and data loss prevention;
- **security applications and measures** that involve logging employee access to the university's systems;
- **use in the workplace of office applications provided as a cloud service**, which potentially could cause a detailed logging activity of the operations performed by employees;
- "***monitoring of personal devices*** *(e.g., PCs, mobile phones, tablets), that employees supply for their work in accordance with a specific use policy, […] which enables the distribution of applications, data and configuration settings, and patches for mobile devices*" (Falque-Pierrotin, 2017).

In this regard, the European High Court of Justice has highlighted the possibility that corporate communication tools (e.g. telephone calls and instant messenger accounts) could also be used for private purposes, but only if this secondary use is limited and proportional (PETZOLD, 1997). Furthermore, the same entity has also stated that this communication flow "*may be covered by the notions of «private life» and «correspondence» within the meaning of Article 8 paragraph 1 [of the European Convention]*" ((European Court of Human Rights), 2016).
Another interesting point is related to the fact that sometimes "*the monitoring of employees is possible not so much of the deployment of specific technologies, but simply because employees are expected to use online applications made available by the employer which process personal data*" (Falque-Pierrotin, 2017). This scenario is significant because the use of cloud-based office applications is exactly an example of this.
Finally, it is important to underlining that "*generally, prevention should be given much more weight than detection*" (Falque-Pierrotin, 2017), so WP29 advises that, controller should prefer to preliminarily block some resources (e.g. websites), instead to perform a continuous monitoring of it.
For a detail analysis, both of data protection techniques (i.e. anonymization, pseudonymisation), and of the data re-identification risks, please refer to the article named "*k-Anonymity*" (V. Ciriani S. De Capitani di Vimercati & Samarati, 2007).

4. The log management system as a mean to ensure compliance with ISO/IEC 27001:2013 and ISO/IEC 27002:2013 standards

An operational implementation of a log management system, from a perspective both organizational and technical, can be also a mean to ensure the compliance with some ISO/IEC 27000's family standards, namely 27001:2013 ((International Organization for Standardization), 2013a) and 27002:2013 [9].
In the Annex A of the ISO/IEC 27001:2013 standard ((International Organization for Standardization), 2013a) are listed 114 controls, divided into 14 main security controls categories and 35 principal categories of security. Inter alia, in the main security control named A.12 "*Operations security*", there is the principal category named A.12.4 "*Logging and monitoring*", which has the control objective of "*to record events and generate evidence*" ((International Organization for Standardization), 2013a). This category is further divided into 4 controls, namely: event logging (A.12.4.1), protection of logs information (A.12.4.2), administrator and operator logs (A.12.4.3) and clock synchronization (A.12.4.4). The standard ISO/IEC 27002:2013 ((International Organization for Standardization), 2013b) is essential for a correct implementation of the ISO/IEC 27001:2013 one; as a matter of fact contain some additional information, such as an implementation guidance and other information, useful for an appropriate application of the control itself.
Comparing (the results of this analysis cannot be reproduced in this paper due to copyright policies applied by ISO) the content of the AgID Base Security Controls and that of the controls described in the ISO/IEC 27001:2013 standard, it is possible to detect a substantial overlap of the same.
In particular, while the controls, defined in the ISO/IEC standards under examination, highlight the importance of a policy that treats these topics, the ABSCs mainly define, and in a more granular way, the technical solutions linked to these policies.
This is consistent with the setting of ISO 27001:2013, which does not deal with what is present within the policy, nor its quality, nor, even more so, the quality of the instruments that govern it.
Rather, the focus of the standard is centered on the presence of the management mean (i.e. the ISMS and its documents) and on the fact that, in it, the objectives of the indicated controls have been taken into consideration.

Finally, it should be noted that the ISO/IEC 27002:2013 standard ((International Organization for Standardization), 2013b) highlights that in event logs could be present sensitive data and personally identifiable information, so is necessary take into account the introduction of appropriate privacy protection measures.
Furthermore, in the same rule is asserted that system administrators should not have permission to erase or de-activate logs of their own activities.
These aspects were taken into consideration during the definition of the University's ISMS.

5. The integration with Information Security Management System

In order to guarantee the full integration of logs management system with the already existing University's Information security management system (ISMS) (Ciclosi F, Mauri M, & Polzonetti A, 2016), a specific technical procedure has been modified. This deals with identifying methods of collection, archiving, accessibility and maintenance of integrity and confidentiality of the log information generated by university's systems. Moreover, the same technical procedure also deals with both the information's verification and their conservation times.
This is a very complex document, even considering its integration with other documents of the Information security management system. In fact, there are references to the synchronization of clocks, to the installation of the Sidecar Collector agents in the Operating Systems, to the configuration of network devices for connection to the Graylog, as well as to the University's business continuity and disaster recovery plans.
Moreover, this technical procedure references also two electronic registers, which are an integrated part of it. In the first one, there are the logs' details generated by the Universities core systems, which are stored in the centralized logs collection system. Instead, in the second one, they are detailed, both the general configuration of the logs collection system, and that of each individual system that sends him its logs.
At the end of 2017, the technical procedure of logs management has undergone significant changes to implement the indications of the University of Camerino working group about the application of the "*Italian minimum security measures for ICT security*" ((AgID), 2016). This is a working group set up on 29 September 2017, in order to meet the requirements indicated in the Circular of the "*Agenzia per l'Italia Digitale*" no. 2 of 18 April 2017 ((AgID), 2017). These aspects are analyzed in detail in my paper, named "*The risk analysis as a unified approach to satisfy GDPR, NIS Directive and ISO 27001 requirements*" (Ciclosi, Gentili, Rappi, & Belfiore, 2018b), presented in Paris at EUNIS (European University Information Systems) 2018 conference.
From an operative point of view, in this procedure are been included some controls of the AgID Basic Security Control's (ABSC) eighth family. Which are a set of controls of the "*Italian Cyber Security Framework*" (Baldoni & Montanari, 2015), who are also derived from the "*CIS Critical Controls for Effective Cyber Defense*" ((The Center for Internet Security), 2015) version 6 of the 2015. In detail, the controls are those of the ABSC type 8.1.3 and 8.2.1, namely, respectively "*Events detected by the instruments are sent to a central repository (syslog) where they are permanently archived*" ((AgID), 2017) and "*All tools mentioned in ABSC_8.1 are monitored and managed centrally. Users are not allowed to alter their configuration*" ((AgID), 2017).

6. Logs classification mode

The guidelines issued by the CODAU (Diomede et al., 2017) highlight that the nature of the data contained is usually critical. Therefore, is needed that the security parameters are set, this for an optimal and necessary management in keeping logs generation. In the ISMS's technical procedure, logs are divided into two groups:

- **system logs**, who are related to systemic and network tracking, and are usually generated by events related to the operating systems or network equipment;
- **application logs**, who are related to applications tracking, and are usually generated by the software.

Also, for a correct log management, is essential that all the systems' clocks are synchronized.
The significant logs for the system were identified (regardless of their format). This was done behalf the security needs, described in the Information Security Management System (ISMS) Policy, and taken into consideration by the Risk Assessment. Later, they are reported according to a diagram in which are present some information about them, namely: description, type, registered events and retention. Table I show an extract of this diagram.
Logs files are useful as safety indicators, so before their cancellation, the relevant values will be saved according to the requested modalities. All logs include, where possible and according to the EU and Italian laws, IP address, event type, time, date and user name.
In accordance with the provisions of the CODAU guidelines (Diomede et al., 2017), the University tracks data generated by network devices and infrastructural components that are included within the following treatment service scopes:

- tools for analysis and security management, both on the network and on client/server systems;
- use of printing services;
- VPN access;
- telephone traffic management and related accounting;
- traffic management of the videoconferencing network, streaming services and video surveillance;
- remote access to user locations;
- access to directory-based resources (e.g. LDAP or AD);
- access to central authentication systems;
- management of users for identity and access management;
- access to virtual machines both on premise and in the cloud;
- access to services both on premise and in the cloud;
- external administrative access on our system resources;
- management of the e-mail system in the cloud.

Analogously, the University tracks session data and application tracking of user activities, which are included within the following treatment service scopes:

- authentication and single sign-on for all web services federated with the University's authentication system;
- user navigation in web applications developed both by the University and by third parties;
- monitoring for statistical purposes of access to websites (e.g. Google Analytics);
- use of client applications developed both by the University and by third parties;
- use of platforms for sending and consulting data in digital preservation.

Table 1 - An example of type of events monitored by the University

Description	Type	Registered events	Ret.
Windows events	System	Authentication to domain machines (failed or not)	180 days
		Activities performed by accounts with administrator privileges	
		System errors	
Network devices log	System	Device authentication (failed or otherwise)	180 days
		Relevant safety events	
		System errors	
Monitoring console	Application	Events of connected systems	180 days

7. Description of the logs collection solution

University of Camerino collects and analyzes logs using a dedicated platform called Graylog. This is currently installed on a University's Computer Center server, in Linux mode. Configuration and control panel are accessible on a SSL connection by connecting to the system's IP address, through the necessary credentials.

Operating systems, devices and applications are configured to collect the desired logs information, and store them according to the defined security parameters. Two systems are identified for the collection of logs. The first one concerning the logs generated directly by the applications in use, while the second one, is pertinent the storing of authentication logs of system administrators. The latter collection system has also been implemented, to meet the requirements, imposed by the Italian supervisory authority on the protection of personal data.

It is not possible to directly connect to the logs manager system, by SSH and as privileged user. Instead, all the authorized administrators must to use their personal account to connect by SSH.

In any case, this particular type of connection can only be made temporarily and only to perform specific system maintenance activities, which cannot be done differently.

Rather, the normal activities related to the use of the system will have to hinder via the web, through HTTPS connection, as described previously.

The Graylog system is been configured for to get the best filter information in order to guarantee a more immediate selection of events that need verification, as well as in order to organize the notification of such events. Moreover, these configurations allow me to create a reporting system to get a general overview of the situation and of its evolution over time. This was also achieved by creating particular custom dashboards, an example of which is shown in the Figure 1.

To this end, University's technicians are working to define rules, also created as needed to have active response to an event considered sensitive.

The configuration of the Graylog system, in use by the Center, provides some basic settings that can be individually modified by the system manager.

As regards the transmission of information between the log-producing devices and the central management console, different methods are used.

Graylog nodes accept data via inputs. Therefore, in the central system I have configured three different input node, namely one for network devices, one for syslog sent by means of UDP protocol and, finally, one beats-input for Windows and Linux based systems.

Instead, the configuration at the level of the individual nodes is different. On the one hand, the Center's technicians have redirected the syslog of network devices, and of any devices that uses this technology to the central system. While, on the other side, system's administrators have installed as a service, in each Windows and Linux node, a special agent (called "*Graylog Collector Sidecar*"). This agent is configured to send the system logs, via HTTPS, to a specific API exposed by the central collection system.

The global function of University's logs collector system is described in a ISMS's technical procedure, which has been prepared in compliance with the following, both laws (EU and Italians), and international standards:

- Directive of the President of the Council of Ministers August 1, 2015 (Renzi, 2015);
- Legislative Decree of 7 March 2005, n. 82 (also known as CAD - Administration Code Digital) (GU n.112 del 16-5-2005-Suppl. Ordinario n. 93, 2016);
- Circolare AgID 18 April 2017, n. 2/2017, containing "*Replacement of circular no. 1/2017 of 17 March 2017, containing: «Minimum ICT security measures for public administrations. (Directive of the President of the Council of Ministers August 1, 2015)»*" ((AgID), 2017);
- CIS Critical Security Controls for Effective Cyber Defense - version 6.0 of October 2015 ((The Center for Internet Security), 2015);
- La Sapienza - 2015 Italian Cyber Security Report of the CIS (Baldoni & Montanari, 2015);
- ISO/IEC 27001:2013 ((International Organization for Standardization), 2013a);
- ISO/IEC 27002:2013 ((International Organization for Standardization), 2013b);
- Regulation (EU) 2016/679 ((European Union), 2016);
- Legislative Decree no. 196 of 30 June 2003, Italian "*Personal Data Protection Code*" (English translate by Italian Authority for the protection of personal data) ((Italian Parliament), 2003).

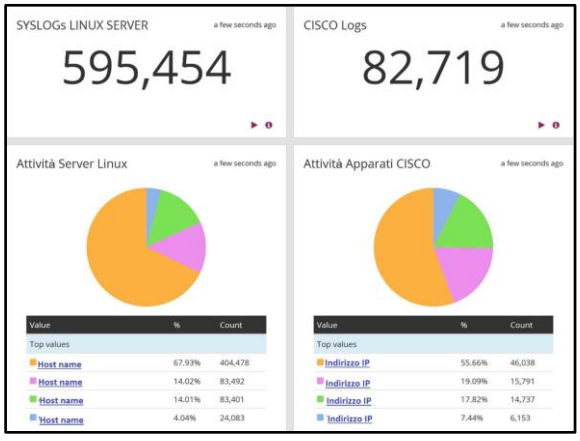

Figure 1 - Example of a Graylog dashboard panel

8. Log storage for disaster revovery purposes

The logs collected by the Graylog system are stored in redounded systems, and are synchronized in a remote storage, as better described in the University's business continuity and disaster recovery plans.

The complete list of logs backed up is kept in a special electronic register (named "*Backup Log Sheet*") that is updated every time the configuration of the backup settings changes. This sheet is divided in three sections, namely: log, recording modality and responsibility.

In the log section, the following information are recorded:

- **Hostname**, who contains the name (or the IP address) of the system from

which the logs are taken;

- **Log type**, who contains the type of the taken logs (e.g. syslog, directory file, name of windows logs).

Furthermore, in the recording modality section, the following information are recorded:

- **notification**, which contains the list of e-mail addresses to which notification messages are sent regarding logs capture and backup events;
- **log consolidation**, which contains information, both on what is consolidated, and about its frequency and scheduling time;
- **retention policy**, which contains information about the typical retention time of these information;
- **backup path**, which contains the full path of backup archives;
- **credentials**, which contain (if available) the user credentials used to capture the logs files from remote systems.

Finally, in the responsibility section, is recorded only the following information:

- **Function involved**, which contains the internal sector that is responsible for monitoring the operation of log acquisition and saving, as well as the updating of the "*Backup Log Sheet*".

9. Logs analysis

The analysis of the collected logs is performed using the dedicated Graylog software tool (described in paragraph 7 and showed in Figure 2).

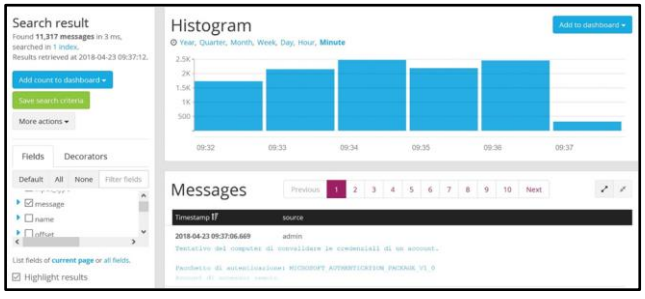

Figure 2 - Example of the Graylog software analysis panel

This activity aims to identify and resolve malfunctions, problems, attacks and any other events that could threaten the normal operation of the University's information system. Moreover, this activity also provides useful data for system's improvement, such as, for example, indicators used in the ISMS.

Now the University is preparing for to define an optimal information filtering method. This is necessary in order to guarantee an immediate selection of events that need verification. Likewise, University is defining, both the procedures for notifying such events, and the implementation of a reporting system, aimed at showing a general outline of the situation, as well as its evolution over time.

In log analysis activity the authorized personnel takes also into account, the network attached devices inventory included in university's ISMS. This inventory is described in detail in my paper, named "*The network attached devices inventory as required both by the Italian requirement of «Minimal measures for ICT security» and by General Data Protection Regulation*" (Ciclosi, Gentili, Rappi, & Belfiore, 2018a), presented in Paris at EUNIS (European University Information Systems) 2018 conference.

10. Conclusions

The use of an integrated approach to the management of information protection, on the subject of centralized management of logs produced by university's devices, represents a piece of a broader methodology adopted by the University of Camerino. This is a general and holistic vision, aimed at guaranteeing data protection and compliance with every requirement, established by laws and by international standards, through their management, within the University's ISMS. This choice has allowed the University of Camerino, among other things, both to increase the continuous improvement of its system, and to satisfy the accountability principle enunciated by Regulation (EU) 2016/679.

REFERENCES

(AgID). (2016). AgID - Misure Minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015). Agenzia per l'Italia Digitale. Retrieved from http://www.agid.gov.it/sites/default/files/documentazione/misure_minime_di_sicurezza_v.1.0.pdf

(AgID). Circolare AgID 18 aprile 2017 , n. 2/2017, Pub. L. No. 2/2017, 1 (2017). Italy. Retrieved from https://www.cert-pa.it/documents/10184/27607/CircolareAgID_170418_n_2_2017_Mis_minime_sicurezza_ICT_PA-GU-103-050517.pdf/7ca821ea-f8cc-4310-9fad-3c6ec1ca7f85

(European Court of Human Rights). (2016). Case of Barbulescu v. Romania (Application no. 61496/08) - Judgment. STRASBOURG: European Court of Human Rights. Retrieved from http://www.bailii.org/eu/cases/ECHR/2016/61.rtf

(European Union). Regulation (EU) 2016/679 of the European Parliament and of the Council, Pub. L. No. Regulation (EU) 2016/679 (2016). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN

(Information Commissioner's Office). (2017). *Big Data, Artificial Intelligence, Machine Learning and Data Protection*. Retrieved from https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

(International Organization for Standardization). ISO/IEC 27001:2013(en), Information technology — Security techniques — Information security management systems — Requirements, Pub. L. No. ISO/IEC 27001:2013 (2013). Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

(International Organization for Standardization). ISO/IEC 27002:2013(en), Information technology — Security techniques — Code of practice for information security controls, Pub. L. No. ISO/IEC 27002:2013 (2013). Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

(Italian Parliament). Legislative Decree no. 196 of 30 June 2003 - Personal Data Protection Code, Pub. L. No. Gazzetta Ufficiale n. 174 del 29 luglio 2003-Supplemento Ordinario n. 123, 1 (2003). Garante per la Protezione dei Dati personali. Retrieved from

http://194.242.234.211/documents/10160/2012405/Personal+Data+Protection+Code+-+Legislat.+Decree+no.196+of+30+June+2003.pdf

(Parlamento Italiano). (2016). *GU n.112 del 16-5-2005-Suppl. Ordinario n. 93. Gazzetta Ufficiale della Repubblica Italiana*. Italy. Retrieved from http://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2005-05-16&atto.codiceRedazionale=005G0104&queryString=%3FmeseProvvedimento%3D%26testoNot%3D%26formType%3Dricerca_avanzata_vigente%26numeroArticolo%3D%26giornoVigenza%3D12%26

(The Center for Internet Security). (2015). The CIS Critical Security Controls for Effective Cyber Defense - Version 6.0. Retrieved from https://cybersecurity.idaho.gov/wp-content/uploads/sites/23/2016/10/CSCmaster.pdf

Baldoni, R., & Montanari, L. (2015). *2015 Italian Cyber Security Report - Un Framework Nazionale per la Cyber Security*. Roma: CIS - CINI. Retrieved from http://www.cybersecurityframework.it/sites/default/files/CSR2015_web.pdf

Ciclosi, F., Gentili, G. P., Rappi, G., & Belfiore, A. (2018a). The network attached devices inventory as required both by the italian requirement of “Minimal measures for ICT security” and by General Data Protection Regulation. In *EUNIS 2018 Congress - Coming of Age in a Digital World - Book of Proceedings* (pp. 14–21). Paris: European University Information Systems Organization (EUNIS). Retrieved from http://hdl.handle.net/11581/408248

Ciclosi, F., Gentili, G. P., Rappi, G., & Belfiore, A. (2018b). The risk analysis as a unified approach to satisfy GDPR, NIS Directive and ISO 27001 requirements. In *EUNIS 2018 Congress - Coming of Age in a Digital World - Book of Proceedings* (pp. 49–60). Paris: (EUNIS), European University Information Systems Organization. Retrieved from http://hdl.handle.net/11581/408250

Ciclosi F, Mauri M, & Polzonetti A. (2016). University ICT Security Certification. *European Journal of Higher Education IT 2016-1*, 101–110. Retrieved from http://www.eunis.org/download/2016/EUNIS2016_paper_39.pdf

Diomede, N. (Università degli S. di M. – S., Ficara, P. (Università degli S. di M.-B., Magri, A. (Università degli S. di M.-B., Morbidi, M. (Università degli S. di F., Pedranzini, F. (Politecnico di M., Prestipino, D. (Università degli S. di M., … Zecca, M. (Alma M. S. – U. B. (2017). *Linee guida in materia di privacy e protezione dei dati personali in ambito universitario*.

Falque-Pierrotin, I. (Article 29 data protection working party). (2017). Opinion 2/2017 on data processing at work (wp249). Brussels: Article 29 Data Protection Working Party.

PETZOLD, H. (1997). Case of Halford v. The United Kingdom (Application no. 20605/92) - Judgment. European Court of Human Rights. Retrieved from http://www.bailii.org/eu/cases/ECHR/1997/32.rtf

Renzi, M. (Presidente del C. dei M. Direttiva 1° agosto 2015 - Sistema di informazione per la sicurezza della Repubblica (2015). Direttiva 1° agosto 2015. Retrieved from https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/direttiva-1-agosto-2015.html

V. Ciriani S. De Capitani di Vimercati, S. F., & Samarati, P. (2007). k-Anonymity. *Secure Data Management in Decentralized Systems, Advances in Information Security*, *33*, *Part I*, 323–353. https://doi.org/10.1007/978-0-387-27696-0_10