UNIVERSIDADE DE LISBOA

FACULDADE DE CIÊNCIAS

DEPARTAMENTO DE INFORMÁTICA

Privacy awareness in Portuguese SMEs

João Manuel Costa Alvega

Mestrado em Segurança Informática

Dissertação orientada por:

Profª. Doutora Ana Luísa do Carmo Correia Respício

2021

Dedicated

To my family and friends.

Also, to all scientifical minds that believe in facts above all our brains misfires and elusions. Never forget even facts must have context. Once, earth was in “fact” the centre of the visible universe.

Abstract

The general data protection regulation is a different approach to the today's dilemma of unrestrained users tracking and user-oriented advertisement. While the regulation is welcomed by users in general, this has meant extra work for small and medium sized organizations.

Like other organizations, Portuguese SMES have to maintain compliance with the regulations and do their best to protect user's privacy. This implies maintaining industry best practices, assessing and managing risk while trying to maintain profitability. With most organizations today having some kind of online presence and cyber-security threats on the rise, Organizations also have to protect their online assets as best as they can under penalty of leaking private information and incur in heftier fines under the regulation.

Obtaining clear and express consent, succinctly explain data processing methods and safeguard user's private data are chores that may have a heavy burden on small organizations that in some cases might be single person or even family enterprises.

These organizations have to maintain competitiveness, compliance with the regulation while also maintaining user privacy, information and data safety, at acceptable running costs.

For this work Portuguese SMEs were surveyed for compliance with the general data protection regulation. From the data obtained we assess their efforts in complying with the regulation and points we believe can be improved.

Keywords: Privacy, GDPR, Risk Management, Best practices, Industry standards

Resumo

A revisão do Regulamento Geral da Proteção de Dados (RGPD) chegou numa altura em que os utilizadores de serviços online sentem-se desprotegidos perante as práticas abusivas das organizações que lhes proporcionam estes serviços e em que se verifica uma desconfiança crescente resultante destas práticas. Entre estas práticas contam-se a recolha desmedida de informação sobre os utilizadores e publicidade dirigida. O RGPD veio regulamentar a recolha de informação pessoal e proteger a informação pessoal dos utilizadores.

Enquanto que, o regulamento é visto com agrado pelos utilizadores em geral, este tem significado trabalho extra para as organizações de pequena e média dimensão (PME).

Tal como outras organizações, as PMEs Portuguesas têm que manter conformidade com as regulamentações e fazer o seu melhor para proteger a privacidade dos sues utilizadores. Isto significa a manutenção das melhores práticas da indústria, avaliar e administrar o risco enquanto tentam manter-se como empresas viáveis dum ponto de vista económico. Com a maioria das organizações da atualidade a ter algum tipo de presença online e as ameaças à segurança informática em crescendo, estas Organizações também têm que proteger estes ativos online o melhor que conseguirem sobre pena de disseminação de informação confidencial e incorrer em pesadas multas perante o regulamento.

A obtenção de claro e expresso consentimento, a explicação sucinta dos métodos usados para processar a informação e a salvaguarda da informação privada de cada utilizador são tarefas que podem ser uma sobrecarga muito grande para as organizações mais pequenas cuja dimensão pode ser tão reduzida como pessoas singulares ou pequenas empresas familiares. Estas organizações têm que se manter competitivas, manter a privacidade da informação dos utilizadores e também manter a conformidade para com o RGPD a custos aceitáveis para a sua sobrevivência.

Para este trabalho sondámos PMEs Portuguesas para a conformidade com o regulamento geral de proteção de dados. Dos dados obtidos avaliamos os esforços dessas organizações em cumprir com o regulamento e identificamos possíveis melhorias que essas organizações possam realizar.

Criámos um questionário que disponibilizámos online e que as organizações puderam interagir anonimamente. Fizemos um total de 56 perguntas que dividimos em 18 conjuntos.

Tentámos saber se os participantes do nosso questionário teriam alguma função relacionada com segurança de dados, segurança informática avaliação de rico ou funções relevantes ao cumprimento do RGPD, tais como responsável pela proteção de dados.

Dado o grande enfase do RGPD na proteção online dos utilizadores e a sua informação pessoal criámos questões especificas direcionadas a serviços informáticos e plataformas online.

Nos anos mais recentes vimos os preços de serviços "cloud" diminuírem drasticamente e proporcionaram a massificação e adoção destes serviços online e "cloud". Questionámos os participantes ser teriam ou não este tipo de serviço e se os provedores destes serviços cumprem com as melhores práticas da indústria. Proporcionando, estes provedores, evidências de hardening bem como relatórios frequentes sobre a segurança dos serviços prestados por estes. Nesta orientação de pensamento perguntamos se os participantes têm um site ou página web. Esta pergunta serviu de base para a pergunta seguinte sobre a utilização de https na página/site, mais propriamente se usam cifras fortes bem como se mantêm estes servidores atualizados e a aplicação de todos os patchs de segurança recomendados. Para chamar a atenção de ferramentas online que possam ajudar na correta configuração de serviços online, questionamos se os participantes com este tipo de serviço teriam uma boa "nota" numa destas ferramentas.

Algumas organizações apenas possuem infraestrutura informática própria. No entanto, independentemente de como é constituída a infraestrutura de cada organização algumas perguntas mesmo que genéricas ajudam a avaliar a cultura informática e a forma como esta tecnologias de informação são empregues. Assim, questionamos sobre as estações de trabalho. Se estas têm antivírus, anti-malware e se são atualizadas frequentemente. O mesmo conjunto de perguntas foi aplicado a equipamentos de rede, firewalls, filtros de spam e servidores.

A segurança dos dados depende também da existência de firewalls com as mais diversas funções e configurações. Assim sendo, fizemos questões sobre a existência destes equipamentos e se os participantes consideram que estes equipamentos estivessem bem configurados para as funções de proteção da sua infraestrutura informática.

No questionário fizemos perguntas sobre a existência de políticas de atualização dos sistemas, bem como políticas de backups. Dentro da temática dos backups questionamos sobre testes de restauro desses backups e o sucesso desses testes. Testes de restauro e o sucesso destes testes servem para viabilizar os backups, bem como base das práticas correntes de inúmeras boas políticas de backups. Abordamos também a existência de políticas de passwords e a atribuição de acessos/privilégios, de acordo com as funções.

As questões sobre acessos são adequadas a diversas situações de controlo na utilização de recursos informáticos. Questionámos sobre acessos físicos a servidores e informação. Sendo no caso dos servidores, se apenas os técnicos devidos têm acesso a estes e se apenas estes são os únicos a administrar estes equipamentos. No caso do acesso à informação, se o acesso era restrito de acordo com a função e necessidade. Estas questões sobre acesso à informação foram mais a enquadrá-las no âmbito do RGPD. Questionámos se as pessoas que têm acesso a dados pessoais estão conscientes com as suas obrigações.

A proteção de dados, a recolha dos dados estritamente necessários, a obtenção do consentimento para a recolha desses dados, a liberdade para que os utilizadores possam ser esquecidos por uma dada plataforma ou corrigir e atualizar os seus dados pessoais, são conceitos reforçados e regulados pelo RGPD. Para as organizações estruturadas por departamentos isto significa a coordenação dos diversos departamentos envolvidos para o cumprimento de todos os requisitos do RGPD. Organizações mais desenvolvidas delegam esta coordenação a responsáveis pela proteção de dados, como regulado pelo RGPD.

No entanto nem todas as organizações têm acesso a este tipo de organização estrutural interna dada a sua dimensão e ou ramo de atividade, tentando chegar a um compromisso entre o desejável, o possível e a legalidade. Para o utilizador que visita ou usufrui destes serviços estas organizações são apenas plataformas/sites online com os seus dados pessoais onde estes depositam a sua confiança de uma correta utilização e proteção desses dados. Esta confiança deve ser transmitida pela organização aos utilizadores, no entanto os parceiros dessas organizações devem ter a mesma relação de confiança entre parceiros. Para validar a confiança das organizações participantes nos seus parceiros, questionámos se acham que seriam informados no caso de um dos seus parceiros ser alvo de um ataque informático. Esta questão é relevante para avaliar a reputação de uma organização bem com o mantimento do nível de confiança dos seus utilizadores e potenciador de uma atenção a potenciais vetores de ataque que possam emergir.

O nosso questionário foi programado de forma a não recolher informação pessoal dos participantes nem quaisquer dados que os pudesse identificar ou as suas organizações. O convite para participar no inquérito foi enviado por e-mail para pessoas, empresas e organizações que já tínhamos tido contacto no passado. Recorremos também a listas públicas de empresas e organizações de várias regiões do país e diversas áreas da economia Portuguesa que convidamos a participar. Antes de aceder à página do questionário, como acontece com outras páginas, o participante tinha que provar que é humano através de um desafio. Concluímos o nosso inquérito com uma questão de

satisfação dos participantes relativamente à contribuição que o inquérito teve para melhorar a sua sensibilização para a segurança, privacidade e proteção de dados.

Palavras chave: Privacidade, RGPD, Gestão de Risco, Melhores Práticas, Standards da Indústria

Contents

List of Figures

List of Tables

Chapter 1
Introduction

Software has been plagued by lawless practices of forcing personal data collection and collection without the explicit user's consent, being the norm for several decades. Even before the massification of the Internet, these despicable practices have been around and were the base of rumours for companies and state data collection. With time these rumours have been confirmed and accepted as facts (Verma, 2015) (Cornwall & Doherty, 2015).

Most software and some hardware we use comes with an End User Licence Agreement (EULA) that in most cases extends beyond reasonable, leaving the user with two choices; accept these EULA and abdicate of their rights or abdicate of their goods and sometimes prepaid fees.

These EULAs have been mostly created with a law jargon that most users do not understand and relegate to foreign countries laws. Even when the user is curious and starts reading them, they are overwhelmed with an unnatural language that relegates the essential information to the end of the EULA or expressed in fine print with the sole intent of misleading users. These EULAs originated a new problem, the user's acceptance of the EULAs without the user even reading them or understanding the extent of delegation of their personal data and privacy to these organizations.

Inserted deep in some EULAs comes a brief and vague description of the user's data collected and its intent usage. Before the full enforcement of the General Data Protection Regulation (GDPR) (Europiean Union, 2016), no mention of data processing practices was even present.

The new EULAs, post GDPR, have new vague information, like "we share your information with organizations within our group", mostly meaning that they sell our information to organizations that they have a bounding contract and, in some cases, also vague information about data processing.

For decades this unbalanced and unlawfully collection of user's data went on. Most like today, the main difference being that the user is somewhat informed and aware of some of this data collections, the organizations practicing these actions have become fearful of expensive fines they may incur and meddle with investors earnings.

It's the collection/mining of user's personal data by organizations not related with state security that the GDPR intends to protect against.

The GDPR was a departure from the directive 95/46/CE (European Union, 1995) in its scope, fines and applicability. All organizations that collect EU citizens personal data, being these organizations from European Union (EU) member states or from outside the EU are obligated to comply with GDPR. This means that even Small and Medium Enterprises (SMEs) must comply with the GDPR, the target of our study.

In light of the GDPR organizations must ask for user's permission to collect their personal information, inform the user of the data processing's they will be preforming and protect that data.

It's quite a task to protect electronic data, given all the vectors of attack that online and off line systems and networks may suffer. For online systems and networks, organizations have to defend themselves against attacks from states (Greenwald, 2012), criminal entities (NG, 2018), bots and the designated "script kiddies". For organizations that depend on offline networks they have to defend themselves from attacks perpetrated by entities willing to go the extra effort of compromising these networks (Falliere, et al., February 2011).

For SMEs the task of complying with the GDPR may involve extra effort that is outside their area of expertise, requiring an increase economical effort to encompass that expertise, by hiring expert professionals or services.

1.1 Motivation

The European Union approved the regulation 2016/679 also known as General Data Protection Regulation (GDPR) on 27 April 2016, this regulation went into enforce on 24 May 2016 and its application on 25 May 2018 (European Commission, s.d.). This regulation although not new, has been given a broader scope affecting organizations inside and outside the European Union (EU) that process EU member states citizens personal information. Another major difference are tougher fines.

Has of June 12 2019, law 58/2019 and 59/2019 was published in the Portuguese Republic Diary 151/2019 series 1 from August 8, 2019 assures the juridical order of execution of the GDPR. This new law adjusted the GDPR to the Portuguese economy, which entrepreneur fabric is mainly composed of small to medium sized enterprises representing 99,9%[1] of the country's entrepreneurship.

Portugal is strongly dominated by Small to Medium sized Enterprises. Is this reality that motivated us to assess the awareness of these organizations to the latest reaffirmation of the General Data Protection Regulation. In Table 1 we present the categorization of SMEs in the EU/EEC.

In 2017 the average size of the SMEs in Portugal was 2,47 persons[2]. This reality makes it difficult for such small sized organizations to be aware of all their duties in regard to the GDPR. The following research questions were motived by this reality:

1. Can these organizations be helped to focus on the relevant portions of the GDPR?
2. Are any platforms available that can help organizations to assess GDPR compliance and guide them?

1.2 Objectives

We have the objective of assessing GDPR awareness in SMEs through an online survey. Alongside our questions we intend on disseminating knowledge off free online tools available to anyone that participates in the survey.

The knowledge of this tools is passed on as additional information in some carefully posed questions that hint to the benefits of these tools.

Unfortunately, the most mature tools are niche tools that only focus in particular problems, like securing a DNS service or securing a webpage. A broader risk assessment or GDPR compliance tool is difficult to develop since most of the time these tools must

[1] According to the report by INE "Empresas em Portugal 2017" 2019 edition (INE, I.P., 2019), that mainly reports about the contributions of the companies to the development of Portugal and its grouse income. On Page 50 is the first comparison between small & medium versus big companies.

[2] This information was retrieved from the accompanying Excel sheets from the report "Empresas em Portugal 2017" 2019 edition (INE, I.P., 2019).

be customized to a particular organization. Some projects do exist that are trying to develop such tools and it's our objective to present them in this work.

1.3 Contributions

With this work we hope to disseminate useful tools gear to help the usage of secure and standardized practices when deploying information computerized systems.
We hint on some web services and entities known to evangelise and provide best practices and manuals.

1.4 Structure of the Document

This document is organized as follows.

Chapter 2, In this chapter we present the definition of some topics and concepts that are used throughout this work.
In Chapter 3, State of the Art, we try to present and describe some useful tools that are or will be available. These tools that can help organizations to prepare tests and some aspects of the GDPR compliance. We also review and discuss current publications and research on GDPR.
Chapter 4, Presents a detailed description of the survey.
Chapter 5, Survey analysis and interpretation of the results.
Chapter 6, In this chapter we present our conclusion and some thoughts.

Chapter 2
Context

This chapter presents the basis for the subjects addressed in this work. Some definitions tend to change with their environment, intent, social and political view. We will be referring to these topics based on these definitions.

2.1 Personal data

Generally, persons have their own idea of what they consider personal and private data and which of that data they are willing and unwilling to share. The 1st paragraph of article 9º of the GDPR defines what data can't be subject to processing. According to this paragraph, these are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. The same has been transposed to national law under article 6º of law 59/2019. By law this is personal data; health, genetic and biometric data can only be collected and/or processed in special conditions and require Data Protection Agencies (DPA) approval.

2.2 Consent

The collection of user information has become a fact of our society. It evolved from metadata collection about software, hardware to user behaviour and profiling. The companies initially denied these practices, then they acknowledged them and for some time now they have been asking our consent to collect user's data. The GDPR, among other things, came to regulate the lawfulness of data collection and the attainment of consents, by defining the general principles of personal data processing, it's special cases, conditions and purposes.
Article 16º of the law 58/2019 redefines and clarifies the circumstances and age in which is licit to collect or process minors' personal data and their consent.

2.3 SMEs

The definition of Small and Medium size enterprises encompasses organizations categorized as Micro, Small and Medium. SMEs are statistically and legally important to any economy.

The category covers the most diverse businesses that together build up the core of most market economies, accounting for the majority of employment, innovation and economic interaction (Kasl, 2018). More so in the case of Portugal where the enterprise fabric is 99,9% composed of enterprises in this category.

Legally the categorization of any enterprise is a complex balance between the number of employees, annual turnover and annual balance sheet total.

Table 1 categorizes SMEs according to the EU/ECC.

Micro enterprises: with less than 10 persons employed and less or equal to 2 million euros annual turnover or annual balance sheet total.
Small enterprises: with less than 50 persons employed and less or equal to 10 million euros annual turnover or annual balance sheet total.
Medium-sized enterprises: with less than 250 persons employed and less or equal to 50 million euros of annual turnover or less or equal to 43 million euros of annual balance sheet total.

Table 1 - SMEs Categorization[3]

In summary **Small and Medium sized enterprises (SMEs)** are companies that employ 1 to 249 persons, present an annual turnover equal to 50 million euros or less and total sheet annual balance equal to 43 million euros or less. This means that enterprises with less than 10 employees can be considered a small or even medium enterprises according to the turnover or balance sheet total.

[3] EU recommendation 2003/361 (THE COMMISSION OF THE EUROPEAN COMMUNITIES, 2003)

Start-ups with their economical and innovative potential are among these microenterprises. SMEs encompass countless unique business settings including the smaller one-person start-up as well as established medium enterprises with complex and developed corporate structures. SMEs play a uniquely dichotomic role in the economy of all countries. This category includes the most progressive and innovative start-ups and pioneers of the digital economy, as well as many very static entities, that stick to the traditional business models and are oblivious to or purposely rejecting the new technologies.

2.4 Organizations

Many times, the definition of organization and enterprise is confusing. Being that enterprises can also be defined as organizations creating greater misunderstandings. For the most part enterprises and organizations have the same definition that's why there is this ambiguity between the two. However, enterprises always have profit as their goal, organizations on the other hand may also be non-profit. So, the distinction of enterprises and organizations is: Enterprises are solely considered for profit and organizations on the other hand are majorly considered non-profit.
The GDPR does not distinguish between enterprises and organizations, if they collect personal information then they must abide by the regulation.

2.5 Best practices

According to the merriam-webster dictionary the definition of best practices can be summoned up as, "a procedure that has been shown by research and experience to produce optimal results and that is established or proposed as a standard suitable for widespread adoption" (merriam-webster Incorporated, 2019). Depending on the usage, an accepted best practice may impact negatively the stability and/or performance of a system. As such, the starting point for the deployment of any set of best practices should be the guidelines of the product(s) being used. Some organizations[4] provide sets of best practices and guides suitable to several usage scenarios. Given that these are the result of

[4] Organizations that provide cybersecurity related best practices guides are ENISA (The European Union Agency for Cybersecurity (ENISA), 2019) and CIS (Center for Internet Security, Inc, 2019)

experience and the development of knowledge a regular update is needed to keep up with new improvements and discoveries.

2.6 Security, risk management and best practices

Although many times used together, security, risk management and best practices may have different objectives. Each of them may be applied independently or used to complement each other with the goal of creating a safe, resilient, robust and easily maintainable system.

Generally, when applying best practices, the objective is to create an easy to manage, robust and resilient system capable of a good level of security, manageable risk and the best possible performance. However, best practices may have a single point of focus be it a program/application or an identified usage, neglecting other interactions and therefore not complying with the general concepts of risk management and security. This single focus results in some software producers creating their own set of best practices geared at providing the best possible service for their products.

Security at its basis is the defence against data compromises, attacks and the eradication of vulnerabilities. On the other end, risk management takes security concerns and leverages them with business objectives. Risk management also encompasses the whole organization by assessing the importance of each system and plans the organization's software and systems life cycles.

According to the area in which the organization operates, the usage of risk management frameworks may be reduced by their obligations to comply with certain requisites. One example; organizations that work with NATO may be obligated to comply with the NIST framework in determent of others.

These frameworks all cover cybersecurity, and/or cyber risk management:

- NIST (National Institute of Standards and Technology, 2019)
- ISO (International Organization for Standardization, 2019)
- COBIT (ISACA, 2019)

The choice of framework may be suitable to the transactions these organizations do or intent to do in the future.

2.7 Encryption

Encryption according to the Cambridge dictionary is defined as; “to put information into a special form so that most people cannot read it:” (Cambridge University Press, 2019). There are several forms and grades of encryption, that are mainly defined in military and civilian, being the difference between them the algorithms applied in each case.
These forms of encryption can be applied in the three states of the information(data) (Almulla, et al., 2014).

- In transit, data being transmitted and/or received
- In use, data being actively or readily available
- At rest, store data or offline

We consider these to be the three states of data.
A misconception most persons have is that in-transit communication encryption is enough to protect data.
Another is that disk level or file system encryption does not ensure the security of data in rest whenever the operating system is in execution, the same also applies to database encryption, in both cases any direct access to the data will result in usable information.
In-execution encryption or application/program level encryption can protect even were filesystems or databases encryption fails to do so. This is possible given that the encryption and decryption of data is done by the program on a per access basis, circumventing the program will result in obtaining encrypted data therefore unreadable. There is an increased overhead associated with working data this way. This kind of encryption can be combined with other encryption methods like in-transit and in-rest to better protect the data. This usage of encryption for itself does not guarantee data masking/obfuscation (Bakken, et al., 2004) or anonymization since this concept has different rules by themself.

2.8 Fines

GDPR fines are calculated and administered by the supervisory authority of each member state. The following criteria are to be used in the determination of an applicable fine to a non-compliant organization (European Union, 2017):

- **Nature of infringement**: number of people affected, damage they suffered, duration of infringement, and purpose of processing

- **Intention**: whether the infringement is intentional or negligent
- **Mitigation**: actions taken to mitigate damage to data subjects
- **Preventative measures**: how much technical and organizational preparation the firm had previously implemented to prevent non-compliance
- **History**: (83.2e) past relevant infringements, which may be interpreted to include infringements under the Data Protection Directive and not just the GDPR, and (83.2i) past administrative corrective actions under the GDPR, from warnings to bans on processing and fines
- **Cooperation**: how cooperative the firm has been with the supervisory authority to remedy the infringement
- **Data type**: what types of data the infringement impacts; see special categories of personal data[5]
- **Notification**: whether the infringement was proactively reported to the supervisory authority by the firm itself or a third party
- **Certification**: whether the firm had qualified under approved certifications or adhered to approved codes of conduct
- **Other**: other aggravating or mitigating factors may include financial impact on the firm from the infringement

Further information available in art. 83 of the GDPR, General conditions for imposing administrative fines[6].

Is with these definitions in mind that we will relate to these topics in this work and what is the intent meaning we expect the audience to understand.

[5] https://www.gdpreu.org/the-regulation/key-concepts/special-categories-personal-data

[6] https://gdpr-info.eu/art-83-gdpr/

Chapter 3

State of the art

In this chapter we investigate the current state of the art with regards to published works, tools and relevant information to the compliance of the GDPR by SMEs.
We give an in-depth overview of tools, projects and services developed to help SMEs assess GDPR compliance, better configure and defend their assets.

3.1 State of The Art

Studies assessing GDPR impact on SMEs are scarce and with time they will likely increase. The existing studies are mostly generalist or geared at big enterprises. However, one such study carries out an assessment on awareness and preparedness of Portuguese SMEs through the voluntary participation in a presential survey (Freitas & Silva, 2018). In this survey participated ten organizations from different regions of the country. The surveys were carried out with the participation of the involved SMEs senior officials whom, given their position and/or responsibility might influence collection, storage and processing of personal data within the organization.
In the study the following subjects were analysed and processed according to the obtained responses:

- Knowledge, Consent Processing Principles and Registry of Processing Activity
- Labour Law and Security
- Rights of Data Subjects
- Data Protection Officer
- Contracts
- Transfer of Personal Data to Third Countries or International Organizations
- Training
- Accountability of Data Controller
- Notification of Personal Data Breach of the Supervisory Authority

The study concluded that regarding the obtention of consent, processing principles and the registration of processing activities, the interviewees were less knowledgeable of their obligations and duties.

This lack of knowledge extends itself into labour laws and their obligations to implement secure mechanisms on the storage of personal data as well as processes compliant with the new GDPR. All the interviewed replied that they had less than 250 employees and that they didn't had, to that date, employed a Data Protection Officer.

Of the organizations interviewed, none had data transfers to countries outside the EU/EEC. The outcome of this study can be best understood by skimming through Figure 1 and its pie representation of all covered subjects and percentage of responses per subject.

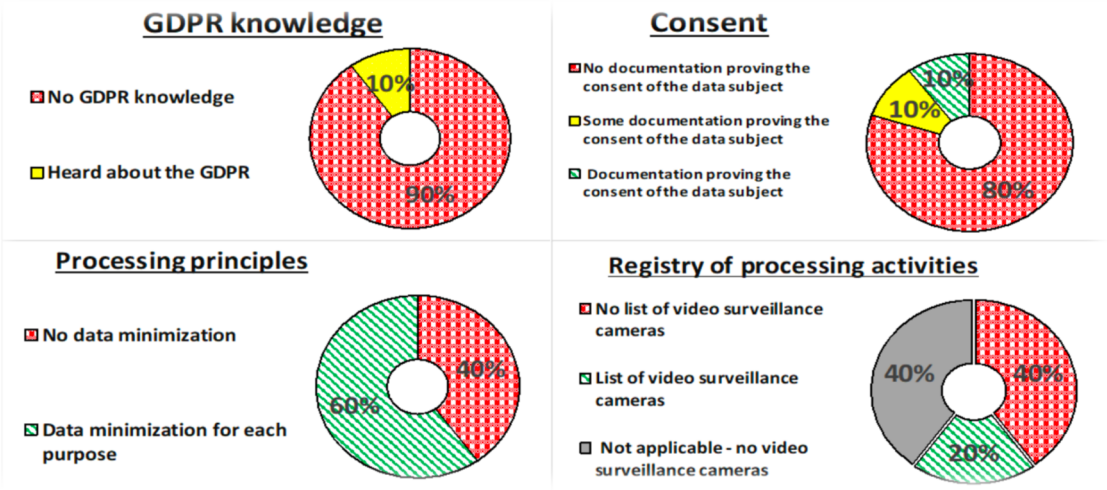

Figure 1 Knowledge, Consent Processing Principles and Registry of Processing Activities extracted from (Freitas & Silva, 2018)

Clearly the protection of rights and freedoms of natural persons is the moving force behind the EU regulation. If a specific data processing practice should likely result in a high risk to those rights and freedoms, then a Data Protection Impact Assessment (DPIA) is mandatory. This DPIA must be carried out prior to those processing practices.[7] Some European countries have dedicated Data Protection Authorities (DPA) that analyse these DPIAs. DPAs have different levels of involvement according to their budget and personnel, nonetheless they have the same objectives. Some member countries have

[7] Article 35 of the RGPD EU2016/679 (European Union, 2016)

several DPAs, like Germany that has 16 state-level DPAs and a federal one. Portugal has a single DPA, the Comissão Nacional de Proteção de Dados (NCDP)[8]. In Table 2 we present some DPAs budgets and the number of employees.

NCDP is an independent administrative body with powers of authority throughout the Portuguese national territory. It is endowed with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection, with strict respect for human rights and the fundamental freedoms and guarantees enshrined in the Portuguese Constitution and the law (Comissão Nacional de Protecção de Dados, s.d.). The Portuguese DPA, NCDP, which is regulated by law 43/2004 from August 18 and delegated by article 3rd through article 8th of Portuguese law 58/2019, with national control rights pertaining to the GDPR.

In line c) of the 1st paragraph of article 6th of this new law the NCDP is delegated with the responsibility of creating a list of data processing methods that must be subjected to a DPIA as stated in the 4th paragraph of article 35th of the GDPR. Paragraph 1st of article 7th of law the new Portuguese law delegates the NCDP with the creation of a second list of processing methods that does not require a DPIA, however the 2nd paragraph states that such list does not negate the creation of a DPIA for whiling parties that still wish to do these assessments. The 3rd paragraph of article 6th from 58/2019 states that both lists must be published in the official webpage of the NCDP.

On September 23rd, 2019 the NCDP presented the deliberation 2019/494 announcing that will not be applying the following articles from law 58/2019.

i. Article 2nd, n 1 and 2
ii. Article 20th, n 1
iii. Article 23rd
iv. Article 28th, n 3, line a)
v. Article 37th, n 1, lines a), h) e k), and n 2
vi. Article 38th, n 1, line b), and n 2
vii. Article 39th, n 1 and 3
viii. Article 61st, n 2
ix. Article 62nd, n 2

[8] Comissão Nacional de Proteção de Dados, https://www.cnpd.pt

This deliberation is the result of an assessment of the law 58/2019 by the NCDP which concluded that the above articles violate the European Union law. For matters regulated in these articles the GDPR will be the foundation to future deliberations.

Country	Budget (M Euros)	Number of employees (FTE)
Sweden (2014)	4.6	40
Italy (2015)	19.2	121
Romania (2015)	0.7	41
France (2016)	19.0	192
United Kingdom (2016)	26.5	442
Germany (2016)	13.7 (federal)	110 (federal)
Ireland (2017)	7.5	60
Portugal (2019)[9]	2.15	7[10]

Table 2 Member states DPAs number of employees and budgets

3.1.1 Where to start?

Some SMEs, due to their size, may have to search for help or even transfer some of these responsibilities and liabilities to other expert organizations that outsource their knowhow and expertise. Many new offers have popped up in the market, offering consulting services in areas related to the GDPR.

General doubts, doubts of member states adaptations and doubts how particular practices may fare against the GDPR will always exist, The EU members states DPAs are a good starting point to get more information about the GDPR or just to keep up to date. These members DPAs will have documentation and information in the members native language which may also include information adapted to those members reality and legislation. Alternatively, there is the official site of the EU that will always have up to date information about the GDPR[11].

9 https://www.cnpd.pt/media/2qjec4m0/plano_atividades_2019.pdf

10 https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/

11 https://gdprinformer.com/getting-started-with-the-gdpr

3.1.2 SMOOTH Project

The Smooth Project[12] is a project funded under the EU Horizon 2020[13] that aims to help Micro enterprises to adopt and comply with the GDPR. Designing easy-to-use and affordable tools aiming at generating awareness in SMEs to their GDPR obligations through voluntary analysis of their level of compliance with the data protection regulation.

This project is the result of the Smooth consortium, which is comprised of twelve partners from six European countries. This consortium has as members universities from Spain and Belgium, Spain's data protection agency and other organizations from the United Kingdom, Poland, Latvia and France (smooth, s.d.). The project goal is "to contribute to the respect citizen's privacy rights as well as to avoid that SMEs are penalized for not complying with the new regulation"[14]. The project intents to achieve this goal by publishing an online interactive handbook specifically aimed at SMEs using mobile and web technologies in conjunction with a cloud platform combining several advanced technologies in the areas of machine learning, text mining and data mining in order to produce customized reports on the most critical aspects of the GDPR to the organizations that request them. The project objectives are also to provide SMEs with advanced tools to solve the detected issues (Presas, 2018).

3.1.3 SSL Server Tests

Other projects were created with the purpose of helping professionals and aficionados understand, configure and manage several Internet exposed services, like web and e-mail servers. These projects offer free and commercial analysis scans of these services, that result in recommendations complying with the industry best practices. Depending on the project, a free analysis may evolve into a commercial proposal of consultation services.

---

[12] https://smoothplatform.eu

13 Horizon 2020 is the financial instrument implementing the Innovation Union, a Europe 2020 flagship initiative aimed at securing Europe's global competitiveness. (European Comission, 2019)

[14] Citation of Rosa Araujo, SMOOTH's project coordinator from Eurecat extracted from the project page. (Presas, 2018)

The tool SSL Server Test[15] by Qualys labs is free of charger even though the organization that operates the service has a for profit business model.

SSL Server Test goes beyond the http(s) protocol. The service is comprised of several scans and analyses of a given proposed domain site for misconfigurations, known vulnerabilities, compliance with known best practices and certificate correctness. The analyses are comprised of several evolving tests, that leverage information queried from the server like DNS, SSL configurations and other more general server configurations. These are not so much web server (program) vulnerabilities or in the webpage presented but analysis of the correct configuration of the web server to provide https pages. However, recommendations may infer on known vulnerabilities of certain web servers and plugins versions, such suggestion may also go against the use of vulnerable cyphers in the protocol with the respective justification and how to proceed with the improvements and configuration. At the end of a successful scan each domain site is scored, being that the most desirable score is A++. This score was presented in the last few years and is mainly awarded to domain sites that apply the latest known best practices, at present one such example can be the adaptation and use of TLSv1.3.
In previous versions the maximum score was A+. The scoring system varies from F, C, B, A, A+ to A++. The scores may vary according to the knowledge of existing vulnerabilities. A domain site with a score of A++ may a few days later receive a score of B if a configuration in use is deprecated and considered severe enough to merit this severe demotion. This practice is used to promote rapid responses by the persons responsible for the domain site regarding severe new known vulnerabilities and encourage them to take corrective measures as soon as possible. A frequent rescan of domain site is highly recommended.
A good score in this site will assure professionals that they are doing their best to protect users' communications with their domain sites using the latest technologies and known best practices.

[15] https://www.ssllabs.com/ssltest, online free service that performs a deep analysis of the configuration of any SSL web server on the public Internet

3.1.4 E-mail server Tests

The proliferation of phishing scams, spam and code/programs that may cripple devices, computers and entire networks are examples of unwonted e-mails. To combat and reduce, unwonted e-mail and prevent e-mail servers hijacking. The configuration of e-mail servers has evolved drastically in the last few years in order to accomplish these objectives.

According to the e-mail server software selected, many configuration combinations may exist. Fine tuning those configurations can be time consuming. Aimed at helping all interested, identify misconfigurations and correctly configure their e-mail servers the site MxToolbox16, provides their users with a set of tests to achieve this. These tests include "listing MX records for a domain in priority order, MX lookup directly against the domain's authorities name server so changes to MX Records should show up instantly.". There is also a diagnostics tool that "will connect to the e-mail server, verify reverse DNS records, perform a simple Open Relay check and measure response time performance." The available tools can also check if any of the MX records (IP Addresses) is blacklisted against 105 DNS based blacklists. (Commonly called RBLs, DNSBLs). (MxToolbox, Inc., 2019)

After the diagnose, we are presented with a dashboard. The dashboard is comprised of the number of total tests realized along with the number of passed and the number of failed tests.

This tool helps all that use it to secure their servers, their communications and guarantees compliance with industry standards ensuring to other servers that they are trustworthy hence guaranteeing the correct flow of e-mails.

Once the e-mail server is correctly configured, compliant and trustworthy some organizations that depend on e-mail for their marketing can also inspect the construction of their marketing e-mails with isnotspam, another online tool.

3.1.5 Isnotspam

Most organizations rely on e-mail to contact their affiliates, customers and potential customers. For this, a correctly crafted e-mail is crucial, avoiding wrongful identification

16 https://mxtoolbox.com/aboutus.aspx

of these e-mails as spam or phishing, prompting the recipient e-mail server to reject these e-mails or categorise as spam.

The site www.isnotspam.com offers its help, on the technical part, so that when crafting newsletter and marketing offerings, its users can spend more time with the design, content and message of their e-mails. “Simply compose your email and send it to the email address listed at the top of the page, using your usual mail server. You will be able to view an online report detailing potential problems (if any) with your email. Our software automatically checks the main elements which cause emails to be rejected by recipient mail servers.” (isnotspam, s.d.)

3.1.6 webcheck.pt

webcheck.pt17 is a new online tool made available on 08 of July 2019 and is the responsibility of the Portuguese cybersecurity centre CNCS and Associação DNS.PT (Associação DNS.PT, 2019).

This is another technical tool aimed at helping identifying misconfigurations in several services like DNS, HTTPS and MX (mail). This tool uses domain name to query its available services and test for the most common misconfigurations. At the end, we are presented with a report of the assessment and some recommendations if applicable.

Although this tool doesn’t dive as deep as some other tools, it has the benefit of gathering in a single tool tests for several services. This tool may be augmented with time providing more tests and/or functionality.

3.2 CIS Standards

Data protection starts at the human side of the equation. The persons involved must be willing to go the required length and do their best to:

- Only share the needed information
- Protect the collected information

17 https://webcheck.pt/pt/sobre/

No one will store gold in a straw safe and hope that's enough to keep it safe. Then, we shouldn't assume that no one will think that just storing information in a given system is enough to keep it safe.

CIS that stands for Center for Internet Security, which "is non-profit entity that harness the power of a global IT community to safeguard private and public organizations against cyber threats." (Center for Internet Security, Inc, 2019) This entity provides global standards that are recognized best practices for securing IT systems and data against the most pervasive attacks. These guidelines are continuously refined and verified by volunteer's and a global community of experienced IT professionals. CIS provides controls and benchmarks to configure and harden systems following IT established best practices, these best practices can be used in conjunction to risk management frameworks. Some of this information is provided free of charge. More up to date recommendations (controls and benchmarks) are available to paying customers and partners. Other ways of obtaining the most recent benchmark are by participating in the revision and creation of new benchmarks. This is achieved by enrolling and, if possible, participating in the mailing list of each benchmark.

Chapter 4

Survey

Surveys are valid means of understanding compliance levels and awareness on any given subject. Therefore, we envisioned an online survey to assess the level of awareness in Portuguese SMEs to the GDPR. We protected the survey from bots with a challenge to verify that the participant is human. This is a protection offered by the chosen platform for the survey.

The survey is composed of some unique questions that reflect our perception of security and privacy regarding IT systems.

Along with those questions, we do the same mandatory questions that are usually present in any academic and commercial enterprises surveys. The survey is constructed in such way that it's impossible for us do identify the participants specific role or origin. However, we do query if the participants have any cybersecurity related role or data protection related occupation.

As previously mentioned, our "unique" questions are posed in such a way to create curiosity and awareness to tools that, at this time, are freely available and can be used as web services. These tools may in some ways be beneficial to any organization, to better secure their business, optimize their systems configuration or just assert their systems compliance with industry best practices.

The survey is split up into 18 groups with a total of 56 questions. Five of the groups have mandatory questions. These questions were created with the intent that our participants may optout of some groups that may not apply to them. Also, we made the first and last question of the survey mandatory, more on that bellow.

4.1 Survey

With the first group of questions we asked our participants the size of their organization and their area of activity. The very first question aside from categorizing the size of the organization, we made it mandatory to help us exclude organizations outside our intended scope.

In the second group of questions we assessed the responsibilities of the participants. We asked our participants if they had any responsibilities that were related with IT, data protection or risk management? We close this group by inquiring our participants if their organization has conducted any internal survey on how would they react in the event of a cyberattack.

The third group is used to assess awareness of the organization employees regarding insecure communications.

Then, we went on and created four groups about data protection.

The first group on this topic of data protection, surveys our participants about the conditions in which the data was stored, if they were protecting the access to the organizations infrastructure and if they were encrypting their devices.

The second group about data protection is used to inquire in which conditions the organization was conducting their data collection and if a clear and informed consent was being obtained from their users.

The third group regarding data protection is about internal data protection. We tried to assess how the organization was dealing with internal communications, video surveillance and telephone recordings if any.

The last group of questions on data protection is about user rights and data transfer to third party companies and countries outside the EU. We went on to inquire the participants on how the organization was dealing with the user right to be forgotten, to alter and update their personal information. We also asked if the organization was sharing users' information with third party organizations or if they transferred that information to countries outside the EU in accordance with the GDPR.

Our 8th group of questions is an adaption to current times when most organizations are moving or have moved part of their infrastructure to the Cloud. This group starts with a mandatory question, asking our participants if they have hosted solutions. This question helped us validate the rest of the responses in this group. Essentially this group is about following best practices and evidence of those best practices.

The second question on hosted solutions, we asked if the Cloud provider provided any guarantee that they were adhering to security best practices for the contracted service.

In the third and last question of this group, we asked if the Cloud providers supplied evidence of adopting hardening best practices and these providers offer security analysis reports.

The 9th group is derived from the same reasoning that compelled us to ask the previous group of questions. This group is solely devoted to webpages, it has the intention of assessing the organization employment of strong cyphers on their webpages and if they were using a scoring system to evaluate their webpage adherence to industry standards.
We started this group of questions with another mandatory response, like in the previous group, with the same objectives.
Did the organizations employ strong cyphers on their site/webpage? This is the second question on this group. In the third question we asked if the organization applied all security recommendations to their site/webpage.
Lastly, in the fourth question we asked if the organization webpage had a score of at least "A" in the analysis tool from Qualys, the SSL Server Test. Clearly this last question was intended to make the participants aware of such services available on the Internet.
Secure communications is the name of the next group where we asked the participants about the usage of secure and authenticated communication channels, the usage of VPNs when communicating with the organization, the usage of at least WPA2 on WIFI and the existence of segregated WIFI networks for employees and visitors.
For group eleven we asked our participants about users and password administration, and the usage of password and role base authentication policies.
In group twelve we asked if they had configured their firewalls to prevent attacks and if they were employing e-mail and malware protection. Following this idea, we asked in the following group about systems update and update policies both for computers and infrastructure components like switches and firewalls.
The group fourteen is solely devoted to backups, we asked our participants if they had backup policies, off-line backups and if they had successfully tested backups restoration.
For the 15th group we dwell on software and driver's development. This group starts with a mandatory question, meant to rule out organizations without this speciality. The questions in this group were geared to cybersecurity, development and test best practices related with software development.
Group sixteen is about incident response. We asked our participants about incident response from a technical standpoint and incident communications with their costumers and the public. In the seventeenth group, that we named penalties, we asked our participants if they were aware of the penalizations and value of the involved fines, in case of GDPR non-compliance.

Lastly, we asked our participants to evaluate and reflect on how much they think the survey has helped their data protection and privacy awareness, by scoring the survey from 1 to 10. The score system is thought-out to start at 1 which means that the survey has not influenced their awareness in those subjects. The increase in score meant an increasingly contribution to the participant's level of awareness.

Chapter 5

Results

In this chapter we present our survey result. The survey was conducted online with the recourse to the LimeSurvey platform. The survey was configured to only collect the answers anonymously. We began by asking our network of acquaintances to participate in the survey. To captivate the participation of organizations we used several means including resorting to e-mailing and social platforms with limited success. Some graphs and tables already express some interpretation of the collected data. We make the raw data available in Appendix B. Further interpretation can be asserted from the raw data, however is outside our intended scope.

Of all the visitors that initiated the survey we had 8 that fully completed our survey and were considered valid. The participation is best understood visually in Figure 2.

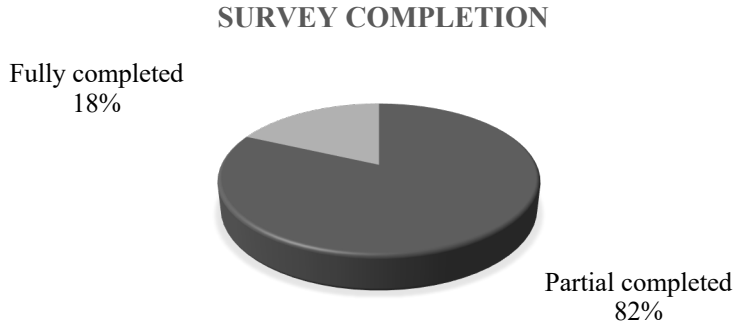

Figure 2 Participation

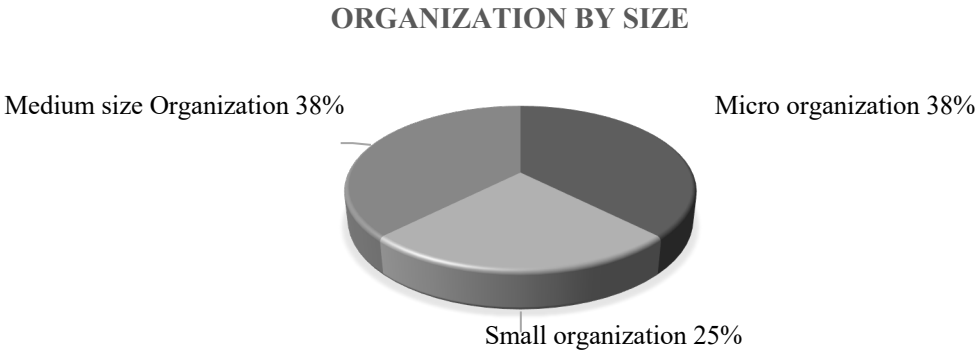

Figure 3 Organization size

Thirty eight percent of the participations were from medium sized organizations, 25% were small and another 38% were micro-organizations, the categorization of the organizations size is also visually demonstrated by Figure 3. In Table 3 we present the survey participation based on their field of expertise and or commercial activity.

Activity	
No group selected	1
Food and beverage	1
Food commerce	1
Cosmetics and perfumery	1
Computer and Technological Services	3
Tourism	1

Table 3 Distribution of responses by business or activity sector

Figure 4 combines apparent unrelated questions the answers do indicate some relation, but doe to the size of the organizations the majority of the participants have multiple responsibilities revelling a common reality in micro and small organizations, the overlapping of functions. The majority of the participants had functions related to IT security, risk management and data protection. We also had responses that indicated that some of the participants don't have a person accountable for IT security, data protection or risk management.

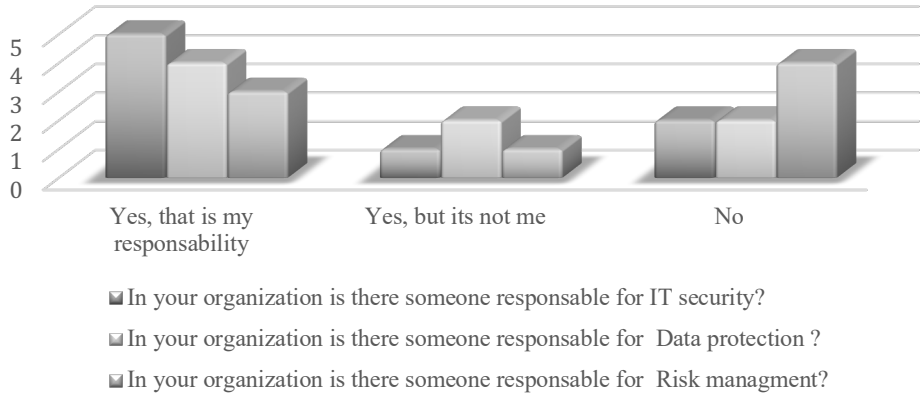

Figure 4 Participants of the survey responsibilities

Fifty percent of participants have done some security assessments to their organization on how they would react in case of a cyberattack. One third claimed to already have done a GDPR compliance assessment, reflecting the general interest of organizations in GDPR compliance as demonstrated in Figure 5.

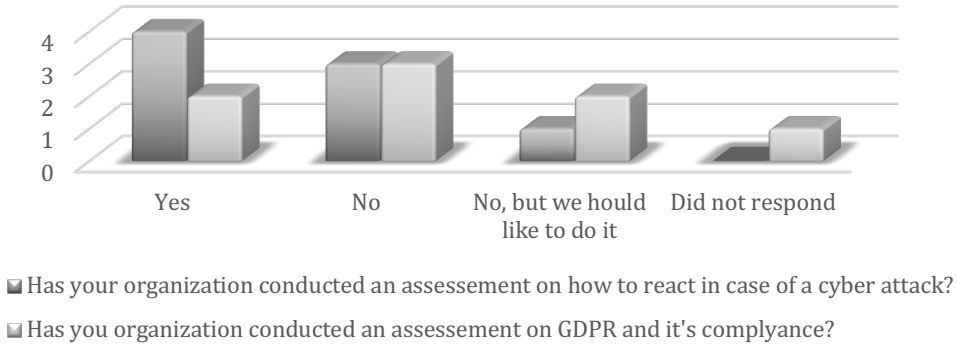

Figure 5 GDPR assessments in the organization

Most organizations seem to be aware of the security risks associated with the processing of private data pertaining to their users/customers. At least 50% answered that they had knowledge on how to handle insecure information and that their employees also had the knowledge on how to minimise security risks. Even a greater percentage, approximate 78% answered that the users that had access to private information had knowledge of their obligations regarding access to that data, as demonstrated in Figure 6.

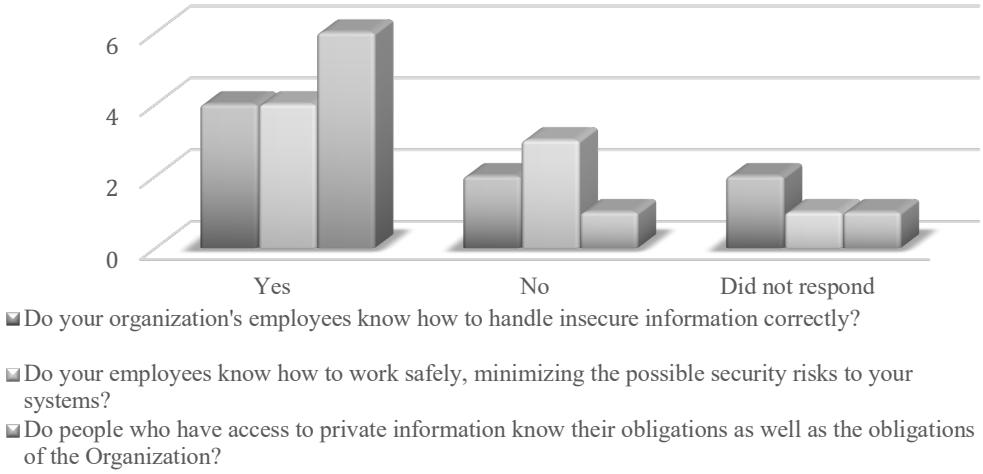

Figure 6 User's obligations and secure/insecure data

When asked about secure communication channels with their customers, 38% answered that they didn't have a communication channel and 25% did had a communication channel but it wasn't a secure one. 37% answered that they had a secure channel to communicate with their customers, as demonstrated in Figure 7.

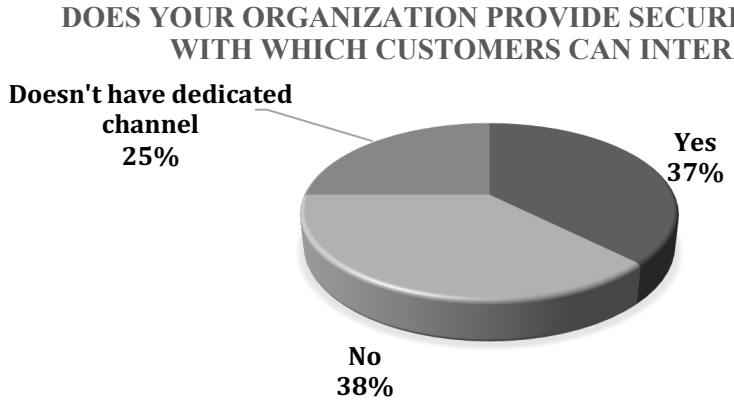

Figure 7 Availability of secure communication channels

Fifty percent of our participants has responded that they stored their information encrypted. To the question if the organization encrypted their equipment's to prevent data retrieval in case of equipment loss or theft, 50% has responded positively. Demonstrating the increase awareness to data protection on mobile devices.

Figure 8 Availability of necessary tools to secure personal information

When asked if their organization had the necessary tools to ensure the security of the collected personal information, 37% responded positive to this question and 38%

responded that still didn't have those tools. We believe that further studies are needed to clarify these responses as visible in Figure 8.

Figure 9, reflects the concerns with remote users and the equipment's they use. If these equipment's are shipped with encryption activated to prevent data retrieval in case of loss. Only approximately 50% responded that they encrypt these devices. The same percentage was obtained for the encryption of store information. Only servers and network encryption faired a little better. The safety of IT infrastructure was also positive, with approximately 62% of participants responding that access to the infrastructure, servers and network, is limited according the persons responsibility.

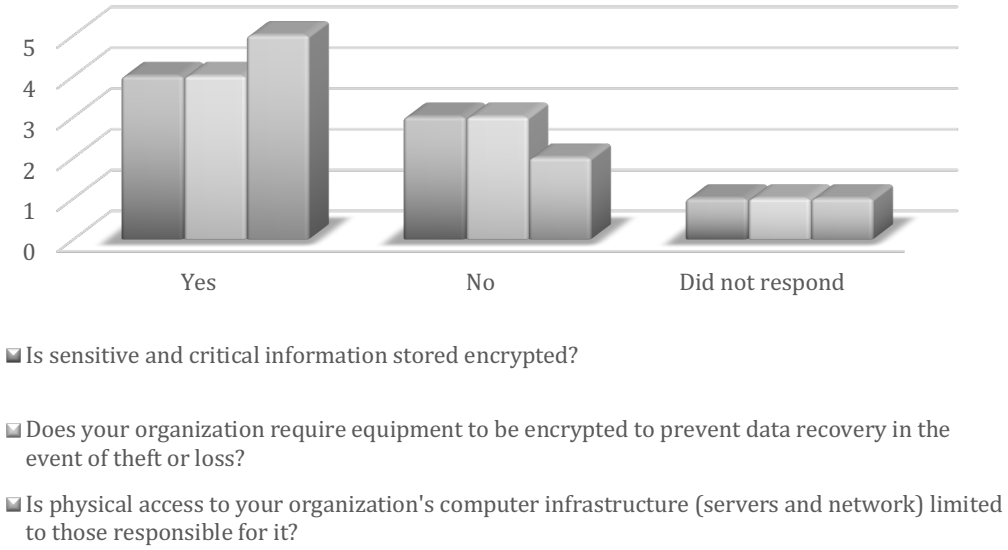

Figure 9 Encrypted information and equipment's

When questioned about the personal information collected, 78% of the participants have answered that they only collect the strictly necessary personal information. Regarding the obtention of clear written consent about the personal information collected, 50% claimed to have clear written consent for the collected personal information, demonstrated by Figure 10. To the question; if the organization has reviewed how and in which circumstances the consent was granted, 50% have responded positively. Demonstrating awareness of data collection laws.

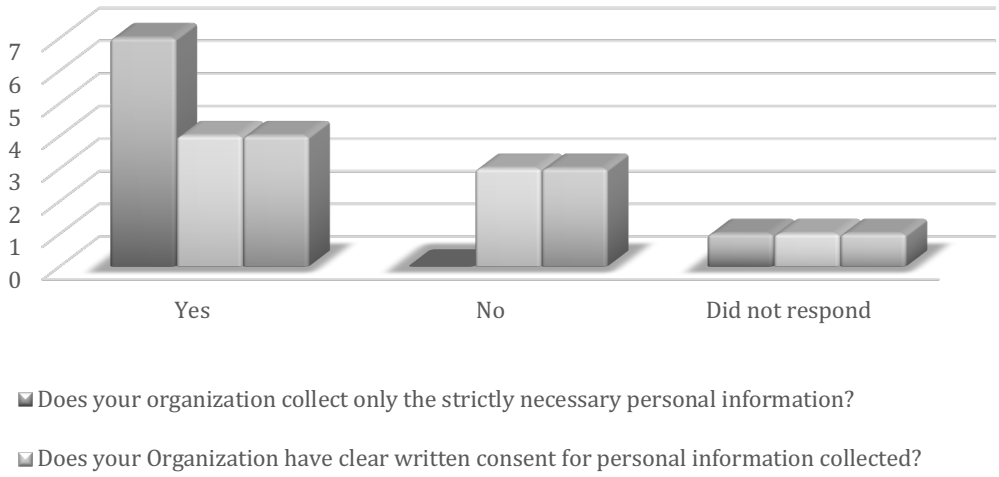

Figure 10 Collection of the strictly necessary information

The Question, “does your applications/programs encrypt their data …”, seemed to create great confusion and misunderstandings. Some professionals replayed with the question “do you mean, do we obfuscate our data?”. Encryption at program/application level does not mean that the complex rules of personal data obfuscation are met. So those would be two different questions. To this question 50% of the participants responded that they also encrypt data at the program/application level, as documented in Figure11.

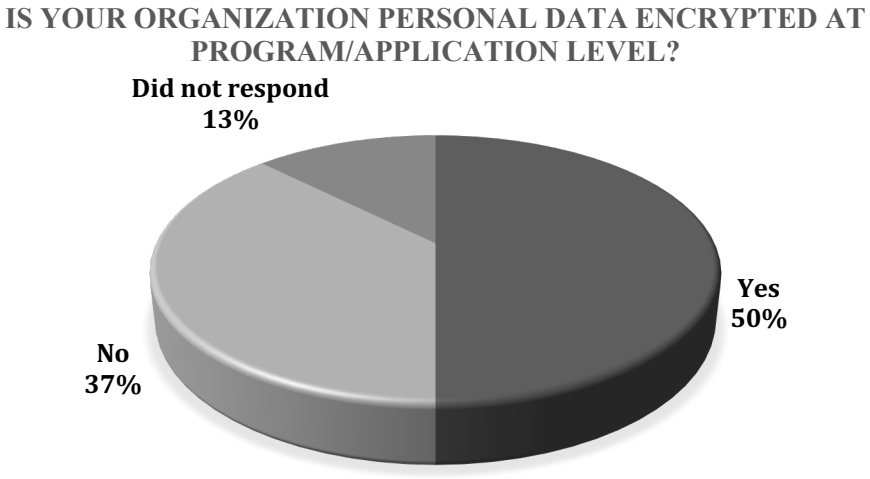

Figure 11 Usage of program/application-level encryption

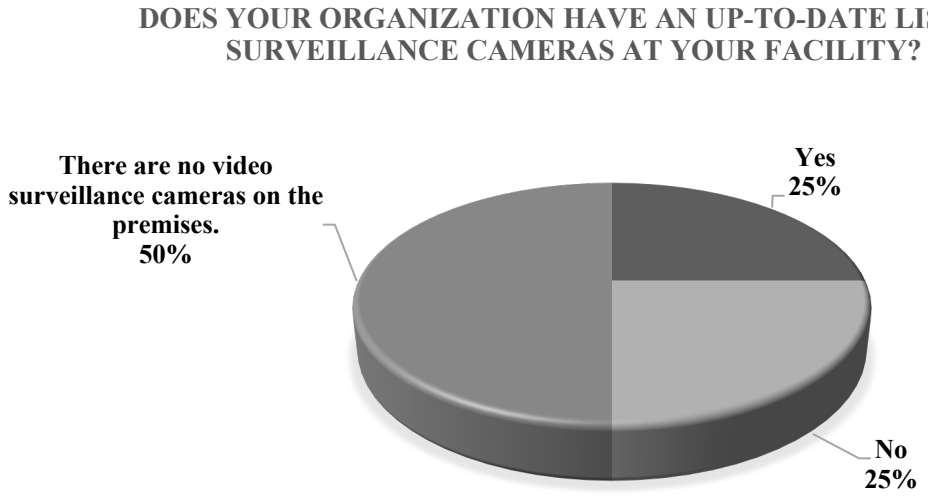

Figure 12 Existence of video surveillance

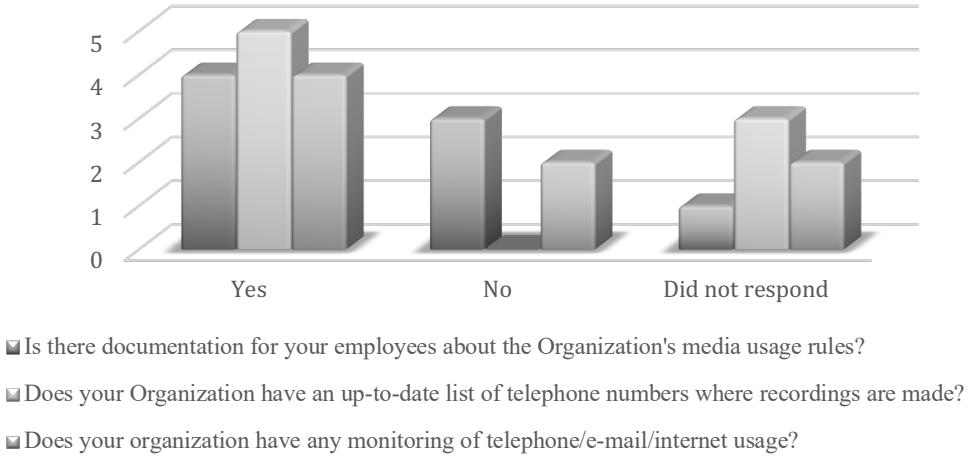

Figure 13 Availability of user monitorization and documentation

The existence of surveillance cameras in their organization was answered positively by only 25% of the participants, as demonstrated in Figure 12.

When questioned about the usage of the Organization's medias and the existence of documented rules and procedures, 50% answered that they had that kind of documentation available. Approximately 62% responded that they had an up-to-date list of the telephone recordings. Once again, 50% of the participants responded that they monitored communications at their organizations, being those telephonic, e-mail and or Internet, as visible in Figure 13.

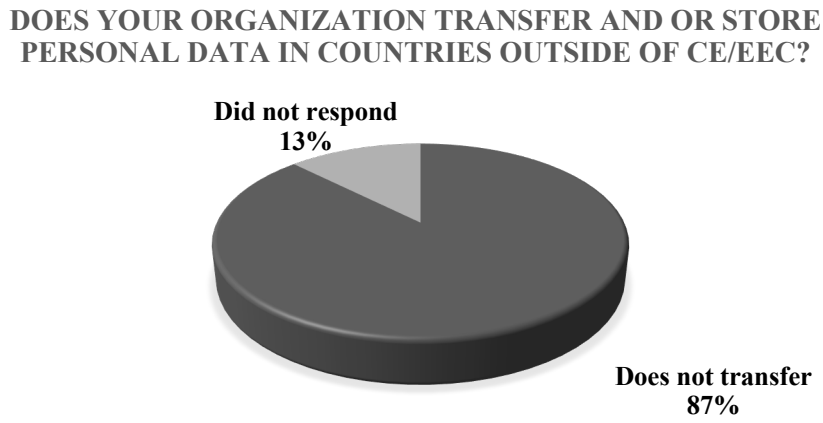

Figure 14 Availability of data transfers to countries outside EU

Figure 14 demonstrates that eighty seven percent of the participants answered that they do not transfer user's personal information to countries outside of the CE/EEC. This may be strongly related to the size of the organization and the respective fields and markets they operate.

Seventy five percent of our participants have answered that they didn't have contracts with third party organizations with the intention of processing personal user's data. Indicating that most privacy data processing that exists was done in house, demonstrated by Figure 15.

Figure 15 Usage of third-party data processing

Figure 16 is about user's rights as described in the GDPR. 62% of the participants replied that they guarantee their user's rights to access, correct and the right to be forgotten in

compliance with the GDPR. On the other hand, only 25% replied that they had and maintain a record of alterations request.

The GDPR has helped sensitize the general public to security motivating professionals to invest in configuration best practices and compelling organizations to do their best to also comply with their users' expectations. The configurations of electronic services have been evolving propelled by consumers opinion and awareness at a reduce pace.

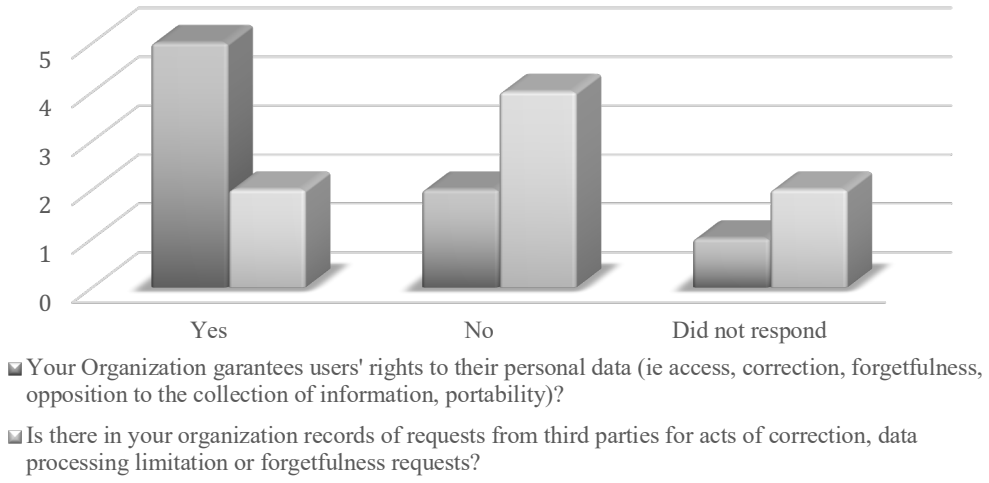

Figure 16 Compliance with user's electronic rights

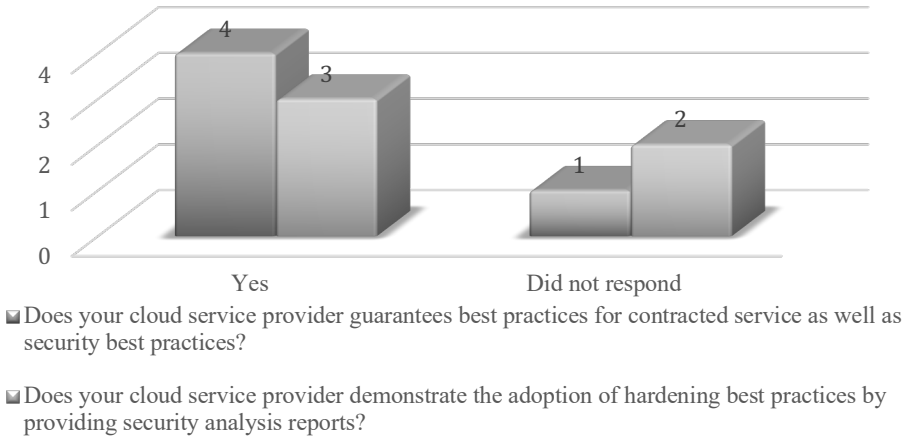

Figure 17 Availability of hosted providers reports

In the expectation of avoiding hefty fines, Organizations have tried to delegate some of these responsibilities to bigger and better prepared organizations like hosted solutions providers, also known as cloud providers. 62% of the participants have replied that they have a hosted solution, demonstrated by Figure 18.

Figure 18 Usage of hosted solution

Even in the case of hosted solutions, organizations are responsible by the service they provide and the safety of private and personal information stored on those systems. Because they have delegated part of the administration to third parties, these third parties should assure their costumers that they also do their best to safeguard data wile guaranteeing compliance with industry best practices, providing evidences through periodic reports. The marketing of cloud solutions is very intense with most marketing propagandas being light of factual information and heavy on trending key words.

Cloud providers, at first glance, have very competitive prices when compared with the creation and maintenance of a dedicated private infrastructure. With time, these offerings have become a compelling viable choice for providing online services.

Of the participants, 80% have answered that their hosting solution provider provides them with guarantees of following industry and security best practices.

60% of the participants have answered that their hosting provider provides them with security analysis and reports that demonstrate the application of industry hardening and security best practices, as demonstrated by Figure 17.

These answers demonstrate a higher concern in assuring their clients they are following industry standards in regard to hardening of information systems. Making the services they provide more reliable and increasing resistance to cyberattacks. This also means that the personal information that these hosted solutions may possess benefit from all these efforts. Although the collection of personal information isn't restricted to electronic information system, the GDPR applies itself beyond those. Of the complexity of hosted services available many organizations, only need a small set of these services, like web hosting. In the next group of questions, we asked our participants if they have a webpage/website however, we did not distinguish between cloud hosted or self-hosted.

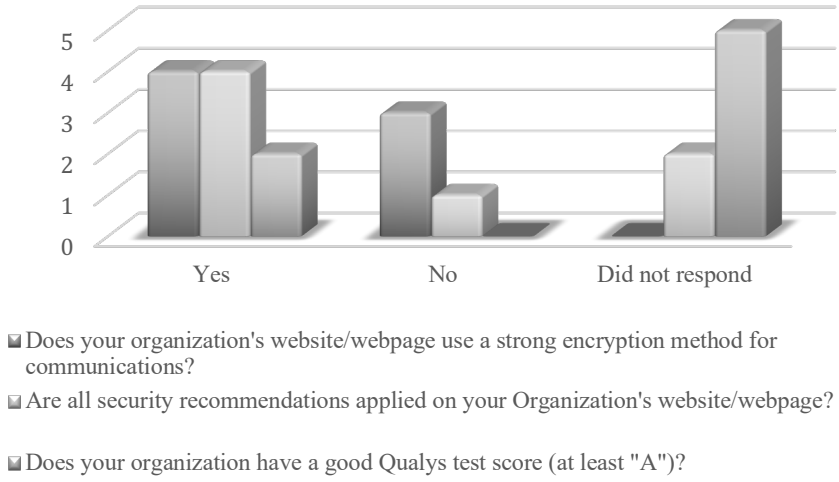

Figure 19 Usage of website or webpage strong encryption

Eighty seven percent of them answered positive. Of those that responded positive to having a web presence, 57% replied that they use strong encryption as their method of communication. 57% also replied that they always applied all security recommendations. To the question about the usage of the assessment tool Qualys and having a score of "A" only 29% responded positively. An expected outcome to this question given the intent was disseminating awareness to these tools. In the next group of questions, we asked about secure communications for roaming and on location as well as communications to the organization's servers, reflected by Figure 19.

Figure 20 Usage of webpage/website

As demonstrated by Figure 20, eighty seven percent of our participants responded that they have a webpage/website.

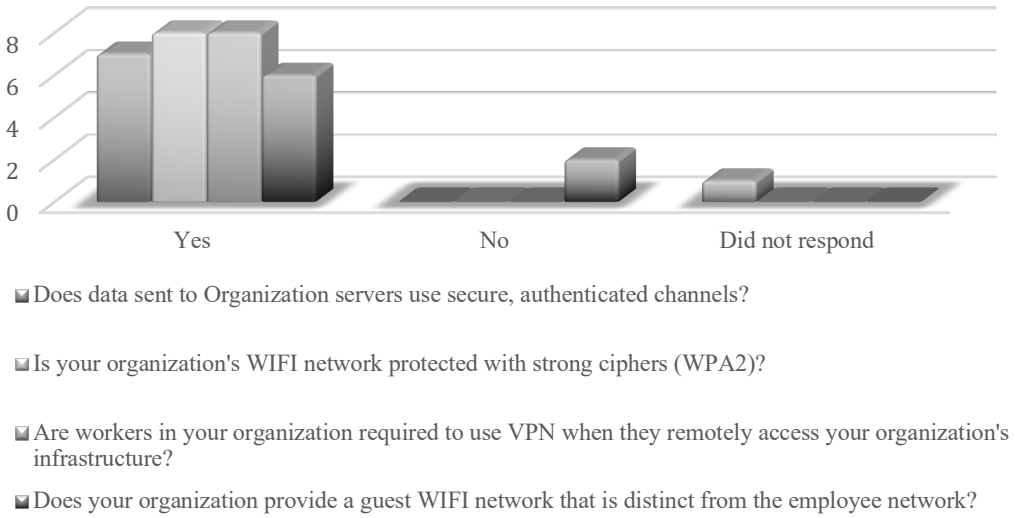

Figure 21 Usage of secure channels

Figure 21 documents that eighty seven percent of the participants responded that they use secure, authenticated channels with their servers. 100% of the participants responded that they use strong ciphers in their WIFI and all their workers are required to use VPN's to remotely connect to the organization's infrastructure. 75% replied that they had and used

segregated WIFI networks for guest usage. In the following group, as documented by Figure 22, we asked about password strength, account lock and role-based access.

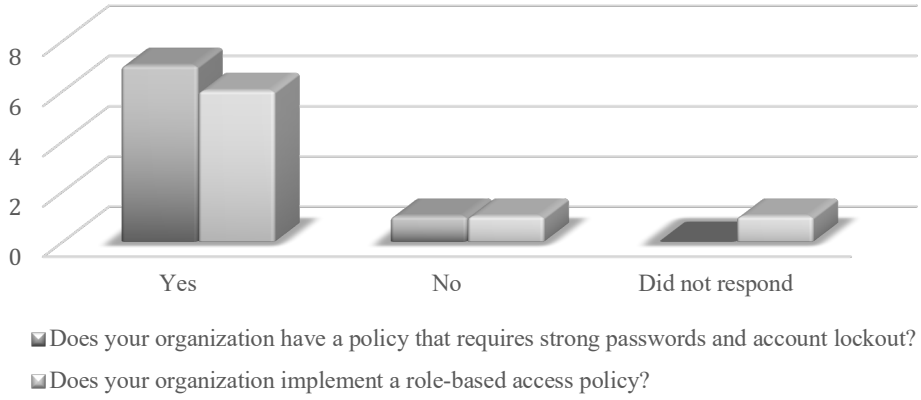

Figure 22 Usage of password policies and role-based access

Eighty seven percent answered that they do have a policy requiring strong passwords and account locking, 75% had an access policy and implemented role-based access. The next group of questions may seem misleading but, like everything software. Firewalls, may have several purposes and the configuration of a firewall can have a general purpose or be carefully configured to achieve a single objective. We asked if their firewall is configured to prevent attacks. 75% has answered “Yes”. 50% of all participants responded that they had a well configured firewall. 25% didn’t know if their firewall was configured correctly and 12% answered that they didn’t have a firewall. To understand this percentage, further studies are needed, documented by Figure 23.

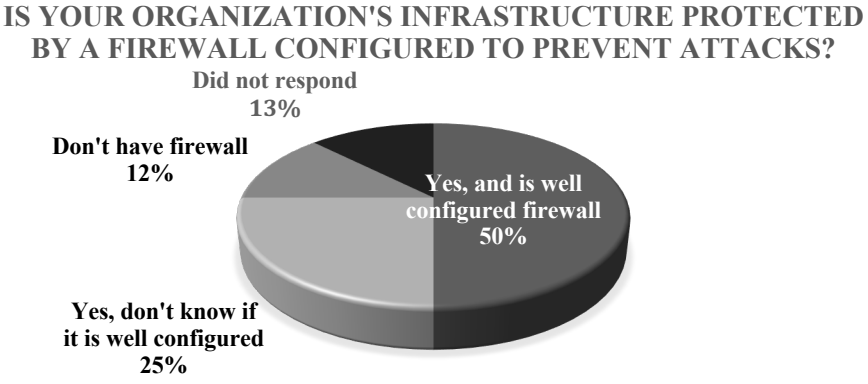

Figure 23 Firewall existence and level of configuration

Directly attacking servers or firewalls may be time consuming and sometimes not feasible since most systems have been tuned to prevent attacks from outside the organization's network. Most attacks have evolved to take advantage of social engineering and try to compromise infrastructures from within. So, an attack vector can be a user's workstation, to compromise that workstation and escalate to the entire infrastructure. We asked the participants if they employed spam filters, anti-malware and antivirus tools in their workstations. Eighty seven percent have responded yes.

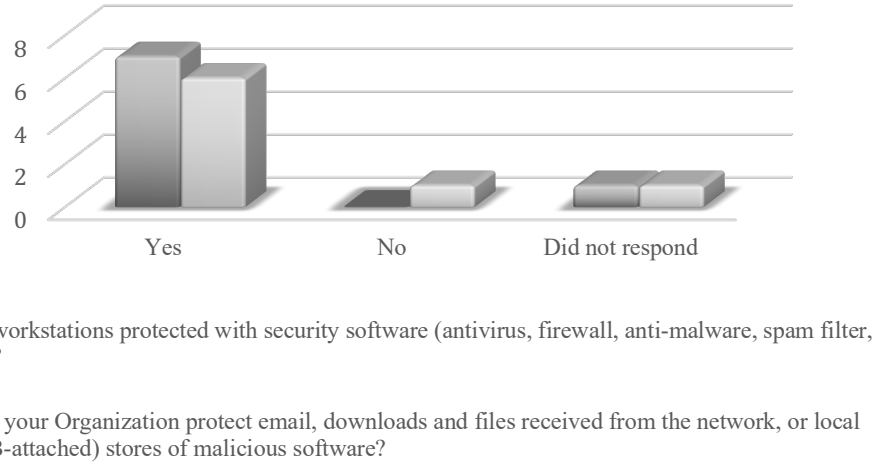

Figure 24 Implementation of secure workstations

Then we asked if their organization protected downloads, e-mails, network transfers and local attached storage (USB, etc). Seventy five percent have answered Yes that they protect. Figure 24 documents these responses.

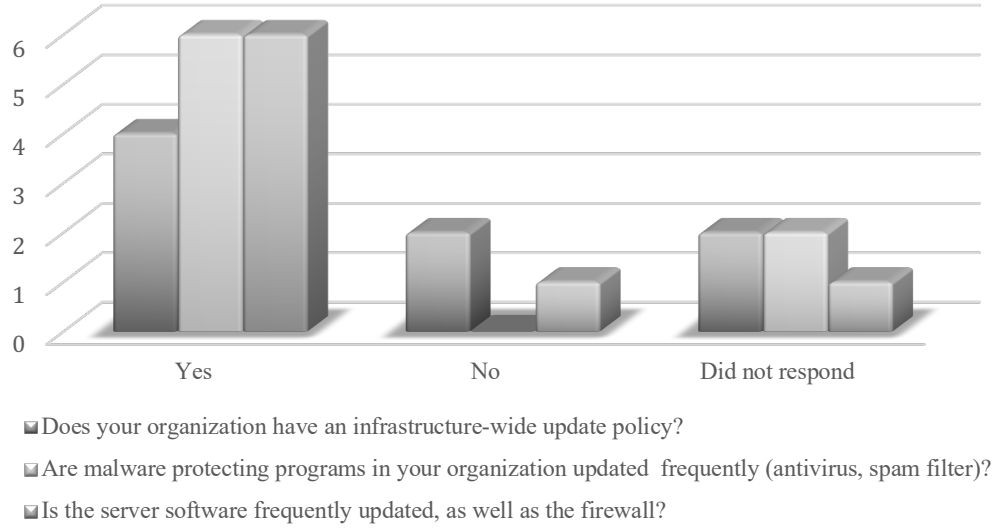

Figure 25 Availability of updates policies

Software updates are very important for several reasons, but one of the most important is safety. However, unplanned updates can be very prejudicial for an organization, in some cases even more severe than some attacks. For this reason, we asked the participants if they had an infrastructure-wide update policy. Fifty percent have answered yes. To the question if they updated programs, safety programs like antivirus, spam filters, etc. Seventy five percent have responded positively.

The same percentage, 75% answered positively, that they updated frequently servers and firewalls, as demonstrated by Figure 25.

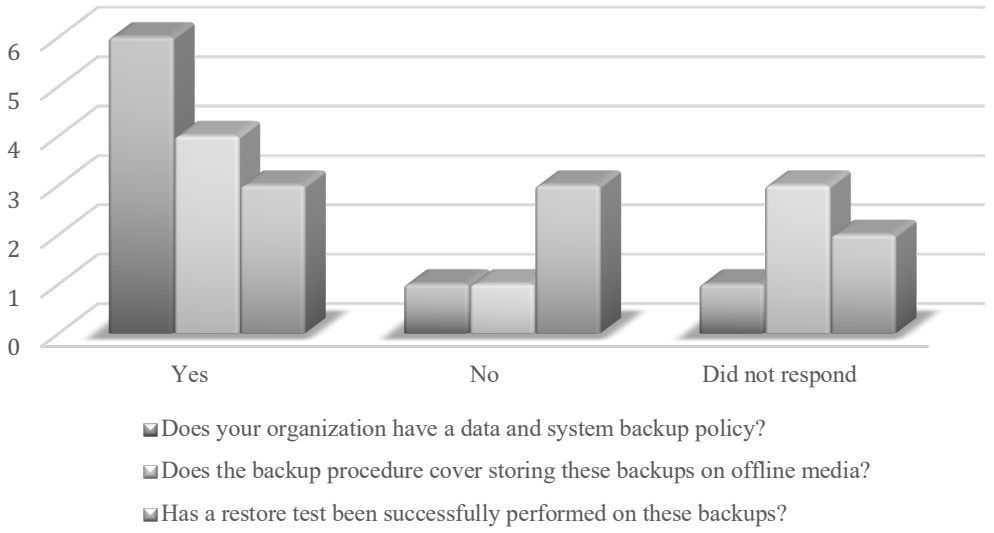

Figure 26 Availability of Backup polices and tests

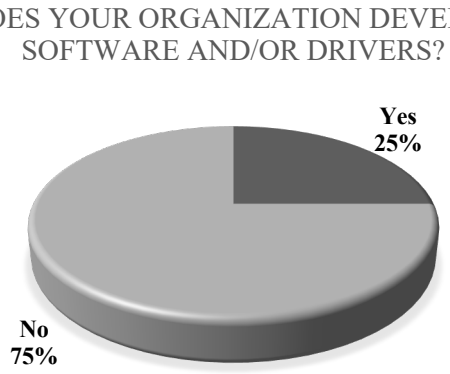

Figure 27 In house software development

Like the updates, backups, are also important for several reasons. Although today great emphasis may be on attacks, the main problem any organization traditionally faces is data loss for the most diverse reasons. An adapted backup policy can mitigate the impacts of data loss or the most recent cyberattacks. Of the participants, 75%, answered positive to having data and systems backup policies; 50% replied that they had offline backups. The percentage of organizations that had tested backup restores and were successful in restoring data was 37,5%. Figure 26 documents this observation.

The following group of questions was directed to a small group of the participants because it was focused on software and/or drivers' development. 25% of the participants answered that they developed software, represented by Figure 27.

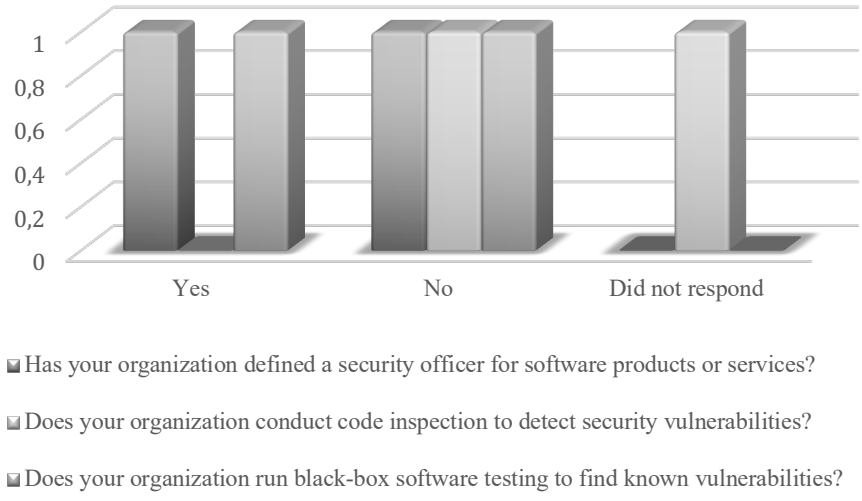

Figure 28 Implementation of security by default

Even though, our current society depends on digital, only a small portion are software developers. That reflects itself on our survey with a niche that responded to this group of questions.

Software development is a complex endeavour so we focused mostly on GDPR related questions like black-box testing. Fifty percent of the eligible participants responded doing black-box testing. Another relevant question was if the organization as a security officer for the products they produce. Once again was a 50/50 answerer to yes and no, as documented in Figure 28.

Figure 29 gives us a view on how would anyone respond/act to a cyber threat/attack? This question is applicable to anyone that uses IT. The attacks that have become public, have ranged from small instabilities to great outages. The questions that we posed were more in the self-awareness field because some attacks can be very devastating to the extent of overpowering even the best prepared teams. We asked if the organization security person(s) were capable of minimizing or preventing an attack to their infrastructure. 87,5% responded positive, that they were capable of this task.

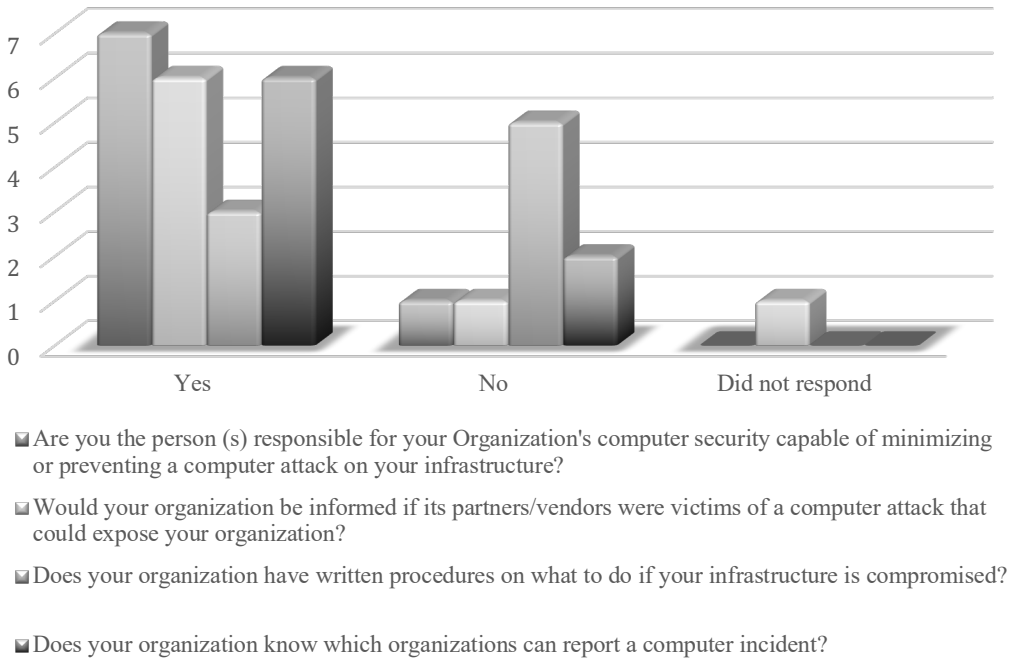

Figure 29 Assertion of threat response

Surrounded by a stigma of ill preparedness, cyberattack information can be damaging to the image of any organization. So, we posed the reverse question not if the organization would publicise or inform of cyber-attacks but, if they would believe that their

partners/vendors would inform them of being victims of a cyberattack. 75% responded that they believe they would be informed. 37,5% responded that they had written procedures for the event of infrastructure compromise. Most persons think that all cyber incidents should be reported to the police. This is not wrong however some organizations may be obligated to report these events to their industry regulator in such small-time frames that they have to first report to the regulator before they can even report to the police authorities. With this in mind we asked if our participants knew to whom they should report cyber incidents. 75% responded they knew to whom they should report cyber incidents.

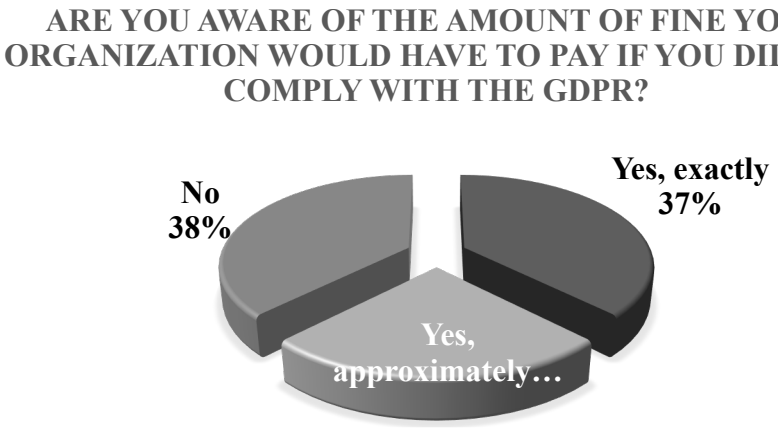

Figure 30 Assertion of fine's awareness

One of the biggest evolutions of the GDPR was the fines, "heavier" than ever before. So, we posed the following question. Since the fines are calculated according to size, severity and other factors. We made the distinction between exact amount and approximately amount of the fine. 62% responded that they were aware of the amounts involved in case of not complying with GDPR. Of those 37% new the exact amount of the applicable fine, as documented in Figure 30.

The Figure 31 displays the score given by the participants to the level of awareness they think the survey raised about cyber, data security and the GDPR.

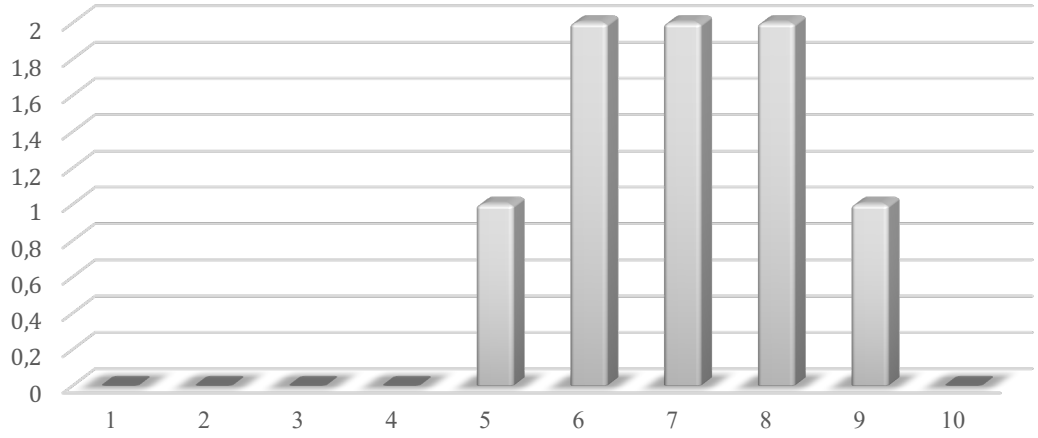

Figure 31 Contribution to cyber and data security awareness

5.1 Our recommendations for SMEs

Our analysis of the responses to some of the questions, prompted us to provide some information that we believe could be useful for some PMEs, mainly regarding firewalls. It's our understanding that simply putting a firewall at the ingress of a given network is a good step but much more can be done. Some consumer firewalls come pre-configured with automations to help the consumer use the Internet without great knowledge. However, this king of automations should always be avoided.

It's our recommendation that dedicated enterprise firewalls should be preferred for SMEs. We list some very good entry enterprise firewalls that have paid versions as well as free or community versions.

- Pfsense[18], this is an easy to install and use firewall that also has a community version.
- Opnsense[19], like the previous this firewall also has a community version and is developed in the Netherlands.
- Ipfilter[20], a firewall base on GNU Linux with a free version developed in Germany.

[18] For more information visit the product official site, PFsense, https://www.pfsense.org/

[19] For more information visit the product official site, OPNsense, https://opnsense.org/

[20] For more information visit the product official site, IPfire, https://www.ipfire.org/

- Untungle[21], also based on GNU Linux, there is a free version with some caveats, some limitations are imposed in the free version so that the user upgrades to the paid version.

If these kinds of firewalls are outside of the SME possibilities at least the following steps should be taken:

- Validate that the management of the firewall is only accessible on the internal network.
- Validate that no automation dynamically opens ingress ports, like UPNP.
- Validate that only the strictly necessary ingress ports are open.
- Validate that the credentials and accounts used in the firewall are different from the factory settings. Some best practices suggest disabling such accounts and new ones should be used.

Some automation can be beneficial in firewalls. All the firewalls here suggested can be automated to prevent some attacks with the installation of plugins, managed inside each firewall. Most common suggested plugin usually is suricata[22] and DNS filtering.

This second one is not available in all firewalls as a plugin or is a paid feature. Some can be configured to also filter DNS with a lot of effort.

As these are plugins their installation, configuration and usage differ from product to product. We consider better to refer to each product manual for more information.

Organizations with a site/web page should consider other piece of software, ModSecurity[23], an application firewall. This software is opensource and is available for Apache, Nginx, haproxy and more. It provides an application-level firewall, allowing the site administrator to filter requests and act accordingly. One possible such act could be preventing an attack with a known string, protecting the services behind it.

---

[21] For more information visit the product official site, Untungle, https://www.untangle.com/

[22] The project page of suricata: https://suricata.io/

[23] ModScurity, previously a commercial solution available at https://www.modsecurity.org, now on end-of-life and end-of-sale. Although packages for major GNU Linux distributions do exist, the community project persists on GitHub, https://github.com/SpiderLabs/ModSecurity with a complete rewrite of the code.

Chapter 6
Conclusion and Future Work

The first question that we proposed to answer was: Can these organizations be helped to focus on the relevant portions of the GDPR?
We believe that all the following are areas were these organizations may benefit with some help.
The attainment of clear consent and the revision of those consents was somewhat low.
In regards to data encryption, is our understanding that some of the organizations should invest in achieving data encryption at the application level, taking grater advantage of their applications.
Few organizations have answered that they had records of acts of correction, data processing and of the right to be forgotten, one of the GDPR key points and punished with fines, is our understanding that further studies must be conducted. These answers may be by the lack of the kind of requests or these requests don't make sense on their line of work.
Infrastructure configuration, mainly firewalls, seamed something that the organizations had some doubts. Although most organizations had one, not all were sure of their correct configuration.
Update policies were also a little low. Not that they didn't do updates, just that they lacked policies to conduct those updates.
On the other hand, backup policies were at acceptable level, though reliability of the data was questionable.
The lack of written procedures for the case of infrastructure compromise. In general, the organizations had demonstrated, essentially lack of procedures, being those written or not.

To the second question: Are any platforms available that can help assess the organizations compliance and guide them?
Unfortunately, no single tool or platform exists. The SMOOTH project was under development with a public pilot ongoing, still to be fully available.

Given the number and the diversity of programs that are operated in any given organization, the only way of guaranteeing GDPR compliance would be to certify each and every program or start to only use GDPR certified programs. To the writhing of this dissertation, such programs were non-inexistent, but it seems to exist legal bases for programs certification (EU GDPR Institute, 2019) and these may appear in the future.

Organizations with GDPR certification will have better chances and will fare better in the European and World markets, taking advantages that the certification will provide. The increase security and privacy awareness of the society will in time also help these organizations fare well economically.

The organizations that replied to our survey were clearly aware of their obligations and that was visible in the answers received. They demonstrated active involvement in complying with the GDPR and the protection of their user's privacy. Although a buzz phrase is "security by default" this is a mentality that must be cultivated and shared. This new mentality will take some time to be implemented and even greater time to see the outcome of this mentality. Not only because humans are averse to some changes but because of "IT legacy". Many organizations are dependent on legacy programs and these must be slowly migrated or ported to secure and compliant versions that will in time better protect privacy, complying fully with the GDPR.

"The tomorrow's present", We've chosen this way because the human being will always regard the future as something distant. Using "the tomorrow's present", at least, in our mind lesser distant future.

The organizations will have to invest in GDPR training and the constant development of their employee's knowledge.

In recent times we've began to notice a shift in mentalities. Many of the organizations have become more acceptant to implementing best practices and prepare systems to easily evolve in compliance and safety. These approaches, will pay back in risk management, industry compliance and security.

It's our belief that with the responses we received, our survey didn't explore all the possibilities to better understand how cloud providers comply with the GDPR and how these providers convey this information to their clients.

References

Freitas, M. d. C. & Silva, M. M. d., 2018. GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management*, 10 November.

European Commission, n.d. *Data protection in the EU.* [Online]
Available at: ttps://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
[Accessed 11 April 2019].

European Union, 2016. Data protection impact assessment. *Official Journal of the European Union,* pp. 53-54.

Custers, B. et al., 2017. *A Comparison of Data Protection Legislation and Policies Across the EU,* s.l.: Computer Law & Security Review.

Kasl, F., 2018. CYBERSECURITY OF SMALL AND MEDIUM ENTERPRISES IN THE ERA OF INTERNET OF THINGS. *The Lawyer Quarterly,* 22 April.

THE COMMISSION OF THE EUROPEAN COMMUNITIES, 2003. Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. *Official Journal L 124*, 20 May.

smooth, n.d. *consortium.* [Online]
Available at: https://smoothplatform.eu/consortium/
[Accessed 26 May 2019].

Presas, M., 2018. *SMOOTH Consortium Helps SMEs Adapting to GDPR.* [Online]
Available at: https://smoothplatform.eu/smooth-consortium-helps-smes-gdpr/
[Accessed 05 06 2019].

MxToolbox, Inc., 2019. *MxToolbox.* [Online]
Available at: https://mxtoolbox.com/
[Accessed 8 Jun 2019].

Center for Internet Security, Inc, 2019. *Home * About us.* [Online]
Available at: https://www.cisecurity.org/about-us/
[Accessed 13 Jun 2019].

isnotspam, n.d. *isnotspam.* [Online]
Available at: http://www.isnotspam.com/
[Accessed 2 Jul 2019].

Europian Comission, 2019. *What is Horizon 2020?.* [Online]
Available at: https://ec.europa.eu/programmes/horizon2020/what-horizon-2020
[Accessed 03 Jul 2019].

merriam-webster Incorporated, 2019. *best practice.* [Online]
Available at: https://www.merriam-webster.com/dictionary/best%20practice
[Accessed 03 Jul 2019].

Cambridge University Press, 2019. *Meaning of encrypt in English.* [Online]
Available at: https://dictionary.cambridge.org/us/dictionary/english/encrypt
[Accessed 08 Jul 2019].

Almulla, S., Iraqi, Y. & Jones, A., 2014. A State-Of-The-Art Review of Cloud Forensics. *Journal of Digital Forensics,Security and Law,* 9(4), p. Article 2.

Microsoft, 2019. *File Encryption.* [Online]
Available at: https://docs.microsoft.com/en-us/windows/win32/fileio/file-encryption
[Accessed 08 jul 2019].

Fruhwirth, C. & Broz, M., 2018. *LUKS1 On-Disk Format Specification,* s.l.: s.n.

National Institute of Standards and Technology, 2019. *National Institute of Standards and Technology.* [Online]
Available at: https://www.nist.gov/
[Accessed 08 Jul 2019].

International Organization for Standardization, 2019. *International Organization for Standardization.* [Online]
Available at: https://www.iso.org/home.html
[Accessed 08 Jul 2019].

ISACA, 2019. *cobit.* [Online]
Available at: http://www.isaca.org/COBIT/Pages/default.aspx
[Accessed 08 Jul 2019].

Bakken, D. E. et al., 2004. Data Obfuscation: Anonymityand Desensitization of Usable Data Sets. *IEEE,* 2(6), p. 35.

Associação DNS.PT, 2019. *Webcheck.pt.* [Online]
Available at: https://webcheck.pt/pt/
[Accessed 09 Jul 2019].

EU GDPR Institute, 2019. *GDPR Certification.* [Online]
Available at: http://www.eugdpr.institute/obtaining-a-eugdpr-institutes-gdpr-certification/
[Accessed 10 Jul 2019].

The European Union Agency for Cybersecurity (ENISA), 2019. *NCSS Good Practice Guide.* [Online]
Available at: https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[Accessed 26 Jul 2019].

Comissão Nacional de Protecção de Dados, n.d. *www.cnpd.pt.* [Online]
Available at: https://www.cnpd.pt/english/index_en.htm
[Accessed 10 Sep 2019].

Verma, A., 2015. *fossbytes.com.* [Online]
Available at: https://fossbytes.com/echelon-project-nsa-confirmed-secret-nsa-spying/
[Accessed 11 Sep 2019].

Cornwall, B. & Doherty, K., 2015. *www.rt.com.* [Online]
Available at: https://www.rt.com/usa/311489-snowden-files-confirm-echelon/
[Accessed 11 Sep 2019].

Greenwald, G., 2012. *www.theguardian.com.* [Online]
Available at: https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden
[Accessed 12 Sep 2019].

NG, A., 2018. *www.cnet.com.* [Online]
Available at: https://www.cnet.com/news/equifaxs-data-breach-by-the-numbers-the-full-breakdown/
[Accessed 12 Sep 2019].

Falliere, N., Murchu, L. O. & Chien, E., February 2011. *W32.Stuxnet Dossier,* s.l.: Symantec.

INE, I.P., 2019. *www.ine.pt.* [Online]
Available at: https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_publicacoes&PUBLICACOESTipo=ea&PUBLICACOEScoleccao=107678&xlang=pt
[Accessed 22 November 2020].

European Union, 2017. *ec.europa.eu.* [Online]
Available at: https://ec.europa.eu/newsroom/article29/items/611237
[Accessed 25 July 2021].

Europiean Union, 2016. *Eur-Lex.* [Online]
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3

A2016%3A119%3ATOC
[Accessed 15 December 2021].

European Union, 1995. *Eur-Lex.* [Online]
Available at: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:31995L0046
[Accessed 15 December 2021].

Appendix A – Survey

Segurança e privacidade de dados em PMEs Portuguesas

Este questionário é parte do projeto de Mestrado em Segurança Informática de João Alvega (fc50730@alunos.fc.ul.pt)
Faculdade de Ciências da Universidade de Lisboa

(Nota: algumas das perguntas presentes neste questionário foram adaptadas de outros trabalhos académicos e soluções empresariais)

Obrigado por participar no nosso questionário dedicado a Pequenas, Medias e Microempresas.

Este questionário destina-se a compreender o estado atual da segurança e privacidade de dados em PMEs Portuguesas.

Dimensão

*A sua Organização é uma:

- Microempresa - até 10 trabalhadores e volume de negócios não excede 2 milhões de euros ou balanco total não excede 2 milhões de euros;
- Pequena Empresa - até 50 trabalhadores e volume de negócios não excede 10 milhões de euros ou balanco total não excede 10 milhões de euros;
- Média Empresa - até 250 trabalhadores e volume de negócios não excede 50 milhões de euros ou balanco total não excede 43 milhões de euros;
- Nenhuma das anteriores.

Se a sua Organização é superior a 250 trabalhadores, este questionário não é para si.
Obrigado, pelo seu interesse.

Escolha da seguinte lista a área na qual desenvolve a sua atividade:

* Escolha uma das seguintes respostas

- ⇒ Agências de viagem
- ⇒ Agroalimentar e Bebidas
- ⇒ Animais
- ⇒ Apoio ao domicílio
- ⇒ Automóveis e Componentes
- ⇒ Banca
- ⇒ Comércio alimentar
- ⇒ Condomínios
- ⇒ Construção e Remodelação
- ⇒ Consultoria e serviços financeiros
- ⇒ Cosmética e perfumaria

- ⇒ Couro e Calçado
- ⇒ Crianças
- ⇒ Desporto
- ⇒ Ensino e Formação
- ⇒ Equipamentos Elétricos
- ⇒ Estética e bem-estar
- ⇒ Eventos
- ⇒ Exportação e ou Importação
- ⇒ Higiene e Limpeza
- ⇒ Hotelaria
- ⇒ Imobiliária
- ⇒ Intermediação de Crédito
- ⇒ Joelharia e Ourivesaria
- ⇒ Lavandarias e Engomadarias
- ⇒ Livrarias e papelarias
- ⇒ Madeira e Cortiça
- ⇒ Mediação de Seguros
- ⇒ Minerais não metálicos
- ⇒ Mobiliário e Decoração
- ⇒ Moda
- ⇒ Outro comércio especializado
- ⇒ Outros serviços para empresas
- ⇒ Outros serviços para particulares
- ⇒ Pescas
- ⇒ Produtos Metálicos
- ⇒ Química Borracha e Plástico
- ⇒ Restauração
- ⇒ Saúde
- ⇒ Serviços Informáticos e Tecnológicos
- ⇒ Serviços Jurídicos
- ⇒ Turismo
- ⇒ Padarias e lojas alimentares
- ⇒ Oficinas auto

Tarefas, responsabilidades

Na sua Organização existe um especialista responsável por

	Sim, é minha responsabilidade	Sim, mas não sou eu	Não	Sem resposta
Segurança Informática	○	○	○	○
Proteção de Dados	○	○	○	○
Gestão de Risco	○	○	○	○

Na sua Organização foi feito algum estudo sobre

	Sim	Não	Não, mas gostaríamos de o fazer	Sem resposta
Como reagir a um ataque informático?	○	○	○	○
Conformidade com o regulamento de proteção de dados?	○	○	○	○

Consciência

Os empregados da sua Organização sabem como lidar corretamente com informação insegura?

- ○ Sim
- ○ Não
- ○ Sem resposta

A sua Organização providencia canais seguros com os quais os clientes podem interagir?

- ○ Sim
- ○ Não
- ○ Não tem canal dedicado
- ○ Sem resposta

Não (não tem nenhum canal de comunicação)
Não tenho canal dedicado (tem um canal de comunicação, mas este não é considerado seguro e ou dedicado, ex. e-mail)

Na sua Organização, trabalhadores sabem trabalhar em segurança, minimizando os possíveis riscos de segurança informática?

- ○ Sim
- ○ Não
- ○ Sem resposta

Utilizar comunicações cifradas.
Utilizar caução na abertura de links e ficheiros.

As pessoas que têm acesso a informação privada sabem as suas obrigações, bem como as obrigações da Organização?

○ Sim	○ Não	○ Sem resposta

Proteção dos dados (Armazenamento)

A informação sensível e critica é armazenada cifrada?

○ Sim	○ Não	○ Sem resposta

A sua Organização obriga a que os equipamentos sejam cifrados por forma a evitar a recuperação de dados em caso de roubo ou extravio?

○ Sim	○ Não	○ Sem resposta

O acesso físico à infraestrutura informática (servidores e rede) da sua Organização é limitada aos responsáveis por esta?

○ Sim	○ Não	○ Sem resposta

Proteção dos dados (Recolha de dados)

A sua Organização possui as ferramentas necessárias para garantir a segurança da informação pessoal recolhida?

○ Sim	○ Não	○ Sem resposta

A sua Organização recolhe apenas a informação pessoal estritamente necessária?

○ Sim	○ Não	○ Sem resposta

A sua Organização possui consentimento na forma clara e em escrito para a informação pessoal recolhida?

○ Sim	○ Não	○ Sem resposta

A sua Organização procedeu a uma análise da forma e em que circunstância foi obtido o consentimento para a recolha da informação pessoal?

○ Sim	○ Não	○ Sem resposta

Na sua Organização os dados pessoais são cifrados ao nível dos programas/aplicações?

○ Sim	○ Não	○ Sem resposta

Proteção dos dados (Interna)

Na sua Organização existe documentação para os seus empregados das regras de uso dos meios de comunicação da Organização?

- ○ Sim
- ○ Não
- ○ Sem resposta

A sua Organização possui uma lista atualizada de câmaras de vigilância das suas instalações?

- ○ Sim
- ○ Não
- ○ Não possui câmaras de videovigilância nas instalações
- ○ Sem resposta

A sua Organização possui uma lista atualizada dos números de telefone nos quais são realizadas gravações?

- ○ Sim
- ○ Não
- ○ Sem resposta

A sua Organização possui alguma monitorização do uso de telefones/correio-electrónico/Internet?

- ○ Sim
- ○ Não
- ○ Sem resposta

Proteção dos dados (Direitos)

A sua Organização garante os direitos dos utilizadores sobre os seus dados pessoais (isto é, de acesso, correção, esquecimento, oposição à recolha da informação, portabilidade de dados)?

- ○ Sim
- ○ Não
- ○ Sem resposta

Existe na sua Organização registo de pedidos de terceiros dos atos de correção, limitação ao processamento de dados ou pedidos de esquecimento?

- ○ Sim
- ○ Não
- ○ Sem resposta

Se a sua Organização tem contratos com terceiros para processamento de dados pessoais, estes contratos cumprem o regulamento de proteção desses dados?

- ○ Sim
- ○ Não
- ○ Não temos contratos com terceiros para o processamento de dados pessoais
- ○ Sem resposta

A sua Organização transfere e ou armazena informação pessoal em países fora da CE/EEC?

- ○ Sim e verificou a sua conformidade perante o RGPD
- ○ Sim, mas não verificou a sua conformidade perante o RGPD

- Não transfere
- Sem resposta

Soluções Hospedadas

*A sua Organização tem alguma solução hospedada (um ou mais servidores na Cloud)?

- Sim
- Não

Caso responda não, pode ignorar as restantes questões deste grupo.

O seu provedor de serviços Cloud garante as melhores praticas para o serviço contratado bem como as melhores praticas de segurança?

- Sim
- Não
- Sem resposta

Nos seguintes links são apresentados um conjunto de boas praticas para sistemas informáticos:
https://www.enisa.europa.eu/
https://www.cisecurity.org/

O seu provedor de serviços Cloud demonstra a adoção das melhores práticas de "hardening", providenciando relatórios de análise de segurança?

- Sim
- Não
- Sem resposta

Nos seguintes links são apresentados um conjunto de boas praticas para sistemas informáticos:
https://www.enisa.europa.eu/
https://www.cisecurity.org/

Páginas web

*A sua Organização tem algum site/webpage?

- ○ Sim
- ○ Não

Caso responda não, pode ignorar as restantes questões deste grupo.

O site/webpage da sua Organização usa um método de cifra forte para as comunicações?

- ○ Sim
- ○ Não
- ○ Sem resposta

São aplicadas todas as recomendações de segurança no site/webpage da sua Organização?

- ○ Sim
- ○ Não
- ○ Sem resposta

A sua Organização possui uma boa pontuação nos testes Qualys (pelo menos "A")?

- ○ Sim
- ○ Não
- ○ Sem resposta

Qualys é um serviço de avaliação das configurações associadas com o protocolo https que está disponível em: https://www.ssllabs.com/ssltest/

Comunicações Seguras

Os dados enviados para os servidores da Organização usam canais seguros e autenticados?

○ Sim	○ Não	○ Sem resposta

A rede WIFI da sua Organização é protegida com cifras fortes (WPA2)?

○ Sim	○ Não	○ Sem resposta

São os trabalhadores da sua Organização obrigados a usar VPN quando estes acedem remotamente à infraestrutura da Organização?

○ Sim	○ Não	○ Sem resposta

A sua Organização proporciona uma rede WIFI para convidados distinta da rede dos colaboradores?

○ Sim	○ Não	○ Sem resposta

Administração de Utilizadores e Passwords

A sua Organização tem uma política que obrigue a utilização de passwords fortes e bloqueio de contas?

- ○ Sim
- ○ Não
- ○ Sem resposta

Passwords fortes são palavras passe que incluem letras maiúsculas, minúsculas, dígitos e carateres de pontuação. Bloqueio de contas no caso de utilizadores que abandonem a organização ou estejam ausentes por períodos prolongados.

A sua Organização implementa uma política de acessos baseados nas funções?

- ○ Sim
- ○ Não
- ○ Sem resposta

Proteção de Malware

A infraestrutura da sua Organização está protegida por uma firewall configurada para prevenir ataques?

- ○ Sim, tem uma firewall bem configurada
- ○ Sim, mas não sei se bem configurada
- ○ Não tem firewall
- ○ Sem resposta

As estações de trabalho estão protegidas com software de segurança (antivírus, firewall, anti-malware, filtro de spam, etc.)?

- ○ Sim
- ○ Não
- ○ Sem resposta

A sua Organização protege o correio eletrónico, downloads e ficheiros recebidos da rede ou armazenamentos locais (ligados por USB) de software malicioso?

- ○ Sim
- ○ Não
- ○ Sem resposta

Atualizações

A sua Organização possui uma política de updates para toda a infraestrutura?

- ○ Sim
- ○ Não
- ○ Sem resposta

Na sua Organização os programas de proteção contra malware são atualizados com frequência (antivírus, filtro de spam)?

- ○ Sim
- ○ Não
- ○ Sem resposta

O software dos servidores é atualizado com frequência, bem como a firewall?

- ○ Sim
- ○ Não
- ○ Sem resposta

Backups

A sua Organização possui uma política de backup dos dados e dos sistemas?

○ Sim	○ Não	○ Sem resposta

O procedimento de backup abrange o armazenamento desses backups em meios desligados dos sistemas (off-line)?

○ Sim	○ Não	○ Sem resposta

Alguma vez foi feito um teste de restauro desses backups com sucesso?

○ Sim	○ Não	○ Sem resposta

Desenvolvimento de Software e Drivers

*A sua Organização desenvolve software e ou drivers?

○ Sim	○ Não

Caso responda não, pode ignorar as restantes questões deste grupo.

A sua Organização definiu um responsável de segurança para os produtos de software ou serviços?

○ Sim	○ Não	○ Sem resposta

Na sua Organização realiza-se a inspeção de código para detetar vulnerabilidades de segurança?

○ Sim	○ Não	○ Sem resposta

A sua Organização faz testes de software do tipo black-box para tentar encontrar vulnerabilidades conhecidas?

○ Sim	○ Não	○ Sem resposta

Resposta a incidentes

É(são) a(s) pessoa(s) responsável(eis) pela segurança informática da sua Organização capaz(es) de minimizar ou impedir um ataque informático à sua infraestrutura?

○ Sim	○ Não	○ Sem resposta

Seria a sua Organização informada se os seus parceiros/vendedores fossem vítimas de um ataque informático que pudesse expor a sua Organização?

○ Sim	○ Não	○ Sem resposta

A sua Organização possui procedimentos escritos de como proceder em caso de comprometimento da sua infraestrutura?

○ Sim	○ Não	○ Sem resposta

A sua Organização sabe a que organismos pode comunicar um incidente informático?

○ Sim	○ Não	○ Sem resposta

Penalizações

Tem conhecimento do valor da multa que a sua Organização teria de pagar, caso não estivesse em conformidade com o RGPD?

- Sim, exatamente
- Sim, aproximadamente
- Não
- Sem resposta

Avaliação

*Avalie como este questionário contribui para melhorar a sensibilização para a segurança, privacidade e proteção de dados.

Por favor considere o seguinte significado:

1 contribuiu muito pouco até 10 contribuiu bastante

	1	2	3	4	5	6	7	8	9	10

Appendix B – Raw survey participation