EAI Endorsed Transactions
on Security and Safety

Research Article EAI.EU

Mapping of the Security Requirements of GDPR and NISD

Najmudin Saqib, Vasileios Germanos, Wen Zeng, Leandros Maglaras*

School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK

Abstract

Privacy and information security have consistently been a priority for the European Union lawmaker. This paper investigates the security requirements of the General Data Protection Regulation (GDPR) and the Directive on security of network and information systems (NISD). This investigation incorporates what is unique about the NISD; how it overlaps with existing frameworks; and how security requirements in the GDPR influence the NISD. This mapping of requirements can help businesses and organizations to distinguish possible difficulties that may experience while conforming to GDPR and NISD, and help them create a consistent cybersecurity framework and structure new security plans.

Received on 06 July 2020; accepted on 31 August 2020; published on 03 September 2020

Keywords: GDPR, NISD, cybersecurity

doi:10.4108/eai.30-6-2020.166283

1. Introduction

The 27 member states of the European Union (EU) have their own regulations up to 2016 covering the assortment, compilation and planning on about their citizens' personal data in relation to the Data Protection Directive (DPD) - Directive 95/46/EC [1]. On 27 April 2016, the EU Commission received an additional General Data Protection Regulation (GDPR) [2] that would have a full impact on 25 May 2018 and replaced Directive 95/46/EC. GDPR is a framework consisting of a set of rules that defines how people can access their data and adds limits on how organisations can use personal data. EU countries were given the ability to amend slightly the regulation to suit their own needs. For example, the UK created the Data Protection Act (2018) that replaced the previous Data Protection Act (1998).

In 2016, the NISD [3] has been adopted. It aims at enhancing the EU's cyber-resilience and addressing the threats posed to network and information systems, as those that process digital data for use, protection, and operation purposes. These systems may become a target to adversary actions and their reliability and security are vital for economic and societal activities. NISD is not explicitly a cybersecurity law but it aims at improving cybersecurity. It applies to two types of organisations, the operators of essential services (OES) and relevant digital service providers (DSPs).

It should be noted that GDPR and NISD are focusing on different aspects. GDPR is related to process personal data, whereas NISD to security of systems and the digital data within them. Moreover, NISD is a broader regulation than GDPR as includes digital data that are not only personal one. However, they both overlap due to security and data protection are related with each other. In general, although these regulations aim at protecting organisations against cyberattacks, in practice, it is quite often difficult to be adopted by an organisation. That is because some of their requirements overlap. For example, a NISD incident may be a personal data breach as defined by the GDPR. This makes difficult the decision to whom an organisation has to report the incident (i.e, to organisation's competent authority - under NISD and/or the information commissioner's office (ICO) - under GDPR).

To address this kind of issues, in the literature many models/frameworks have been proposed that integrate several regulations. These models can help organisations to adopt properly these regulations and help them to identify current security problems and

*Corresponding author. Email: leandros.maglaras@dmu.ac.uk

structure new security plans. In [4], members of the Cyber Technology Center of De Montfort University proposed a Holistic Cybersecurity Maturity Assessment Framework, which incorporates all security and privacy regulations, and best practices that Higher Education Institutes must be compliant to. Furthermore, this framework can be used as a self assessment or a cybersecurity audit tool. In this work, synergies, overlaps and difficulties that arise from security and data protection requirements were analyzed and mapped into an maturity model. During this work the technical security measures that must be imposed to an organization due to GDPR and NISD (and NIST) best practises were identified and merged. The current article that is conducted from members of the same institute in DMU, complements the aforementioned work since it focuses mostly on organizational, policy making and practical issues rather than technical ones.

In [5], the common requirements between the ISO/IEC 27001:2013 and GDPR are identified and those requirements of GDPR are not addressed by ISO/IEC 27001:2013. This work can be used by ISO/IEC 27001 compliant organisations to extend the already existing security control policies towards data protection, and as a guidance to comply with GDPR. In [6], the National Institute of Standards and Technology (NIST) introduced the Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. This framework improves privacy engineering practices by supporting privacy by design and assist organisations protect individuals' privacy. In [7], a framework is presented that can be used by organisations that handle personal data. The amount and the type of these data is constantly increasing. Also, the number of cases where is necessary for an organisation to cooperate with another one to process these data is increasing. Thus, there is a need to protect the privacy of these data. The presented framework is structured by mapping the requirements of the privacy framework and principles defined in ISO/IEC 29100; the ISO/IEC 27018; the ISO/IEC 29151; and GDPR. This framework can be used by personal data controllers and processors.

In this paper, we conduct a mapping of GDPR and NISD that investigates which sections of these regulations are most taken into account by organisations while implementing these acts; what are the principles and intentions for forming these regulations; and how NISD and GDPR impact the security requirements. This mapping can help chief information security officers (CISOs) and DPOs on understanding their roles and create a consistent cybersecurity framework inside the organisations. This can help them analyze the benefit of implementing information security technologies [8, 9].

The contributions of this article are:

- We present a review of the existing regulations
- We conduct an interaction analysis between these two European initiatives
- We introduce a mapping of GDPR and NISD requirements
- We present in a tabular form the differences among them

This paper is organized as follows. Section 2 provides a review of the existing regulations. Section 3 provides a literature review of NISD. Section 4 focuses on GDPR. Section 5 focuses on the interaction between the GDPR and NISD, and how NISD overlaps with GDPR. Section 6 concludes the paper.

2. Related work

The historic background of guidance mandates and information assurance in the EU dated back to the early 70's after rapid progress on data innovation and an extended debate on security. This follows the expanded handling of individual information on personal computers, when the Hesse province of Germany established the main national data assurance legislation on the plan. The Data Protection Treaty of the Council of Europe came into effect back in 1985 comprising the world's main constitutionally defined requirements for information security [10]. The DPD 95/46/EC was discharged in 1995 to coordinate part-sets on how EU staff are to be secured with regard to individual information preparation and the free development, among EU part-states, of such information [1]. In 2009, the EU Commission promoted a survey of DPD 95/46/EC and identified a number of views which could be strengthened, for example by developing a reasonable EU Internal Market for international organizations, to stick with the various legislation in various EU parts rather than to express them [11].

In January 2012 (European Commission, 2012), the main proposal for the new guideline was released. In different occurrences, the EU and its part states, the proposal was discussed and altered [12]. Finally, in April 2016, it became a guideline and came to power on 4 May 2016, when the Council of the EU and the European Parliament adopted this proposal (European Union, 2016), that it applies for all part states [13].

The primary changes acquainted with the new regulation (GDPR) is that a privilege to be overlooked has been presented (article 17 of the GDPR) [14] and people will have simpler access to their information and the privilege to see how their information is being prepared (article 15 of the GDPR) [15]. People will likewise reserve a privilege to move their information between specialist co-ops (article 20 of the GDPR)

[16] and to know when an information controller or information processor has lost information because of an interruption or hack (article 34 of the GDPR) [17]. There are additionally arrangements in the GDPR that expresses that information security is to be a piece of items and administrations from the most punctual phases of improvement to security settings per default, which are a set of levels that guarantees and organizes information assurance (article 25 of the GDPR) [18].

Recently several works try to focus on NISD [19, 20] or GDPR [21]. Some early works also present both the two security initiatives of the EU but focusing only on the legal perspective [22] or the implications on processing of personal data [23]. According to our knowledge, this is the first article that presents an in depth analysis of both legal documents and presents the interactions among them as well as the overlaps and differences that they have, from a practical perspective.

2.1. Commission Directive 95/45/EC

Because of GDPR, the Commission Directive (CD) 95/45/EC should be revised in order to find out the institutional reasons for cancelling it and adopting the GDPR. In particular, the articles related to the protection of information security and identity insurance policies are included in CD 95/45/EC of the European Parliament and Council of 24 October 1995, concerning the welfare of citizens in relation to the planning, and the free development of personal information [24]. This was made as an optional act which included the limited terms of only around three years with an execution date. The CD received in the mid-1990s to manage ongoing relationship-building in the advanced world. It was the main report at European level to ever deal with insurance enquiries about the protection of personal data in the field of the assortment, preparation, storage and transmission.

It is important to determine the consequences for personal and enterprise information management before attempting to modify the CD's particular structures, strengths and limitations. The CD was composed when information preparing included techniques that appeared to be inventive during the 1990s - documenting frameworks and PC centralized computers. Maintaining a strategic distance from the dangers identified with such arrangements was generally simple by making commitments for processors and connecting various methods to the specific activities. Its principle design was to blend the current guidelines of the various nations (Member States) to ensure the privilege of enlightening information of the subject and to evacuate the snags with the expectation of complimentary development of individual information on the European market. In any case, consideration must be put on the way that it was not among the destinations of the Commission Directive to make a lawful structure which could address future information preparing and security challenges [25].

The information protection standards established by the 1995 Directive (as a general application) [24] are as follows: Reasonable and legal handling of individual information; assortment for clear, explicit and accurate purposes; adequacy, importance and proportionality for reasons of assortment and handling; and give only what is essential in order to collect or manage your own details.

For the most part, the CD governs the processing and storage of specific records (counting a detailed description of special cases to be handled). The framework of Directive 46/95/EC covers a wide range of transparent and private knowledge organizations, imposes substantive restrictions on information processing by such objects, provides increasing privileges for information topics and requires public notifications and supports for certain activities [26].

Regarding the Directive 95/45 in the main section and the distinctive valid setting, it makes it clear that it is not so adequate to handle the ever evolving universe of the collection, movement, correction and reuse of information. However, it certainly indicates the beginning of the feasible road map for defense and knowledge safety. In [27], it is stated that CD 95/45 molds various types of laws, even outside the EU. Moreover, it introduces a convincing concrete European pattern of knowledge security.

2.2. ENISA

The European Networks and Information Systems Agency (ENISA) [28] has a common vision of maintaining a high standard of networks and Information System Security (ISS). It is the EU Agency for network and ISS and is a designated network and information systems professional hub for Member States, the private sector and the people of the EU.

In its initial establishment on 10/3/2004 in accordance with Regulation (EC) No 460/2004 [29], ENISA was created by the European Parliament and Council as an information exchange point between stakeholders which strengthened cooperation in parallel. In the meantime, its authority has been extended many times throughout terms of length and renewed once with the current changes in addition to Regulation (EU) No 526/2013 [30], which includes applicable requirements of ENISA, (Regulation (EC) No 1007/2008 on 24/09/2008 and Regulation 580/161) on setting up of the European Network and Information Systems.

The ENISA response mechanism is mainly aimed at preventing and, in situations where these occur, reacting to cyber attacks from a network and in-training networks, and at last handling them effectively

Table 1. ENISA Strategy 2016-2020

Expertise	Anticipate and support Europe in facing emerging network and information security challenges, by collating, analysing and making available information and expertise on key NISD issues potentially impacting the EU taking into account the evolutions of the digital environment.;
Policy	Promote network and information security as an EU policy priority, by assisting the EU institutions and Member States in developing and implementing EU policies and law related to NIS;
Capacity	Support Europe maintaining state-ofthe-art network and information security capacities, by assisting the Member States and EU bodies in reinforcing their NISD capacities;
Community	Foster the emerging European network and information security community, by reinforcing cooperation at EU level among Member States, EU bodies and relevant NISD stakeholders, including the private sector;
Enabling	Reinforce ENISA's impact, by improving the management of its resources and engaging more efficiently with its stakeholders, including Member States and EU Institutions, as well as at international level.

and without interruption. Five areas of activity are identified in accordance with its strategy [28] as show in Table 1.

3. Network and Information Systems Directive (NISD)

The NISD offers the theoretical framework for necessary measures to be put in place by local stakeholders [3], considering the fact that integration at corporate and legislative level would be jeopardized by its right transposition into national laws. The European Commission has also introduced a Communication on 13.09.2017 to support Member States in the consistent application of the NISD throughout the EU [3]. The NISD offers essential criteria on establishing operators essential services (OES) and describing Digital Service Providers (DSP) and emerging technology service goods and terminology for maintaining a mutual understanding between Member States and EU stakeholders, for the purposes of developing a cohesive Europe-wide strategy.

3.1. Overview

In order to protect essential services and infrastructure by improving the safety of their networks and knowledge systems, the NISD establishes legal provisions. On 6 July 2016, the European Parliament implemented the NISD. The Directive is to be transposed into national legislation by EU Member States by 9 of May 2018. The UK introduced the Network and Information Systems Legislation 2018 (NIS Regulations) [31], which is applicable from 10 of May 2018. Moreover, in the NISD is incorporated the National Cyber Security Policy 2016-2021 [32], which provides an effective regulatory framework to protect the vital national infrastructure in the UK.

In accordance with the NISD, legal measures are taken to increase the general level of network and safety within the EU by the following [33]:

- Ensure that Member States provide an on-site national network and knowledge systems security framework, comprising the National Cybersecurity strategy, a Computer Security Incident Response Team (CSIRT), a Single Point of Contact (SPOC), and the National NIS competent authority (or authorities);

- Member States will also engage in the CSIRT Network for the aim of promoting rapid and productive technical collaboration on common protection events in networks and awareness structures as well as exchanging vital information;

- The network and communication management protection platform is widely used across industries that are critical to our industry and to our community and rely heavily on information networks such as electricity, transport, water, telecommunications, and digital infrastructure. Businesses in the areas defined as OESs by Member States will need effective and proportionate security measures to handle their network and information infrastructure threats. Core business suppliers may also be required to notify the relevant authority of accidents. The main DSPs — search engines, cloud computing and online marketplaces — also have to meet the requirements set out in the Directive for health and educational incidents.

The EU referendum took place on 23 June 2016 and the citizens of the UK subsequently decided to leave the EU. The UK would remain a full member of the ECU Union until the conclusion of exit negotiations and the rights and obligations of EU membership remain all in effect. In this period, the government would continue to agree, introduce and execute EU laws. After the UK has left the EU, the results of the talks on a long-term

relationship between the UK and the EU would decide the agreements in regard to EU legislation. It is the intention of the UK Government that the NISD will still apply in the United Kingdom upon leaving the European Union [34]. Between August and September 2017, the UK held a public consultation on its NISD proposals [35]. This consultation covered six key topics:

1. The way essential services are identified;
2. A national implementation management framework;
3. Safety requirements of essential services operators;
4. Incidents reporting requirements for essential services operators;
5. The requirements on digital service providers; and
6. A penalty regime proposed.

3.2. Oversight and enforcement

The NISD regulations shall be supervised and implemented by a specified competent authority and shall be held responsible for the application of the NISD national structure in support of its State policy. Although the responsible authorities are governed by the NISD regulations in their industry, they have an accountability role in enforcing regulations across the UK by the the Department for Digital, Community, Media and Sport (DCMS). The UK Government has decided that, with each competent authority having a detailed understanding of each sector and its related challenges, a multiple competent authority approach is needed to ensure the most relevant approach for the UK. Therefore, for each industry or area protected by the NISD regulation, responsible authorities have been appointed.

In respect of all regulatory decisions relating to NISD regulations, the competent authorities shall have the sole authority and responsibility. The National Cyber Security Center (NCSC) will support the competent authorities who shall give the competent authorities technical advice and, as a result, fulfill the SPOC's and, consequently, the CSIRT duties, other than the health sector during which NHS Digital handles cyber incidents. In the list below, the responsibilities of competent authorities are presented:

- Analysis of the NISD regulation's equipment in their area and region;
- Preparation and publishing of guidance to assist OESs or DSP in fulfilling the necessity of the NISD regulations;
- Establishment of the distinguishing criteria of their sector / region for the OESs;
- Keeping an inventory of all approved OESs, including a sign of the value of each operator;
- Evaluate compliance with requirements of the Directive for NISD operators;
- Determine the thresholds for reportable incidence in their fields or regions;
- Cooperate with other competent agencies to provide consistent advice and surveillance to OES or DSPs;
- Receive incident reports;
- Ensure that non-cyber accident protocols are performed on-site and provide guidelines to businesses concerned with non-cyber incidents;
- Evaluate incidents; and
- Implement the provisions of the NISD legislation including notifications and prohibitions.

3.3. Monitoring the appliance of the NISD regulations

The OES or DSPs which meet, or are appointed by the reserve power, the assignment thresholds of this sector are required to comply with the requirements of the NISD regulations [31]. A structured approach to engagement with designated operators would be required for effective monitoring. Competent authorities will consider developing a compliance mechanism to track the implementation of the regulations. A determination to exchange with the operators in their sector or area shall be made, and the character of this mechanism shall be the competent authority concerned.

Such a process must be proactive for competent authorities regulating OES. It indicates that competent OES authorities will operate in collaboration with industry, provide guidelines, communicate with OES members, and introduce an assessment process, including an audit plan. A proactive monitoring system focused on active control only once an event took place, it would serve to satisfy the requirements of the NISD regulations. The method is confined to ex-post monitoring, i.e. post-incident, for the Office of the Intelligence Commissar (ICO), responsible for regulating DSPs. Therefore, the ICO is encouraged to provide guidance and support for DSPs and to have an effective way of identifying if an event occurred and taking action once it has taken place.

3.4. Identification of Operators of Essential Services and Digital

Essential Services

Schedule 2 to the regulations [31], defines requirements for determining who contributes to the NISD regulations. The levels for each sector are different: energy, electricity, transportation, safety and digital infrastructure. It is the OES's duty to identify itself and to alert and communicate with the competent authority, which is responsible. Competent authorities in their industry or area should however be diligent when communicating with prospective OESs.

If the authority determines that the agency is an OES, the NISD regulations include the power to allow the authority to collect the necessary information in order to assess whether the company satisfies the edge standards and officially designates the institution as an OES. If an agency, which requirements is considered by a competent authority, is not associated with an OES, the authority concerned that, by notification, revoke the designation deemed. Similarly, if an individual does not meet the requirements to be designated as an OES, a qualified body can revoke a designation.

If the OES is not certain whether or not they are bound by the NISD, the appropriate body responsible for providing this confirmation will notify them. If an individual is not beyond the edge of assignment as the OES, then the Competent Authority decides that there may be substantial detrimental consequences of an event involving protection affecting supply by that entity to the critical service, instead the Competent Authority may agree to appoint the entity as an OES according to regulation 7 of the NISD rules [34]. Such marking ability should only be used as an exception to pick OESs. The body must be clearly explained in the reasons for naming an agency, if appropriate, to avoid unnecessary legal challenges, the classification of the company should be accepted beforehand. Responsible Authority may take charge of an inventory of the OES within their industry or area in order to ensure that the UK is able to satisfy the regional reporting requirements and liaise with competent authorities representing an analogous field in specialized administrations. The SPOC is liable for distributing the volume and importance of the annual report to the ECU Commission for other Member States of the OES. Competent Authorities are responsible for handling and updating the inventory of OES in their sector or region on a biennial basis.

Digital Service Providers

DSPs are considered to be online markets, search engines, cloud services providers. The NISD regulations contain additional explanations as well as the Government Response to consultation [31]. DCMS claims that to have a NISD DSP, it must provide its services to external entities or companies. For example, when an operator provides its workers with network naming facilities, this operator will not be within reach for its employees but not for employers. If both an OES and a DSP are entities, the entity shall follow all structures in compliance with the NISD [3]. Under these conditions, DCMS firmly urges the responsible body, and hence the ICO, to coordinate the efforts to reduce overlap by itself and the governed operator and to insure that the operator is not standardized.

A DSP with less than 50 employees or €10 million a year turnover, is exempt from the requirements of the NISD regulations. The exemption is meant to reduce the regulatory burden on small and micro-enterprises and only applies to individual companies. A company that is part of a larger group may also be required to include employees headcount / turn / balance sheet data from that group. This often refers in relation to the SME carve-out clause in Article 16(11) of the NISD in Committee Recommendation 2003/361/EC [36]. In a timeline defined by the ICO, DSPs are expected to register with the ICO. This registration is intended to make DSPs easier to identify. DCMS encourages the ICO, as soon as practicable, to place such registration on the spot and to inform potential DSPs and DSPs as appropriate.

3.5. Determination of incidents

Regarding NISD regulations [32], an incident will be: (i) Any event with an effect on network safety or the IT systems used to provide essential services; (ii) any event where network and knowledge systems are secured. Network power and knowledge systems have the power to resist any action affecting the provision of services, genuineness and integrity in a certain degree of confidence, and this has a major impact on the continuity of the critical services they provide.

For the OESs, the competent authority accountable for each sector is liable for the dissemination, for every sector with accident monitoring requirements, of the many impacts to be defined by the NISD. In November 2017, the Competent Authorities received guidance on determining thresholds for incident reporting. Within the scope of the Commission Implementing Regulation 2018/151 of 30 January 2018 [37], the accident notification requirements have been introduced for DSPs.

To reach consensus on all requirements of the sectoral Lead Department (or Departments), and subsequently of the NCSC, DCMS urges Competent Authorities to discuss and reach an agreement. When deciding the appropriate criteria, the responsible authorities are required to inform the OESs. Cross-border interaction with the Republic of Eire is further facilitated in the

case of Northern Ireland. The aim of this agreement is to coordinate the North and South approaches of the border to facilitate the smooth running of critical systems serving each nation. Therefore, in Northern Ireland, competent authorities should work with other competent authorities within the UK and competent bodies in the Republic of Eire to keep HMG informed and, therefore, SPOC of progress if necessary.

3.6. Enforcement

If a DSP or OES does not comply with NISD, it is by way of knowledge and administrative correspondence that competent authorities may take various measures to impose their judgments. In order to give competent authorities maximum flexibility in the precise process of any enforcement action, a process is often initiated under the NISD Regulations [31]. Competent Organizations should take into account that simply having an incident doesnt authomaticaly lead to a penalty according to the NISD. An autdit should take place in order to specify whether or not adequate and proportionate security measures and prosecutions were in place.

Competent Authorities must be as transparent as possible when establishing their enforcement processes or undertaking enforcement actions. Transparency is one of the legislative principles of excellent regulation and underlies key provisions of the Code of Regulators and the Strategic Code of Practice of the Scottish Regulators [38]. In order to make OESs and DSPs clear of their approach, it is crucial for the competent authorities to publish their policies. A step-by-step compliance mechanism in which OES and DSPs are alerted should be enforced by competent authorities.

The competent authorities need to take into account the following mandatory factors by considering an enforcement action, including financial penalties, to ensure that this action is acceptable and proportionate:

- Either OES or DSP representation.
- The regulation launches any measures taken by an OES or DSP to comply.
- Any measures taken by an OES or a DSP to correct results of failure to comply.
- Whether the OES or DSP has had enough time to implement the regulations and requirements.
- Whether the breach is likewise enforceable under a different regulatory framework.

The competent authorities should also notice their responsibilities to comply with the expansion duty, which allows a person carrying on a regulatory position to contribute to the advisability of supporting the economic cycle (the 'development duty'). While carrying out their duties, the value of the practice of regulatory roles while order to promote the economic cycle must be taken into account, in order to ensure that regulatory action is only taken when required and that any intervention is proportionate.

There is a risk that many pieces of legislation may be violated at a time because operators will need to adapt to a wide variety of laws. If an infraction arises that contradicts quite a piece of legislation, the competent authorities will note that and negotiate with others the best solution if practicable but will stay pragmatic, so long as this is reasonable and proportionate, to conduct their own responses to any violation. The Competent Agency decides that the financial penalty for an OES or the DSP should be discussed with the OES or the DSP the outcome of the investigation.

3.7. Monetary penalties

If necessary, competent authorities shall have the right, in accordance with the NISD regulation, to levy significant financial penalties [31]. Full analysis of penalties is required to establish that the punishment is sufficient and commensurate with the offense for which the penalty is levied, and thus the industries in dispute. In light of the operator's comments, measures need to be taken to comply with the NISD regulations, measures taken to address any consequences and other legislation that is breached, the competent authorities shall consider them. The competent authorities need to fair and take into consideration factors for each industry or area in a coherent way over the whole of the UK and between sectors. What is a cost-effective and reasonable monetary penalty is different worldwide. A strong, proportionate, transparent and defensible framework for penalties should be implemented by Competent Authorities. Standards should be defined and be unambiguous during this penalty framework.

3.8. Appeals

The competent authorities are required to provide an impartial and clearly explained route to appeal against regulatory decisions or failure to act in accordance with the Regulators Code, in line with the regulator's code and, consequently, the Scottish Regulators ' Strategic Code of Practice [38]. This will be an internal process, but it should not be a matter of individual Regulation Officers who took the decision or action against which the appeal was brought.

The NISD regulations [31] also require competent authorities to determine an independent appeal procedure, if requested, for an appeal against: the appointment of OES that do not meet thresholds; and any monetary sanctions. The aim of this appeal is to complement an established appeals process for the responsible authorities. Responsible authorities will insure that

their appeal processes are fair, open and accessible for everyone regulated, be they autonomous or internal.

3.9. Cost recovery

The OES or DSP are often required to pay the reasonable cost of the investigation in order to complete an examination or inspection. The NISD regulation also includes an impact on the recoupment of reasonable costs from regulators by competent authorities. In performing a relevant function under the NISD regulations, a competent authority may establish a system to recoup reasonable costs incurred in or on behalf of that authority (see Part 6 of the Regulations) [31]. The Competent Agency shall provide the OES or DSP with a report specifying the work done, the expense and the time period covered by the payment. In 30 days following issuance of the invoice the bill is due by the OES or DSP and can be recovered as a civil debt. If a competent body wishes to recover costs via a hard and fast fee-based regime, a substitute fee regime may need to be determined [31].

As with any new fee system, Competent Authorities will seek the approval, before implementing a bill, of their respective government agencies and/or HM treasury. Every fee scheme should be transparent and take the impact on the sector (e.g. through consultation with the sector) into account. When additional legislation is necessary to enforce such a policy, the competent authority would comply with its relevant department.

4. The General Data Protection Regulation

The General Data Protection Regulation (GDPR) 2016/679 [2] was adopted on 27 April 2016 after years of dialog and preparations on the ECU Parliament and Council with a view to the processing of private data and the free circulation of such data. They began application as of 25 May 2018 and, after the expiry of the two-year transitional period, may revoke Directive 95/46/EC. The GDPR does not need additional laws enforced by Member States in the regulation because they can be controlled and have a direct effect. The GDPR was directed at the reform and harmonization of EU data protection laws. The technological occurrence and the disruptive world demanded major changes in data privacy. For the business, GDPR inevitably means new responsibilities, structural changes and cost of compliance on the one hand, but most significantly, security; the elimination of barriers, and hence the responsibility of data transfers. The EU institutions recognize development through the implementation of the law, incorporate certain facets of the business system and lay the foundation for recent legislation which is compatible with the technologically advanced world.

The reforms in EU data protection law that are most applicable to companies will be covered in this segment. Scientists and clinicians are mainly concerned that the GDPR must conform to the principles mentioned below. Certain amendments are listed or not covered either, as they are governed in the previous Regulation in the same way, or do not make extreme variations in the business process.

4.1. Scope

The relevant rules of the EU are extended with favor of GDPR to all or most EU manufacturers / controllers. However, the Regulation seeks to provide data protection for both citizens within and outside the EU. GDPR has an expansionary strategy in accordance with the Directive on "Equipment Usage" by implementing a universal implementation of EU laws and regulations. The latest rules are based on the extraterritorial impact of a law by expanding its implementation scope to non-EU inspectors or processors [26]. By setting up Section 3, GDPR expands the breadth of its operation to non-EU inspectors or processors where the procurement operations are linked to: (i) the provision of products or services for those data subjects within the EU, irrespective of whether payment of the info subject is necessary; or (ii) track their actions as far as the behavior of such data subjects is concerned within the EU.

Many authors give special interpretations to two slightly controversial aspects of this concept in order to explain the terminology used by the EU lawmaker. For instance, this statement: "provides very easy links to a website or email address; the use of language or money commonly used in one or more Member States may also be shown to give an opportunity to purchase goods / services there". Also, another statement is the following: "comportment tracking" is when users are monitored on the network utilizing formulas using a profiling method to make decisions. The key regulatory moment of EU statutory history, with the two clarifications on processors/controllers outside the EU, guarantees the clarity of one package of regulations (regarding the integrity of data and data protection) under GDPR for non-EU businesses already targeted at EU residents through marketing strategies [2].

In the case that personal information is handled "under the operations" of such an entity that it is listed, regardless of the specific location of processing (EU or not), the GDPR will be applicable; the Regulation applies to companies which have EU "institutions" [39]. The word "government" has been amended by the Court of Justice of the European Union within the 2015 Weltimmo v NAIH case [40]. Many key principles are often drawn from the ruling (which are often used as guidance):

- The legitimate kind of an institution cannot be a determining factor, it may be a local agency, affiliate, office of sales etc.;

- The location where the organization reported must not be definitive with respect to the knowledge processes; the definition of 'state' is to be loosely interpreted

A meeting of an EU delegate is provided as an external requirement for non-EU controllers and processors subject to EU data protection law. Similarly, to this the controller or processor shall be in the position of the delegate. The new functions of the supervisory authorities are mainly responsible for this regulation. European authorities shall ensure that the GDPR is upheld and that information sharing issues are covered through the right to contact the official in regard to the exploitation of knowledge [2]. In making this specific change, instead of at the place of service of the entity, the legislature transfers the main goal of the law for the relation with the EU citizens.

4.2. Harmonizing data protection rules

One of the reform's most important objectives was to harmonize the regulation on info-protection for all EU Member States. In this context, consultations have taken place between the organizations about just what shape the law will take. The legislator now selects the form of the regulation, taking account of the previous directive. Second, the compilation of the legal document indicates that existing matters relating to EU data protection legislation harmonization will no longer exist. Furthermore, it is evident that the Commission has followed the idea that regulation is directly applicable by including regulations during a legislative era. While between implementation and the final enforcement of the law, a deadline may be defined, the GDPR is used explicitly, and no transposition in the countries is necessary. The EU representative choosing a legal document indicates the plans to establish a data protection and privacy issue for the EU [41].

The new legislation must ensure the security of privacy through Member States in a cohesive way and can enable the free flow of private information between the Member States when it continue to implement the GDPR system [42]. The new legislation must guarantee the protection of privacy in every Member State. Not only at the level of people is this dimension of the transition significant. There is hardly any business that exists on one market in a globalized world and has a global atmosphere that is in accordance with the EU's values – 'free flow of commodities, capital, services and people', as defined in the Treaty on the Functioning of the ECU Level [43]. The EU authorities are aiming to give companies the ability to handle their data in compliance with the relevant rules and principles in any jurisdiction within the framework of the GDPR through the harmonization of regulations. Therefore, both primary and latter roles should place on the data processors / controllers a fair responsibility with respect to the relevant topics.

4.3. One-stop shop

The so-called 'one-stop shop' clause is linked to the uniformity of the data protection law. This concept is often used in other fields of legislation to avoid situations where multi-regulators are accountable by an analogous organization in several Member States to govern their similar operation. The standardized decision-making method is given to bring this law into effect. In the light of the GDPR, the EU Member State Data Protection Agency, in the case of a private data controller / processor set up in two or more Member States, where the controller or processor has its primary institution, would be able to supervise its operational operations overall by Member States [44].

The GDPR reflects a significant shift in interaction with the data security authorities for multinational companies competing on a variety of EU markets. As an illustration of this, we may think of one individual company that offers service in many Member States, but the bigger proportion of assets are in one Member State, e.g. Netherlands. GDPR allows companies to remain in contact with only one national data protection agency [45]. According to the GDPR, that means that there are "key services" of the business, which is why the Dutch DPA is responsible for the organization's oversight and supervision of IT operations. The initiatives should be based on using a one-stop shop system in order to avoid creating more problems than solving them. In order to develop a privacy plan which addresses a number of data protection hazards, the company will be prepared to contact a leading DPA [46]. The outcome is designed by EU officers which adopt a fair and equitable compliance policy. The process by which DPA cooperates is named 'consistency framework' and aims to lead to a consistent application of the Regulation. The EU Commission and thus the European Data Protection Board [47] must control DPAs. As this is often done, DPAs from different Member States avoid making contradictory judgments and policies on similar matters.

4.4. Consent

The criteria for approval are supposed to change the consumer information processing paradigm, because GDPR strengthens the standards under which user information is accessed. GDPR approval is, as in the Directive, a legal basis for data transfers. Though it was included in the previous legislation, the Regulation

substantially changes the classification pattern. GDPR makes it harder for firms to obtain a valid consent compared with the Directive. Under the previous rules, controllers were granted conditional and "opt out" approval under special circumstances. The GDPR restricts the principles because companies should obtain the consent of "a statement or transparent positive action" by the subject matter. The consent should be: safe, precise, notified and transparent, in accordance with the provisions of the GDPR [48].

4.5. Controllers, joint controllers, processors

The GDPR follows the existing practice by transferring most of the data protection obligations and responsibilities to application controllers. By accordance with the Directive, the GDPR states clearly that joint controllers will exercise their rights against each of the controllers by their shared responsibility for enforcement.

The term "processor" is analogous to the concept of a human, lawful, state, public, entity or other body processing data on behalf of the knowledge controller. However, the GDPR introduces another new aspect in their responsibility in data infringement reporting [49]. After this, processors are required to take note in writing about the service practices of each manager and assign an information compliance officer if necessary. The GDPR is liable for their data infringement reporting responsibilities [50].

4.6. Privacy by design / default

Two specific principles are acknowledged in the Regulation: 'Project secrecy' and 'Minimum confidentiality'. The EU level privacy information security by design / default was not included in the Directive through comparatively new approaches; nevertheless, certain elements could be described in the directive. In a business context, the GDPR notes, companies become the target of a duty with which data protection of consumers should also be taken into account throughout the whole information collection phase at the very first concept stages of a project. To grasp and evaluate the two definitions even easier, they will be clarified separately [2]:

- Privacy intentionally - through its means, in the initial design phases and throughout the whole process of new products, processes and services involving personal data, organizations' implementation of acceptable technical and organizational measures considering the privacy law

- Data protection by design - indicates that the default collection should be the most privacy sensitive if one or more of the program or programs require choosing the privacy topic at which point their data might be exchanged with other users.

The senator understood that secrecy can not only be assured by statute. Through incorporating the two new concepts (through by design / default), the EU authorities have accepted the fundamental importance of privacy as an aspect of information preparation and distribution and operating framework for every organization and company.

4.7. Notification of breaches

The GDPR establishes a European-wide data protection reporting requirement for the primary period of EU legislation. Article 33 of the Act [2] specifies that, within 72 hours of or after the offense has been performed, officials should be informed by the organization. It is often only if the organization would determine that there were no real risks to data subjects incurred by a breach of the records. If the controllers / processors are not so willing, then they will face penalties of up to 4% or up to €20 million worldwide. An equal fine is applied to organizations if the DPA reviews an organization's activities for the security of private information and concludes that they are inadequate and therefore inappropriate for the potential risk.

The law not only requires the organization to share knowledge that an infringement on data concerning privacy was perpetrated by defining the reporting standards under GDPR. In fact, what the Regulation implies is that companies should include data categories, records affected and approximately the number of data subjects affected and therefore details of what hackers or employees are to do [51].

However, privacy infringements are not unique to law internationally, they are enforced in the US, in Australia; in certain Member States, in the UK and Italy; but the GDPR scale backed and assured by the large fines, in particular, expands and enhances the scope of the knowledge violation notice. This criterion provides the principal difficulty in determining the severity of the company's data leak. The knowledge of a data leak reported to the organization within the first weeks following a serious violation shall be seen in the most common cases. Although the organization recognizes that the tapes or other type of assault have been broken, the time-limit of 72 hours may be inadequate for the organization to accurately predict the effects for individuals. In this case, it will be extremely important for companies before the GDPR begins to develop a system to determine whether a breach is of considerable risk and must be alerted. In this sense it is very essential. For a company to grow into the need and related timetable, it will be difficult.

4.8. Demonstrating compliance with the GDPR

The new legislation on data security also includes the following aspects of the GDPR. We are categorized into a separate section because all of them allow organizations to show conformity with the regulations, proposals, and other aspects of GDPR previously discussed.

Codes of conduct

This Directive incorporates the idea of codes of conduct as to how to demonstrate compliance with the info-data protection law. The central aim of the codes of ethics is similar to GDPR - these standards function in order to enhance total conformity with the Regulation and are implemented in organizations. There is, however, some new aspects which should be listed as they affect companies. For the DPA, more agreements for the publishing of codes of conduct have first been identified. The law calls for the submission to the professional DPA of draft codes of conduct and the adoption or modification, if applicable, of them after release. The DPAs also have the duty to nominate an independent body to track the code's compliance through the application of the codes. Furthermore, non-EU controllers and processors may use compliance with authorized codes for cross-border data transfers. This regulation creates the opportunity for international business growth as it simplifies cooperation for businesses to extend their market or cooperate with other non-EU partners.

Certification

Certification may be the most contentious and debated data protection reform proposed by the GDPR [2]. GDPR acknowledges the credential as a legal document officially in relation to the Directive. It is one of the methods included within the Law for self-regulation. Certification would act as a strong indicator for customers that other companies have faith where data security is concerned, and the company has taken reasonable steps to insure the data collected is protected. The EU lawmaker supports the usage of third-party systems to show conformity with the data protection regulation as the mechanism is voluntary [52].

An authorized testing organization shall conduct the certification process. This entity will advise the supervisory authority of the judgment with appropriate justification only in the case of both the awarding and withdrawing of the credential from the company.

From a legal standpoint, Eric Lachaud provides two reasons on the credential - "special points" and "managing method" in [53]. The registration, as a "trademark", protects the third parties' interests and labels this procedure or its effects as a "program". Nevertheless, Lachaud disputes in his paper whether its requirements have been followed in the initial concept of including approval in the Regulation. The author's main argument is that the process described does not comply with some EU regulations and does not provide the organization with enough opportunities for its role in this phase (especially in the case of small and medium-sized enterprises). However, the author emphasizes that the credential can be a private qualification with no legal consequences, which can be troublesome for the essential use of the process.

The certification process is often perceived to be both a liability and a business opportunity [54]. Therefore, as companies continue to develop and cross-border data transfer is a day-to-day issue, this approach can promote international relations with countries which have already developed qualification (such as the USA) which ultimately will result in less expense. The certified certification body will, on the other side, offer additional business incentives for third parties.

Data Protection Officer

In compliance with the GDPR, the hiring of a data protection officer ("DPO") is mandatory for certain private and public organizations [2]. The task of this position will be to control the production activities of the businesses. Specific criteria are defined according to which DPO should be named by organizations:

- The server may be a public authority or - an excessive collection jurisdiction with specific categories of information referred to in Article 9 and private data involving offenders and offenses referred in Article 10 can require regular and institutional supervision of knowledge subjects.
- It is important to note that a previous draft Regulation includes a specific criterion – for businesses with around 250 workers, it was mandatory to name a DPO. It was most probable that the EU lawmaker found the test to be focused not on objective tests but on qualitative assessment.

The role of the DPOs is not well-defined in industry based on the terms of the law. In that direction the "DPO guidance" on the implementation of the regulations of the GDPR concerning the need for controllers and suppliers to nominate a DPO are issued along December 2016 by the working group of Article 29 [2]. The title, place and ultimately the duties of the DPO, taking into account its function within the corporate structure, shall be covered in this text.

4.9. Data Protection Impact Assessment

The GDPR allows businesses to conduct an data protection impact assessment (DPIA) for the intent

of estimating the potential risks that occur in any new production activity. Although the organization's basic requirements under the old Directive provide a valid basis for possible high-risk operations, several EU companies are currently needed under the Regulation.

The new technologies are mainly responsible for the implementation of this regulation into the GDPR. Innovation and technology 'conquer' consumers and unfortunately people do not always know completely how well their data are handled. The explanations for the new legislation on privacy are complicated. The controllers prevent data errors (subsequent to negligence) and, respectively to heavy penalties, by evaluating the potential risks involved with the transmission operation before actually applying it.

Two similar procedures must be followed for the purposes of the current business impact research. The risk assessment organizations are to decide if there is a possible high danger – must not be mistaken with the overall risk control mechanism [55, 56]. However, the distinction in compliance with Article 35 of the GDPR, the DPIA is dealing with risk management as a whole, including organizations and practices [2]. As for risk management as a whole; the distinction indicates that although a certain danger scenario under the latter may be justified, the risk in the processing of the personal data and the interaction with the personal space cannot be justified.

4.10. New rights for the individuals

All the above laws are intended to guarantee, firstly, individuals' freedom and, secondly, to promote and make businesses easier to access. With this in mind, the GDPR deals with the problems with new rights given to people in the context of the market difficulties. Moreover, such improvements mostly increase the intensity of the freedoms or provide EU citizens with totally new privileges. The details involved are to engage in the data collection and not make them oblivious to their own results. Furthermore, functional rights are granted to people to say that their own identity is backed by regulation.

The Rights to be forgotten

This significantly enhances the ability for the customer to order the controller / processor to delete his / her personal information from his / her devices and automated and written records. If the material is not required, the person may ask for "the right to be lost" if the law does not apply, if the subject may withdraw its acceptance, etc. The law calls for greater flexibility for the client when they address a wider range of erasure demands. In fact, it often constitutes an additional duty to take appropriate and prompt action to inform third parties that any references have been sought by the person.

In [57], it is shown the reason for the organizations implementing this particular procedure in GDPR. The argument was based on the "freedom to forget" concept because the question of processors and controllers' responsibility for personal data in the search engine was revealed. The Court of Justice has accepted this opinion by creating a general principle, revised and explained in accordance with the developments in the digital world and included in the GDPR. Another key point which academics sometimes overlook but which is articulated as a concern by practitioners is the reality that the company structure requires a process that is often used to execute data 'erasure'. In fact, companies handling large-scale information should have tools that define the importance of expertise in the context of its use; to be preserved or lost.

"Pseudonymization"

The Regulation introduces a new EU data protection law principle which does not reveal data and does not fully identify data when processing data. "Pseudonomyization" allows companies to distribute such details so that they often interact with both sets of expertise independently without additional information [2]. This technique protects the person's identity because the details cannot be related to the individual. The utility of the approach is preserved for businesses as it permits the use of data without revealing the identity of the user and reduces risk of breaches of information.

Data portability

The right to data portability is an important right that the GDPR gives to data subjects [2]. The purpose is to give the user an opportunity to collect, reuse and move their personal data from one data manager to another; from one IT setting to another [58]. The key phases in the "Digital Single Market" are often seen together [59].

Organizations should provide the information in a "machine-readable" and accompanying format, and the data subject will send the details to a supervisor or, perhaps under certain situations, to a rival. Since this law offers the controller a reciprocal duty, it is not limitless for the client. The GDPR notes that the organization has no requirement to implement such authentication systems in order to be technologically compliant with the transition of the knowledge.

5. Interaction Between the GDPR and the NIS Directive

The two pieces of legislation are significantly overlapping, often applicable to the same incidents. The EU Network and Information Systems (NIS) Directive [3] is, thanks to the introduction in the UK by 9 May 2018, enabled by organizations to provide the most essential

services and report incidents affecting the technology, data and networks (systems) of the UK. In order to ensure that UK operators are ready to influence the growing number of cyber-threats in essential industries, the NISD needs to take steps to combat threats to IT systems such as energy failures, hardware and environmental dangers as well as cyber-infractions as Wannacry and NotPetya attacks. The "Digital Service Providers" (DSP), where the "less strict" regime is definitely introduced to cloud service providers, online marketplaces and search engines, has another aspect to the NISD.

It also represents awareness of the crucial role performed by these forms of shared online infrastructure in the economy as a whole, hence the incorporation of digital service providers under NISD now presents such service providers with an additional potential infringement responsibility. At the end of summer 2017 the government of the UK advised the introduction of NISD. DSPs are deemed to be necessary to identify organizations falling under the DSP concept. The DSP framework is potentially less strict as compliance evaluation and implementation can be enforced immediately after an incident or where a company is informed of non-compliance with this Directive or applicable legislation by the competent authority. DSPs which employ less than 50 people and whose annual turnover or total record does not exceed €10 million are automatically excluded from the scope of the government's decision.

5.1. Three types of DSPs

The Government acknowledged the problem with identifying a DSP when reacting to a general public survey on 29 January 2018 but clarified that three kinds of DSPs will remain in place to enable the Competent Authority and the DSP itself to understand whether DSPs are within the framework or not.

1. Online Marketplaces: identified as a website that intermediaries the distribution of products and services between buyers and sellers. Classified ads websites or shops online are not included.

2. Online search engines: enable users to access the general public on the global web – this does not require site engines operated by other website engines.

3. Cloud Computing Services includes any DSP that allows access to a distributed and dynamic set of physical and virtual tools that exchange, including the delivery of public cloud services of a corresponding character: Infrastructure as a Service (IaaS). According to the consultation response, online gaming, entertainment or VOIP services will probably have been excluded, but Software as a Service (SaaS) providers "do a decisive part of the UK economy and they are right to take responsibility for it".

Could Service Providers (CSPs) posed the most concerns with the definition of what kind of entities under the Directive should be classed as DSP. A number of topics included a need to include integration, content providers, data centers and managed services in broader areas, such as the extension of Cloud and SaaS definitions, while others felt that the definitions of all DSPs were too narrow to fall within the Directive. This raises concerns that the guidelines are not transparent as to deceptive use "online", and asks whether new kinds of "Cloud services" will occur in the future, given that new technologies are already evolving which do not fall in well with IaaS, SaaS and Platform as a Service (PaaS) definitions. CSPs are worried that these requirements are not enough. The additional costs which could be included in programs are illustrated by individuals who could come under the concept of DSP. In response to the consultation, the government, however, kept its definition and pointed out that the government has always tried to clearly define who was in scope and who was not and restrict their scope to those companies that are best able to lose services in a single Kingdom economy, which must comply with the Directive.

The NISD inventory contains 14 security principles to ensure compliance for DSPs [60]. In fact, the DSPs will take into account the National Cyber Security Center's 14 (different) security guidelines introduced [61]. The compliance regulation (Regulation), issued shortly after the government's reaction to the consultation, further defines the conditions to take into account when takes steps to introduce a safety level. More broadly, the Implementing Regulation establishes the parameters to determine whether an event has a considerable impact and whether an event is considered significant. Incidents which have a 'significant impact' to be reported to the ICO within an equal 72-hour span, as needed by the GDPR [2].

The effect of an event is called "substantial" in which, according to the Law (Article 4) [62]:

- For a total of 5 million usage hours (i.e., the number of affected users in the EU over an hour), the service provided by the DSP became inaccessible;

- The accident has resulted in a loss of credibility, reliability or secrecy of data or the services it provides or is obtained through a DSP network or device involving 100 000 users across the EU;

- The accident raised a public safety danger, triggered unrest, or contributed to material damage of more than €1 million to at least one individual within the EU.

Table 2. Differences between GDPR and NIS Directive

	GDPR	NIS
Came into effect	25 May 2018	9 May 2018 (implemented in the UK by the Network Information Systems Regulations)
Concerned with	Personal data only – data breaches (i.e., "a breach of security leading to the accidental or unlawful destruction, loss, alternation, unauthorised disclosure of, or access to, personal data transmitted or otherwise processed")	Interruption to service – an incident (i.e., "any event having an actual adverse effect on the security of network and information systems")
Applies to	All data controllers and data processors	OESs and DSPs (subject to certain exceptions)
Sanctions	Up to the higher of 4% of annual global turnover or €20m. Different infringements can arise from a single breach and sanctions can be cumulative	Capped at £17m in the UK
UK Regulator	ICO	OESs: relevant CIA (sector specific); DSPs ICO
Report to Regulator	Any data breach "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons" (data controller only)	OES: notify either CA or CSIRT of "incidents having a significant impact on the continuity of the essential services they provide". DSPs: notify either CA or CSIRT of "any incident having a substantial impact on the provision of a service {...} that they offer within the EU".
Timing of report to Regulator	Without undue delay and not later that 72 hours where feasible.	Without undue delay (UK to add "and not later than 72 hours where feasible")
Report to data subjects	Any data breach "when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons".	OESs: not requirement but CA or CSIRT may inform the public. DSPs: no immediate requirement but many have to inform an affected OES or be required by CA or CSIRT to inform the public.
Timing of reports to data subjects	Without undue delay.	No requirement.

- Personal services companies, especially with big business consumers, will need to analyze concern, whether customers object to lack of service or damage caused by the accident, whether disclosing an occurrence alluded to in item 4 above could or might not pre-empt DSP's role.

Organizations requesting NISD monitoring will also be subject to the GDPR reporting requirements, although the NISD reporting plan is much more complex than the need to disclose personal data breaches in compliance with the GDPR. The GDPR and NISD employ different standards to determine, with far greater detail given under NISD Implementing Regulations, what could be deemed to be the technological and operational controls. What does appear possible is that a DSP reporting private infringement under DPD could unintentionally lead to the emphasis on the DSP equivalent which does not comply with the safety elements begun in Article 2 of the Implementing Regulation [2]. The violation is not considered as an event of a "substantial impact" under NISD. NISD failure could end up with penalties of up to £17 million. The Government of the UK has announced, in relation to the amount of penalties possible under the overall Data Protection Regulation (GDPR), that it would place a combined ceiling on £17 million for contraventions on the 2 bands

– and so a penalty band will include all contraventions. The government of the UK acknowledged and may prohibit voluntary coverage as a risk to "multiple threat", while reiterating that it will have to act reasonably, adequately and proportionately. Nonetheless, we have to take protection seriously and the government also hopes that the high amount of penalties would promote behavior changes.

5.2. The NIS Directive: for whom and what does it mean?

In May 2018, the GDPR in addition to its enforcement, a British Data Protection Act amendment created the standards of GDPR as UK regulations. In turn, by promoting the implementation of the universal and European standards, NISD was also introduced in UK Law in May 2018, helping in the EU to improve the protection of network and software systems. To organizations offering essential services or those supplying those who provide these services, it is of special importance. Nonetheless, there is nothing to think about conformity with the NISD. Organizations will gain conformity through the introduction of best practices in International Standard on Information Security and the implementation of comprehensive Disaster Recovery and Business Continuity Management Systems. The NISD discusses the challenge of loss of service in IT networks and information structures where GDPR is dealing with the protection of private data. In particular, the protection of essential services involves fines up to £17 million or 4 per cent of worldwide turnover, and individuals who fail to implement effective cybersecurity measures will be penalized. The measures laid down in the NISD are part of the five-year National Cyber Security Strategy of the UK Government. These are intended to ensure secure and defensive from cyberattacks from the critical networks and resources of the UK. In addition to showing a responsive cybersecurity, operators in power, transport, water, oil, safety and digital infrastructure have to prove that they need comprehensive incident response plans on the spot.

Nevertheless, the NISD Regulation is not restricted to these organizations. It is vital that UK technology companies decide whether or not the NISD applies, as it relates not only to essential services but to important service provider suppliers. This encompasses organizational mess and includes online markets, online search engines and cloud services. The Departments of Education, Entertainment, Media and Sport have made clear that their proposed penalties up to £17 million as a final resort. While this amount is highly significant, operators should prove that sufficient risk analyses are required, effective precautions have been introduced, solid incident response measures have been established and the system is widely employed, the sanctions will not be enforced. Therefore, the key is to show that the NISD is at the heart of the cyber defense strategy of an organization. The following steps must be addressed: recruitment of staff through penetration testing, control of accidents, stability readiness and continuing resilience. All who are already in the path of GDPR implementation need to be required to comply with the requirements of the NISD, but it is important to understand what further steps must be taken. Thanks to the management of this process, professional support is crucial and cost-effective. SRM has helped many organizations become ready for ISO27001 certification [63] and can support the continuity of business and disaster recovery. SRM consulting teams can manage the method without dalliance or budget with experience and expertise across a wide range of organizations, and a sound understanding of what the NISD is all about.

5.3. NISD Impact and GDPR Security Requirements

We can notice that the GDPR and NISD overlap significantly. All legislation requires operators to incorporate risk-based security measures and both laws provide provisions for reporting of incidents. These do defend different interests, though, and should refer to multiple types of incidents.

Firstly, we need to note that there are different rules that activate expertise under the Directive and subsequently the GDPR. The GDPR shall apply, with few exceptions, to a person or entity that processes or monitors the personal data of the EU residents related to the provision of products or services. The NISD is much closer for service providers and digital service providers employing 50 or more. Therefore, only in comparison to these operators, the similarity exists. Secondly, the Directive is fully focused on network security, where the objective of the GDPR is to preserve personal data. Therefore, the GDPR includes regulators, while the Directive allows operators to safeguard their networks properly, to ensure the delivery of the services. Although these priorities frequently intersect, the safeguards will also vary in some cases. Encryption, for example, will help protect personal data under the GDPR by shielding the network from misuse in compliance with terms of the Directive.

It is the same for the notice of a breach. The GDPR includes safeguards, without unreasonable pause or, if possible, not less than 72 hours after they have become informed of a violation, to alert the relevant authority. It is doubtful that the breach of private data will contribute to a danger of people's rights and liberty. Thus, it is only when personal data have been at stake where GDPR needs disclosure of an infringement. On the contrary, the Directive requires notification for violations if the provision of the service is seriously disrupted. There are no provisions for jeopardizing

specific information since it is not protected by the GDPR. The Directive also penalizes operators who do not carry out adequate security procedures or who do not alert the competent authorities of a case.

Finally, operators shall only notify the competent authorities in accordance with the Directive. But the GDPR includes controls to alert subjects of details, i.e. Persons — where the abuse of their rights and freedoms faces a "high risk". In addition to regulatory measures, the GDPR gives certain people a specific right of protest. Only administrative fines are provided for in the Directive.

The order stipulates that it will adhere to the GDPR 'without discrimination', we cannot determine with certainty what occurs by contradicting commitments. In cases where the operator has violated the provisions of the two laws, the Directive is likely to result in additional liability. Could GDPR, therefore, act as a compliance aid under the Directive? There will undoubtedly be many issues with the introduction of these new laws over the next few years.

From a practical point of view, organizations that need to comply with both GDPR and NISD will need to be able to understand how these affect their business operations and overall processes. In order to accomplish this, novel maturity models that incorporate both regulations need to be developed and used [4] in accordance to ISO or NIST standards. Also security measures that take into account requirements from both legal frameworks must be deployed, especially those that are focusing on critical infrastructures [64] and industrial control systems that is the heart of many OESs [65].

5.4. GDPR and NISD at a glance

Debbie Heywood, in [62], identifies GDPR-NISD in relation to infringement reporting requirements and differences. On 9 May 2018, Network Information Systems Regulations 2018 implemented the NISD in UK legislation. Although the GDPR is broadly available, NISD only affects certain companies. The GDPR focuses on personal data, while the NISD is more concerned with the network and system security and service interruption. Organizations collected by NISD must also have to adhere to GDPR for all personal data. In Table 2 we identify the main differences between the two legislative sets.

6. Conclusion

Although GDPR and NISD are related to different types of data they overlap since security and data protection are related to each other. Moreover, both regulations aim at protecting organisations against cyber attacks. Their adoptions from the organisations is often a challenging task as CISOs and DPOs face difficulties to understand their roles and design consistent cybersecurity frameworks inside their organisations, due to the regulations' requirements overlapping. To address this issue a mapping of GDPR and NISD requirements is presented that can help organisations to adopt properly to these regulations, help them to identify current potential security issues and structure new security plans.

References

[1] Refworld, "European union, directive 95/46/ec of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data," 1995. https://www.refworld.org/docid/3ddcc1c74.html.

[2] E.-L. A. to European Union law, "The general data protection regulation," 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504.

[3] E. P. C. of the European Union, "Making the most of nis – towards the effective implementation of directive (eu) 2016/1148 concerning measures for a high common level of security of network and information systems across the union com/2017/047," 2017. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0476.

[4] A. Aliyu, L. Maglaras, Y. He, I. Yevseyeva, E. Boiten, A. Cook, and H. Janicke, "A holistic cybersecurity maturity assessment framework for higher education institutions in the united kingdom," *Applied Sciences*, vol. 10, no. 10, 2020.

[5] T. A. Diamantopoulou V. and M. Karyda, "From iso/iec27001:2013 and iso/iec27002:2013 to gdpr compliance controls," *Information and Computer Security*, 2020.

[6] "Nist privacy framework: A tool for improving privacy through enterprise risk management," 2020. https://www.nist.gov/document/nistprivacyframeworkpreliminarydraftpdf.

[7] I. O. for Standardization, "Iso/iec 27701:2019 security techniques — extension to iso/iec 27001 and iso/iec 27002 for privacy information management — requirements and guidelines," 2019. https://www.iso.org/standard/71670.html.

[8] Z. Wen and G. Vasileios, "Benefit and cost of cloud computing security," in *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, SmartWorld / SCALCOM / UIC / ATC / CBDCom / IOP / SCI*, pp. 291–295, IEEE, 2019.

[9] Z. Wen, K. Maciej, W. Paul, and G. Vasileios, "Formal verification of secure information flow in cloud computing," *J. Inf. Secur. Appl.*, vol. 27-28, pp. 103–116, 2016.

[10] V. P. P. De Hert, *The Data Protection Regime Applying to the Inter-Agency Cooperation and Future Architecture of the EU Criminal Justice and Law Enforcement Area*. 2014.

[11] M. B. N. Robinson, H. Graux and L. Valeri, "Review of the european data protection directive," 2009. https://www.rand.org/pubs/technical_reports/TR710.html.

[12] European Parliament, "Regulation of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation)," 2012. https://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf.

[13] E. Commission, "Data protection in the eu," 2016. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.

[14] I. Consulting, "Article 17: Right to erasure ('right to be forgotten')," 2016. https://gdpr-info.eu/art-17-gdpr/.

[15] Privazyplan, "Article 15: Eu gdpr "right of access by the data subject"," 2016. https://www.privacy-regulation.eu/en/article-15-right-of-access-by-the-data-subject-GDPR.htm.

[16] I. Consulting, "Article 20: Gdpr right to data portability," 2016. https://gdpr-info.eu/art-20-gdpr/.

[17] I. Consulting, "Article 34: Gdpr communication of a personal data breach to the data subject," 2016. https://gdpr-info.eu/art-34-gdpr/.

[18] Privazyplan, "Article 25: Eu gdpr "data protection by design and by default"," 2016. https://www.privacy-regulation.eu/en/article-25-data-protection-by-design-and-by-default-GDPR.htm.

[19] L. Maglaras, G. Drivas, K. Noou, and S. Rallis, "Nis directive: The case of greece," *EAI Endorsed Transactions on Security and Safety*, vol. 4, no. 14, 2018.

[20] G. Drivas, A. Chatzopoulou, L. Maglaras, C. Lambrinoudakis, A. Cook, and H. Janicke, "A nis directive compliant cybersecurity maturity assessment framework," *arXiv preprint arXiv:2004.10411*, 2020.

[21] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 2017.

[22] D. Markopoulou, V. Papakonstantinou, and P. de Hert, "The new eu cybersecurity framework: The nis directive, enisa's role and the general data protection regulation," *Computer Law & Security Review*, vol. 35, no. 6, p. 105336, 2019.

[23] M. D. Cole and S. Schmitz, "The interplay between the nis directive and the gdpr in a cybersecurity threat landscape," *University of Luxembourg Law Working Paper*, no. 2019-017, 2019.

[24] E.-L. A. to European Union law, "Commission directive 95/45/ec," 1995. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0045.

[25] d. H. Paul and P. Vagelis, "The council of europe data protection convention reform: Analysis of the new text and critical comment on its global ambition," *Computer Law & Security Review*, vol. 30, no. 6, pp. 633–642, 2014.

[26] B. L. Privacy and D. Security, "The final european union general data protection regulation," 2016. https://www.wsgr.com/images/content/1/5/v2/15414/BloombergBNA-0116.pdf.

[27] P. M. Schwartz, "The eu-us privacy collision: a turn to institutions and procedures," *Harv. L. Rev.*, vol. 126, p. 1966, 2012.

[28] enisa, "Enisa: European union agency for cybersecurity," 2004. https://www.enisa.europa.eu/.

[29] G. Greenleaf, "Renewing convention 108: The coe's' gdpr lite'initiatives," *142 Privacy Laws & Business International Report, SSRN.*, vol. 17-3, pp. 14–17, 2016.

[30] E. P. C. of the European Union, "Regulation (eu) no 526/2013 of the european parliament and of the council of 21 may 2013 concerning the european union agency for network and information security (enisa) and repealing regulation (ec) no 460/2004 text with eea relevance," 2013. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32013R0526.

[31] E. P. C. of the European Union, "The network and information systems regulations 2018," 2018. http://www.legislation.gov.uk/uksi/2018/506/made.

[32] enisa, "National cyber security strategy 2016-2021," 2016. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf.

[33] N. C. S. Centre, "Nis guidance collection," 2018. https://www.ncsc.gov.uk/staticjson/ncsc-content/files/NIS%20Guidance%20Collection%201.0.pdf.

[34] E. Parliament, "Review of the directive on security of network and information systems," 2020. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-review-of-the-nis-directive.

[35] Gemserv, "Consultation on the security of network and information systems directive," 2017. https://www.gemserv.com/consultation-security-network-information-systems-nis-directive/.

[36] E. P. C. of the European Union, "Committee recommendation 2003/361/ec," 2003. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:EN:PDF.

[37] E. P. C. of the European Union, "Commission implementing regulation (eu) 2018/151," 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2018%3A026%3ATOC&uri=uriserv%3AOJ.L_.2018.026.01.0048.01.ENG.

[38] S. Government, "Scottish regulators' strategic code of practice," 2015. https://www.gov.scot/publications/scottish-regulators-strategic-code-of-practice/.

[39] L. W. Power, "The lesser-known decision of the court of justice of the european union," 2015. https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/weltimmo-the-lesser-known-decision-of-the-court-of-justice-of-the-european-union.

[40] I. C. law, "C-230/14 - weltimmo," 2015. http://curia.europa.eu/juris/liste.jsf?num=C-230/14.

[41] V. Papakostantinou and P. de Hert, "The new general data protection regulation: Still a sound system for the protection of individuals," *Computer Law & Security Review*, vol. 32, pp. 179–194, 2016.

[42] K. Irion and G. Luchetta, "Online personal data processing and eu data protection reform," in *CEPS Task Force Report of the CEPS Digital Forum*, 2013.
[43] E.-L. A. to European Union law, "Consolidated version of the treaty on the functioning of the european union," 2012. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF?uri=CELEX:12012E/TXT&from=EN.
[44] W. G. Voss, "Looking at european union data protection law reform through a different prism: The proposed eu general data protection regulation two years later," *Journal of Internet Law*, vol. 17, no. 9, 2009.
[45] welivesecurity, "Is gdpr good or bad news for business?," 2017. https://www.welivesecurity.com/2017/02/09/gdpr-good-bad-news-business/.
[46] Deloitte, "Gdpr top ten #10: One stop shop." https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-one-stop-shop.html.
[47] EDPB, "European data protection board." https://edpb.europa.eu/edpb_en.
[48] G. Maldoff, "Top 10 operational impacts of the gdpr: Part 3 – consent," 2016. https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/.
[49] M. Hintze, "Viewing the gdpr through a de-identification lens: A tool for compliance, clarification, and consistency," *International Data Protection Law*, vol. 8, no. 1, pp. 86–101, 2018.
[50] W. G. Voss, "European union data privacy law reform: General data protection regulation, privacy shield, and the right to delisting," *Business Lawyer*, vol. 72, no. 1, pp. 221–233, 2017.
[51] Deloitte, "Gdpr top ten: #6: Privacy by design and by default," 2017. https://www2.deloitte.com/lt/en/pages/legal/articles/gx-gdpr-top-ten-privacy-design-default.html.
[52] R. O'Brien, "Privacy and security: The new european data protection regulation and it's data breach notification requirements," *Business Information Review*, vol. 33, no. 2, pp. 81–84, 2016.
[53] E. Lachaud, "Why the certification process defined in the general data protection regulation cannot be successful," *Computer Law & Security Review*, vol. 32, 2016.
[54] E. Lachaud, "The general data protection regulation contributes to the rise of certification as regulatory instrument," 2017.
[55] IAPP, "Top 10 operational impacts of the gdpr: Part 9 - codes of conduct and certifications," 2016. https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-9-codes-of-conduct-and-certifications/.
[56] A. Cook, R. Smith, L. Maglaras, and H. Janicke, "Measuring the risk of cyber attack in industrial control systems," BCS eWiC, 2016.
[57] E.-L. A. to European Union law, "Judgment of the court (grand chamber). google spain sl and google inc. v agencia española de protección de datos (aepd) and mario costeja gonzález.," 2014. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.
[58] F. Bieker, M. Friedewald, M. Hansen, H. Obersteller, and M. Rost, "A process for data protection impact assessment under the european general data protection regulation," in *Privacy Technologies and Policy*, pp. 21–37, Springer International Publishing, 2016.
[59] E. Commission, "Guidelines on the right to "data portability"," 2017. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.
[60] NIS, "National inventory systems." https://nis.spherical.pm/.
[61] NCSC, "The national cyber security centre." https://www.ncsc.gov.uk/.
[62] G. Associates, "The data protection principles under the general data protection regulation," 2019. https://www.gdpr.associates/the-data-protection-principles-under-the-general-data-protection-regulation/.
[63] I. O. for Standardization, "Iso/iec 27001 information security management." https://www.iso.org/isoiec-27001-information-security.html.
[64] A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, "A novel hierarchical intrusion detection system based on decision tree and rules-based models," in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 228–233, IEEE, 2019.
[65] A. Cook, H. Janicke, R. Smith, and L. Maglaras, "The industrial control system cyber defence triage process," *Computers & Security*, vol. 70, pp. 467–481, 2017.